(19) CONFEDERAZIONE SVIZZERA
ISTITUTO FEDERALE DELLA PROPRIETÀ INTELLETTUALE

(11) CH 709 506 A2

(51) Int. Cl.: G06F 21/34 (2013.01)
G06F 21/72 (2013.01)

Domanda di brevetto per la Svizzera ed il Liechtenstein
Trattato sui brevetti, del 22 dicembre 1978, fra la Svizzera ed il Liechtenstein

(12) DOMANDA DI BREVETTO

(21) Numero della domanda: 00573/14

(22) Data di deposito: 14.04.2014

(43) Domanda pubblicata: 15.10.2015

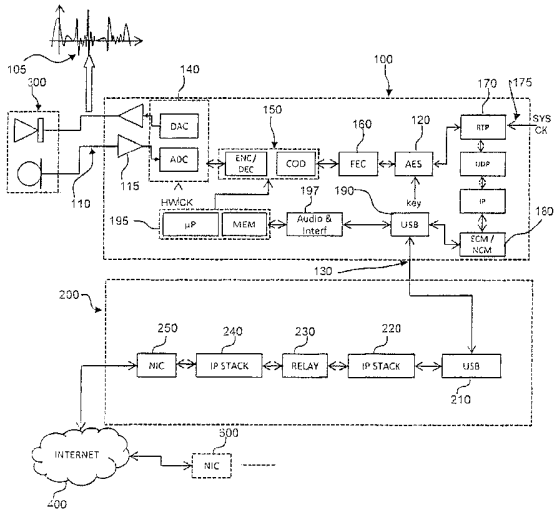
(71) Richiedente:
Quantec SA, Corso San Gottardo 86
6830 Chiasso (CH)

(72) Inventore/Inventori:
Pierluigi Pentimalli, 35030 Selvazzano Dentro (IT)

(74) Mandatario:
Fiammenghi-Fiammenghi, Via San Gottardo 15
6900 Lugano (CH)

(54) Dispositivo portatile di ricetrasmissione di flussi audio crittografati e metodo associato.

(57) Metodo di ricetrasmissione di flussi multimediali crittografati tra almeno un primo ed un secondo utente, il detto metodo essendo caratterizzato dal fatto di comprendere l'utilizzo di un dispositivo (100) di ricetrasmissione di flussi multimediali connesso ad un rispettivo elaboratore elettronico (200) da parte sia del primo che del detto secondo utente; il detto metodo comprendendo un primo passo di attivazione preventiva di una sessione di comunicazione in chiaro tra detto primo e detto secondo utente attraverso un software per l'effettuazione di comunicazioni multimediali nella quale il detto dispositivo (100) opera in una prima configurazione di trasmissione in chiaro, e un secondo passo di instaurazione di una comunicazione crittografata, nella quale il detto dispositivo (100) opera in una seconda configurazione di ricetrasmissione cifrata per mezzo di uno stadio o motore crittografico (120); detto metodo comprendendo un passo in cui il detto dispositivo (100) causa l'apertura di una sessione per trasferimento dati crittografati tra gli elaboratori elettronici (200) del detto primo utente e detto secondo utente distinta dalla sessione di comunicazione in chiaro utilizzata dal detto software per l'effettuazione di chiamate, ed in cui un flusso dati almeno audio ricetrasmesso tra i due utenti durante la loro comunicazione è selettivamente commutato tra detta sessione di comunicazione in chiaro e detta sessione di trasferimento dati crittografati sulla base di un criterio predefinito; detto metodo comprendendo un passo in cui il dispositivo (100) continua a utilizzare contemporaneamente il canale multimediale del software di comunicazione preesistente mentre protegge la comunicazione tra i due utenti commutata sul canale crittografato.



Descrizione

Campo della tecnica

[0001] La presente invenzione riguarda il campo dei dispositivi elettronici in grado di crittografare dei dati e informazioni in formato digitale al fine di renderli più sicuri, ed in dettaglio concerne un dispositivo portatile di ricetrasmissione di flussi audio crittografati. La presente invenzione concerne altresì un metodo di ricetrasmissione di flussi audio crittografati.

Arte nota

[0002] La tecnologia di comunicazione che permette la trasmissione di flussi di dati audio e/o video su reti a protocollo IP, altresì nota in una sua caratterizzazione come VoIP, con la sua crescente diffusione sta ridefinendo gli standard di comunicazione per l'utenza nel suo complesso, sia che si tratti di utenti finali (cc.dd. end user), sia che si tratti di operatori del settore media o del settore delle telecomunicazioni (quali i carrier telefonici, le società di servizio, ISP, fornitori di accesso, etc).

[0003] Sono pubblicamente noti diversi tipi di soluzioni di comunicazione VoIP, nella maggior parte dei casi di tipo software, che sono integrate e/o integrabili su computer, set-top-box, radiotelefoni cellulari, tablet PC o altri dispositivi elettronici similari.

[0004] Esistono poi prodotti hardware, come telefoni VoIP, di tipo cablato o cordless, destinati ad utenti finali a livello domestico, SOHO, piccole e medie imprese, e soluzioni di comunicazione via protocollo IP di tipo infrastrutturale su rete specifica, che sfruttano gateway, proxy VoIP, gatekeeper o conference servers per trattare e gestire flussi in streaming VoIP e, più generalmente, flussi di tipo multimediale.

[0005] Con VoIP generalmente si definisce una ben precisa tipologia tra le varie tecnologie per la comunicazione di flussi media audio e/o video; spesso, a causa della fama ormai acquisita, con VoIP, ci si riferisce automaticamente a software già noti e molto diffusi come, ad esempio, Skype® che grazie all'implementazione di una propria rete P2P (Peer to Peer) evoluta di tipo «SP2P» (Super P2P) è riuscito a crescere nel tempo raggiungendo una dimensione mondiale sostenendo, contemporaneamente, milioni di comunicazioni in tempo reale.

[0006] Alla base del VoIP risiede la possibilità di trasmettere una voce codificata in modo numerico su un flusso dati di tipo generico, frutto di una complessa elaborazione matematica basata, come di principio, sulla ciclicità del parlato umano. E' infatti noto che campionando il parlato umano su finestre temporali dell'ordine di qualche millisecondo, la forma d'onda, corrispondente al parlato umano campionato e trasformato in segnale elettrico, assume una certa periodicità. Nel corso degli anni sono stati quindi sviluppati dei codificatori o codec audio, principalmente per applicazioni di telefonia mobile su rete cellulare e/o satellitare e poi anche per VoIP, che si occupano di modellare il parlato umano attraverso funzioni matematiche traducibili in flussi dati numerici, che sfruttano la scomposizione della voce umana secondo una pluralità di parametri che comprendono ad esempio e non limitatamente, l'ampiezza del suono in frequenza (pitch), il guadagno associato (gain), o le frequenze delle formanti dei vari fonemi. Il flusso di dati analogico che proviene ad esempio da un microfono viene dapprima acquisito e trasformato in digitale, poi compresso e infine codificato con tecniche con o senza perdita di qualità, in modo tale che una volta decodificato e decompresso si possa rigenerare un flusso dati audio che sia il più simile possibile all'originale o che più in generale preservi al meglio possibile la comprensibilità del parlato.

[0007] Esistono codificatori audio di svariate tipologie e classi (CELP, MELP, ACELP), di cui alcuni sono soggetti a licenza d'uso. I codec per applicazioni VoIP moderni, che tra l'altro sono utilizzati per applicazioni di telefonia mobile, generalmente appartengono alla classe AMR-WB. Tecnicamente, questi codificatori multirate adattativi, trattano flussi dati audio almeno a 16 kHz e 16 bit, la cui banda passante è cioè pari a 8 kHz, notevolmente più larga (da cui il nome «wide») rispetto ai vecchi codec con banda passante reale di 3.2–4 kHz dei sistemi di telefonia precedenti. Esistono poi codec in grado dì gestire delle bande passanti ancora maggiori, e cioè in grado di riprodurre in modo sempre più fedele segnali audio contenenti componenti in frequenza sempre più alte, estendentisi fino anche a 20 kHz. Tali codec sono noti in gergo tecnico con il nome di super-wideband o full band.

[0008] Si può quindi affermare in modo riassuntivo, che alla base di ogni buon sistema VoIP ci siano almeno i seguenti elementi:

- un buon network di comunicazione, almeno in grado di recuperare e gestire eventuali errori di comunicazione (packet loss, jitter, etc. ...). disconnessioni e transienti, di collegare due o più utenti velocemente, e di instradarne le chiamate sul percorso migliore;
- un buon codec per flussi audio di tipo «speech», ovvero VoIP
- un buon sistema di segnalazione e gestione delle chiamate (tra i più noti, si può citare a mero titolo di esempio il protocollo SIP-Session Initiation Protocol);
- un'interfaccia utente, che sia preferibilmente intuitiva e semplice nell'utilizzo.

[0009] Come illustrato in fig. 1, la quale mostra un diagramma a blocchi schematico di un sistema di VoIP di tipo noto su di un singolo lato utente, i sistemi di. tipo noto presentano un assieme trasduttore audio 1, che nell'esempio riportato in figura è realizzato da ima cuffia con microfono, che attraverso uno stadio amplificatore o buffer 2, instrada il flusso audio captato dal microfono verso un convertitore analogico/digitale 3, che riceve in ingresso – oltre al flusso dati audio analogico

105 proveniente dallo stadio amplificatore o buffer 2 – anche un segnale di clock tipicamente proveniente dall'hardware, dell'elaboratore elettronico sul quale è in esecuzione il sistema VoIP o, nel caso di sistemi digitali come cuffie con microfono ad esempio con collegamento USB, generato internamente. Il flusso audio diviene quindi un flusso dati numerico (generalmente in formato PCM, Pulse Code Modulation) che viene trasmesso in ingresso ad un macroblocco 4 di codifica entro il quale esso è dapprima codificato dai codec audio 4a e successivamente elaborato da un codificatore di canale 4b per essere trasmesso ad uno stadio di forward error correction (FEC) 5, e quindi cifrato da uno stadio di criptazione o motore crittografico 6 (che ad esempio e non limitatamente può impiegare una algoritmo di tipo AES o altri algoritmi di cifratura a blocchi) che riceve in ingresso sia il flusso dati elaborato dallo stadio di forward error correction (FEC) 5, sia una chiave 7 crittografica ignota – che nella pratica è scambiata con tutti i partecipanti ad una medesima chiamata in conferenza (o conference) protetta oppure, più in generale, in grado di accedere al contenuto multimediale in tal modo protetto. Successivamente il flusso dati è passato a livello applicazione su protocollo RTP (blocco RTP 8), sfruttando un segnale di clock di sistema 9 (SYS CK) in modo tale da garantire la corretta gestione dei flusso dati come servizio di comunicazione in tempo reale sulla rete di comunicazione, tipicamente Internet. Quindi, il flusso dati è inviato ad uno stadio UDP 10 che opera una conversione verso il protocolio UDP per poi passare i pacchetti di dati così elaborati allo stack IP 11 e quindi al controllore di interfaccia di rete 12 che fisicamente provvede a trasmettere i dati fuori dall'elaboratore elettronico sulla rete Internet 13, verso il controllore di interfaccia di rete 14 del destinatario (indifferentemente uno o più di uno).

[0010] E' da notare che al giorno d'oggi le applicazioni software VoIP contemplano altre funzioni secondarie quali chat (Instant Messaging) o scambio in tempo reale di file. L'evoluzione dei software per Voice-over-IP è divenuta tale da trasformarli in veri e propri sistemi groupware di classe enterprise, come ad esempio e non limitatamente Microsoft® Lynk® o Skype® nelle sue declinazioni business.

[0011] La Richiedente ha osservato che allorché si trasmette un flusso dati su di una rete non protetta com'è Internet, dal punto di vista della sicurezza sia che questi dati af'feriscano da un ambiente generico (dati, trasmissione di file, audio e video streaming, etc.) o sia che essi siano dati specifici di una comunicazione VoIP non v'è alcuna differenza: l'unico modo per proteggere la comunicazione da intercettazioni altrui, consiste nel non lasciarla più «in chiaro» ricorrendo alla crittografia e contemporaneamente facendo in modo che la chiave crittografica sia sempre sotto il proprio controllo e cambi di volta in volta; ciò implica che ad ogni nuova sessione di comunicazione di anche tra due medesimi utenti, la chiave crittografica non sia mai la stessa, e si utilizzino pertanto chiavi crittografiche a perdere, o one-time keys. Se questo non può essere garantito, la comunicazione benché crittografata perde sicurezza. Infine, la crittografia senza il controllo della chiave crittografica non garantisce un sufficiente livello di riservatezza per lo scambio dei dati, qualunque essi siano.

[0012] Infatti, anche proteggendo la chiave crittografica, la crittografia eseguita su di un elaboratore elettronico a livello software non è sicura: per essere sicura dovrebbe essere- gestita a livello hardware su di un dispositivo autonomo, e in qualche modo indipendente dall'elaboratore elettronico stesso, dall'inizio alla fine del processo di ricetrasmissione di dati.

[0013] In altre parole, la Richiedente ha notato che analogamente a quanto avviene con la funzione di stampa dello schermo su di un tradizionale personal computer, è sempre possibile acquisire i flussi audio in chiaro trasmessi da un elaboratore elettronico, ancorché numerici. Leggendo direttamente dalla periferica audio del computer, o leggendo direttamente nella memoria RAM i byte in transito da e verso la periferica hardware di riproduzione ed acquisizione audio (cioè, la scheda audio), utenti mal intenzionati possono estrarre dal flusso di dati il messaggio «in chiaro» attraverso una post-elaborazione delle informazioni in tal modo acquisite piuttosto semplice, addirittura ricorrendo a programmi largamente disponibili in Internet.

[0014] Per la Richiedente, quindi, le soluzioni di comunicazione VoIP prettamente software non sono sicure, siano esse in esecuzione in un normale personal computer di ogni tipo e genere, così come in uno smartphone, tablet e dispositivo mobile di ultima generazione. Pertanto, anche noti software VoIP addirittura come Skype® non sono in grado di fornire una sufficiente sicurezza nella trasmissione di flussi audio e più in generale flussi media, in quanto benché il software stesso provveda a crittografare il flusso dati audio, l'acquisizione e la riproduzione del flusso stesso avviene da una periferica (la scheda audio del dispositivo utilizzato, appunto) che trasmette e riceve, evidentemente, «in chiaro», senza alcuna capacità crittografica nativa, ovvero hardware. Inoltre, la chiave crittografica eventualmente utilizzata non è nota all'utente, bensì gestita direttamente dal produttore/realizzatore del software. E', quindi, ignota al reale utilizzatore del sistema VoIP o, comunque, del sistema dì trasmissione e ciò crea un'ulteriore intrinseca debolezza nel sistema di trasmissione sicura del flusso audio vocale.

[0015] La Richiedente ha inoltre notato come i codec audio dei software di comunicazione VoIP non siano in grado di gestire efficacemente un flusso dati generico in ingresso, ed in particolare un flusso dati audio crittografato ancor prima di essere codificato dal codec. Questo in quanto buona parte dei parametri di scomposizione e parametrizzazione di un segnale audio vocale che sono utilizzate dalle funzioni ed algoritmi dei codec, sono concepiti proprio per operare su di un segnale dotato di una certa periodicità temporale, e non su di un segnale crittografato la cui correlazione temporale e struttura di spettro in frequenza si differenziano sensibilmente da quanto avviene per la voce umana.

[0016] Dal documento WO 2013 121 275 è noto un dispositivo portatile per la crittazione/decrittazione e/o compressione/decompressione di dati il quale comprende almeno un chip di supporto per autenticazione, almeno una prima porta di input/output di dati adattata per essere interfacciata con dispositivi esterni, almeno una seconda porta di input/output

di dati adattata per essere interfacciata con dispositivi esterni; almeno un'unità di elaborazione dati che comprenda un microprocessore dotato di un motore crittografico.

[0017] La Richiedente, attraverso la presente invenzione, si prefigge quindi lo scopo di realizzare un dispositivo portatile di ricetrasmissione di flussi audio, video e/o audio e video crittografati che permetta ad un utente di comunicare in modo sicuro con un altro utente dotato del medesimo dispositivo.

[0018] Più in dettaglio, lo scopo che la Richiedente si prefigge è quello di fare si che l'utente possa comunicare in modo sicuro con un altro utente sfruttando una rete di trasmissione dati.

[0019] Ancora più in dettaglio, con la presente invenzione la Richiedente si prefigge di realizzare un dispositivo e di descrivere un metodo che permetta la detta ricetrasmissione mediante sistemi e/o software VoIP pre-esistenti.

Sommario dell'invenzione

[0020] Secondo la presente invenzione viene realizzato un metodo di ricetrasmissione di flussi multimediali almeno audio crittografati tra almeno un primo ed un secondo utente, il detto metodo essendo caratterizzato dal fatto di comprendere l'utilizzo di un dispositivo di ricetrasmissione di flussi multimediali connesso ad un rispettivo elaboratore elettronico da parte sia del primo che del detto secondo utente; il detto metodo comprendendo un primo passo di attivazione preventiva di una sessione di comunicazione in chiaro tra detto primo e detto secondo utente attraverso un software per l'effettuazione di chiamate nella quale il detto dispositivo opera in una prima configurazione di trasmissione in chiaro, e un secondo passo di instaurazione di una comunicazione crittografata, nella quale il detto dispositivo opera in una seconda configurazione di ricetrasmissione cifrata per mezzo di uno stadio o motore di crittazione; detto metodo comprendendo un passo in cui il detto dispositivo causa l'apertura di una sessione per trasferimento dati crittografati tra gli elaboratori elettronici del detto primo utente e detto secondo utente distinta dalla sessione di comunicazione in chiaro utilizzata dal detto software per l'effettuazione di chiamate, ed in cui un flusso dati almeno audio ricetrasmesso tra i due utenti durante la loro comunicazione è selettivamente commutato tra detta sessione di comunicazione in chiaro e detta sessione di trasferimento dati crittografati sulla base di un criterio predefinito.

[0021] Vantaggiosamente, la detta sessione di comunicazione di dati in chiaro utilizzata dal detto software per l'effettuazione di chiamate è mantenuta aperta durante la detta sessione di trasferimento di dati crittografati.

[0022] Vantaggiosamente, il detto criterio predefinito comprende la trasmissione di un codice identificativo, eseguita alternativamente da uno dei due dispositivi coinvolti nella detta comunicazione tra detto primo e secondo utente; la detta trasmissione del detto codice seme avvenendo mediante una sessione di comunicazione preventivamente aperta mediante il detto software per l'effettuazione di chiamate.

[0023] Vantaggiosamente, il detto codice seme causa la selezione di un codice di cifratura preventivamente memorizzato all'interno di una memoria di entrambi i detti dispositivi: detto codice di cifratura essendo mantenuto segreto su ognuno dei detti dispositivi ed essendo utilizzato per eseguire la crittazione del detto flusso di dati audio.

[0024] Vantaggiosamente, la detta sessione di trasferimento di dati crittografati causa una ricetrasmissione dei detti dati crittografati su di una rete di trasmissione dati suscettibile permettere la connessione tra detto primo e detto secondo utente.

[0025] In dettaglio l'instaurazione della detta sessione di comunicazione in chiaro comprende un passo di introduzione di un mezzo trasduttore audio in una porta o interfaccia di ingresso/uscita del detto dispositivo di ricetrasmissione di flussi multimediali preventivamente air instaurazione della detta sessione di comunicazione di trasferimento di dati crittografati, e comprende inoltre un passo di connessione del detto dispositivo di ricetrasmissione di flussi media ad un elaboratore elettronico attraverso una porta di comunicazione, la detta connessione causando la presentazione di un'interfaccia audio al detto elaboratore elettronico suscettibile di selezionare il detto dispositivo di ricetrasmissione di flussi media come periferica di input/output di stream audio ricevuti, trasmessi o direttamente elaborati dal detto elaboratore elettronico.

[0026] Secondo la presente invenzione viene inoltre realizzato un dispositivo di ricetrasmissione di flussi audio crittografati, il detto dispositivo comprendendo:

- almeno un porta o interfaccia di ingresso/uscita per flussi di dati almeno di tipo audio suscettibili di essere trasmessi e/o ricevuti in chiaro da/verso mezzi trasduttori,
- almeno una porta o interfaccia di connessione con un elaboratore elettronico, detta porta o interfaccia di connessione essendo configurata per permettere almeno di trasmettere e/o ricevere un flusso di dati almeno audio crittografato rispettivamente da e/o verso il detto elaboratore elettronico:
- uno stadio o motore di crittazione, elettricamente connesso a detta porta o interfaccia di ingresso uscita e a detta porta o interfaccia di connessione, e configurato per fornire e rispettivamente ricevere a/da detta porta o interfaccia di connessione un flusso dati crittografato contenente almeno dati, di tipo audio;
  ed in cui il detto dispositivo è configurato per presentare al detto elaboratore elettronico un'interfaccia di ricetrasmissione di dati almeno audio; il detto dispositivo inviando al detto elaboratore elettronico, secondo un criterio predeterminato, un comando per la commutazione della ricetrasmissione del detto flusso dati almeno audio ricetrasmesso da/verso detta almeno una porta o interfaccia di ingresso/uscita.

[0027] In dettaglio, il dispositivo è configurato per permettere la trasmissione del detto flusso dati audio e/o video attraverso la detta interfaccia di ricetrasmissione di dati audio e/o video in chiaro verso un software di comunicazione preesistente, preferibilmente di tipo VoIP, suscettibile di interconnettere almeno un primo utente con un secondo utente; detto dispositivo essendo configurato per ricevere un comando di commutazione verso una sessione di comunicazione crittografata; detto stadio o motore crittografico essendo attivato da detto comando o segnale di commutazione.

[0028] Vantaggiosamente la detta interfaccia di ricetrasmissione di dati audio e/o video è un'interfaccia di tipo Audio Class.

[0029] Vantaggiosamente, il detto stadio o motore crittografico opera una crittazione del detto flusso di dati audio e/o video con una chiave utilizzata una sola volta, selezionata sulla base di un segnale di codifica di seme condiviso con un secondo utente del medesimo dispositivo e generata a partire da un segreto comune tra i dispositivi e già noto a priori nonché dal un mutuo scambio di dati specifici tra il detto dispositivo ed un altro dispositivo coinvolto nella comunicazione.

[0030] Vantaggiosamente detti dati specifici comprendono almeno un codice di identificazione scambiato con un altro dispositivo prima dell'instaurazione della detta sessione di comunicazione crittografata, in cui lo scambio del detto codice di identificazione avviene su di una sessione preventivamente instaurata da software di comunicazione, ed in cui il detto dispositivo è configurato per trasmettere una richiesta di apertura della detta sessione crittografata per la ricetrasmissione dati a pacchetto verso un altro elaboratore elettronico, detti dati a pacchetto comprendendo il detto flusso dati crittografato scambiato tra detto dispositivo e detto elaboratore elettronico attraverso la detta porta o interfaccia di comunicazione.

[0031] Vantaggiosamente, la detta sessione di ricetrasmissione di dati a pacchetto è una sessione basata su di un protocollo di comunicazione di tipo UDP.

[0032] In dettaglio il detto dispositivo è configurato per causare il mantenimento dell'apertura di una sessione di comunicazione preventivamente aperta mediante il detto software per la comunicazione durante la trasmissione del detto flusso dati crittografato su detta sessione crittografata per la ricetrasmissione di dati a pacchetto.

[0033] In dettaglio, il detto dispositivo è vantaggiosamente configurato per causare la trasmissione di un segnale fittizio verso detto software per la comunicazione.

[0034] Il detto segnale fittizio è vantaggiosamente selezionato tra un rumore bianco e/o detto codice seme.

[0035] Vantaggiosamente, il dispositivo comprende uno stadio di codifica audio avente un ingresso alimentato con un flusso di dati numerico comprendente almeno un flusso di dati audio ricevuto da mezzi trasduttori audio elettricamente connessi alla detta porta di input/output; detto stadio di codifica audio comprendendo mezzi di codifica e/o decodifica e/o compressione/decompressione audio specificatamente configurati per eseguire un'elaborazione numerica dei detti dati basata sulla codifica del parlato.

[0036] In dettaglio, i detti mezzi di codifica sono vocoder del tipo o derivati del Code-Excited Linear Predictor, Mixed-Excitation Linear Prediction o Algebraic Code-Excited Linear Prediction.

[0037] Vantaggiosamente, infine, il detto dispositivo comprende inoltre uno stadio di conversione analogico/digitale ricevente, avente un ingresso alimentato dalla detta porta o interfaccia di input/output e un'uscita alimentante il detto ingresso del detto stadio di codifica audio con il detto flusso dati numerico comprendente una trasformazione nel dominio digitale del detto stream audio.

Descrizione delle figure annesse

[0038] L'invenzione verrà ora descritta con riferimento alle figure allegate in cui:

la fig. 1 illustra uno schema a blocchi di un sistema di trasmissione di flussi audio del tipo voice-over-fP di tipo noto;

la fig. 2 illustra uno schema a blocchi del dispositivo di ricetrasmissione di flussi audio crittografati. oggetto della presente invenzione, allorché connesso con un elaboratore elettronico;

la fig. 3 illustra un diagramma rappresentante una pluralità di interfacce che vengono presentate all'elaboratore elettronico allorché il dispositivo oggetto della presente invenzione vi viene connesso;

la fig. 4 illustra uno schema a blocchi semplificato in cui un primo ed un secondo utente comunicano tra loro mediante rispettivi assiemi comprendenti un proprio elaboratore elettronico ed un proprio dispositivo oggetto della presente invenzione secondo una configurazione di tipo peer-to-peer;

la fig. 5 illustra uno schema a blocchi esemplificativo della commutazione tra una sessione di comunicazione tra il detto primo e secondo utente attraverso un software VoIP installato sul detto elaboratore elettronico e una sessione di comunicazione sicura, in cui il flusso di dati è dapprima crittografato dal dispositivo oggetto della presente invenzione;

la fig. 6 illustra un diagramma rappresentante la coesistenza di una prima sessione di comunicazione gestita dal detto software VoIP ed una seconda sessione di comunicazione sicura gestita attraverso il dispositivo oggetto della presente invenzione;

la fig. 7 illustra uno schema simile a quello di fig. 4, ma in cui la comunicazione tra i due utenti avviene su di un sistema di tipo client/server.

Descrizione dettagliata dell'invenzione.

DEFINIZIONI

[0039] Ai sensi della, presente invenzione per elaboratore elettronico si deve intendere un qualsiasi sistema o dispositivo elettronico in grado di scambiare un flusso di dati, preferibilmente quantunque non limitatamente a pacchetto attraverso di un canale di comunicazione qualsiasi con un altro sistema o dispositivo elettronico del medesimo o diverso tipo; il detto elaboratore elettronico deve possedere un'unità di elaborazione dati o microprocessore in grado di causare la ritrasmissione almeno parziale del detto flusso di dati verso un dispositivo hardware esterno – nello specifico il dispositivo oggetto della presente invenzione – attraverso una porta, di comunicazione digitale; conseguentemente, una lista non esaustiva di dispositivi elettronici in grado di essere considerati «elaboratori elettronici» ai sensi della presente invenzione comprende dei personal computer, dei computer di tipo desktop e workstation oppure di tipo server, tablet PC o elaboratori di tipo portatile, utilizzanti un qualunque sistema operativo di tipo libero (Linux, etc.) o soggetto a uso in-licenza (Windows, Mac OS, etc), telefoni cellulari di tipo smartphone, etc.

[0040] Ai sensi della presente descrizione si farà riferimento a flussi di dati numerici o digitali di tipo media o multimediali per intendere flussi dati audio e/o audio video.

[0041] Ai sensi della presente invenzione con l'acronimo VoIP o Voiee-over-IP si intende l'insieme dei protocolli di comunicazione digitali e di tecnologie in grado di permettere una conversione telefonica e/o audiovisiva su di una rete Internet o su di altri tipi di rete a commutazione a pacchetto in cui vengano impiegati, generalmente ma non limitatamente, protocolli senza connessione (protocolli del tipo IP di classe datagram del tipo UDP) per il trasporto di dati numerici, non afferenti al dominio analogico.

[0042] E' da notare che benché nel corso della presente invenzione si faccia riferimento ad un esempio preferito di macrosistema di ricetrasmissione di comunicazioni sicure attraverso la rete Internet, tale tipologia specifica di rete di scambio dati non deve essere intesa in modo limitativo come unico canale di supporto della trasmissione dati. Infatti, l'elaboratore elettronico sopra descritto potrà trasmettere informazioni su di una qualunque rete di trasmissione dati e, conseguentemente su di un canale di. trasmissione, anche non cablata o non fisica quale è ad esempio la rete telefonica cellulare, la rete telefonica satellitare o una rete radio/cellulare privata, o ancora una rete di tipo geografica come Internet oppure una rete privata virtuale (VPN), una rete Intranet, una rete locale (LAN) o anche personale (PAN) realizzata tramite tecnologie wireless come Bluetooth, Wi-Fi e così via.

[0043] Nel corso della presente descrizione verranno presentate differenze tra trasmissioni in chiaro e trasmissioni crittografate; il punto di «osservazione» della cifratura è posizionato all'ingresso di ogni elaboratore elettronico che verrà descritto nel corso della presente descrizione. Pertanto sono da intendersi come «in chiaro» tutte quelle comunicazioni crittografate a livello software o hardware all'interno dell'elaboratore elettronico e/o direttamente dal programma software VoIP, o ancora tutte quelle comunicazioni che non sono crittografate del tutto. Viceversa, le trasmissioni crittografate sono quelle la cui operazione di crittazione è effettuata da hardware e/o software esterno all'elaboratore elettronico stesso.

DESCRIZIONE DEL DISPOSITIVO

[0044] Come illustrato in fig. 2, con il numero di riferimento 100 è indicato nel suo complesso un dispositivo portatile di ricetrasmissione di flussi media crittografati, il quale è configurato per permettere una ricetrasmissione di dati media o multimediali almeno di tipo audio con comunicazioni protette tra un primo ed un secondo utente posizionati in posizioni remote, ognuno dotato di un elaboratore elettronico 200 al quale connettere un rispettivo dispositivo 100: gli elaboratori elettronici 200 sono tra di loro connessi su di una rete di trasmissione dati 400.

[0045] La forma di realizzazione preferita e non limitativa del dispositivo 100 oggetto deila presente invenzione comprende una prima porta o interfaccia di input/output 110 per stream audio, che alimenta in ingresso uno stadio di buffer o amplificatore 115 la cui uscita è elettricamente connessa con uno stadio di conversione analogico/digitale 140, il quale riceve in ingresso un segnale di clock HW CK proveniente da un generatore interno al dispositivo oggetto della presente invenzione. Lo scopo dello stadio di conversione analogico/digitale 140 è quello di convertire lo stream audio che è nel dominio analogico in un flusso di dati numerico che possa – attraverso una serie di elaborazioni che verranno descritte in dettaglio in seguito – essere suscettibile di essere crittografato.

[0046] Preferibilmente, quantunque non limitatamente, la prima porta o interfaccia d input/output 110 è un jack femmina per la connessione di un set cuffia/microfono, ma tale tipologia di connettore non deve essere intesa in modo limitativo; la

definizione di «interfaccia» vuole quindi individuare anche quelle connessioni con i set di cuffia/microfono di tipo wireless, o con altre porte diverse da un tradizionale jack audio come ad esempio, ma non limitatamente, l'interfaccia USB.

[0047] Dopo lo stadio di conversione analogico/digitale 140 si crea quindi un flusso dati di tipo numerico continuo nei tempo e il cui contenuto rappresenta la digitalizzazione, del segnale analogico 105 catturato o trasmesso dai mezzi trasduttori 300, rappresentati ad esempio da un assieme di cuffia e microfono elettricamente connessi alla porta di input/output 110, la quale può essere nello specifico e non limitatamente un connettore jack di tipo femmina, tradizionalmente usato per la connessione di cuffie con microfono.

[0048] Lo stadio di conversione analogico/digitale 140 alimenta un ingresso di uno stadio di codifica audio 150 il quale comprende un encoder audio ed un codificatore di canale. Preferibilmente, quantunque non limitatamente, lo stadio di codifica audio 150 è un vocoder di tipo a predizione lineare, del tipo Code-Excited Linear Predictor, Mixed-Excitation Linear Prediction o Algebraic Code-Excited Linear Prediction. Successivamente, lo stadio di codifica audio 150 invia il flusso dati codificato verso uno stadio di codifica FEC 160, il quale provvede ad elaborare il flusso dati numerico introducendo ad esempio bit ridondanti al flusso informativo costituito dal flusso di dati numerico.

[0049] Il flusso di dati così codificato è trasmesso ad uno stadio di crittografia 120 il quale comprende al suo interno un motore crittografico, preferibilmente operante su blocchi di dati come nel caso della codifica AES, DES, 3DES, Ghost.

[0050] Attraverso lo stadio di crittografia 120 si implementa una crittazione del flusso di dati con una chiave crittografica di sessione del tipo usa e getta, in modo tale che a parità di utenti, ogni nuova sessione di comunicazione venga crittografata con una chiave diversa. Più in dettaglio, la chiave utilizzata per la crittografia del flusso dati è selezionata sulla base di un codice seme (o seed) che è l'unico ad essere trasmesso sul canale di comunicazione tra i due elaboratori elettronici 200 del primo e secondo utente. La chiave crittografica è derivata da tale codice seme, che è trasmesso una sola volta ed è pertanto definito number at once (nonce), ed è preferibilmente generato da chi inizia la comunicazione. Il codice seme o number at once è anch'esso generato dallo stadio di crittografia 120 e preferibilmente è rappresentato da un numero di 256 bit ad aita entropia. La chiave crittografica è derivata da tale number at once tramite una funzione di hashing non biettiva del tipo SA 256 o superiore.

[0051] E' da notare che dato che l'AES256 è un protocollo di crittografia a blocchi concepito per operare su blocchi di dati di una predeterminata dimensione, è necessario un suo adattamento al fine di renderlo compatibile con un flusso di dati numerici contenente dati di tipo almeno audio, quantunque codificati e/o elaborati; infatti, tale flusso di dati assume le caratteristiche peculiari di uno stream, in cui i vari frame audio hanno dimensione molto piccola e tipicamente variabile; l'elaborazione apportata sull'algoritmo di crittografia è, vantaggiosamente e non limitatamente, una tecnica standard di ciphertext styling.

[0052] Il flusso dati elaborato dallo stadio di crittazione 120 è passato a livello applicazione su protocollo RTP (stadio RTP 170), sfruttando un segnale di clock di sistema 175 in modo tale da garantire la corretta gestione del flusso dati come servizio di comunicazione in tempo reale su reti a latenza variabile e non predeterminata, come Internet. Quindi, il flusso dati così elaborato è inviato ad un ingresso di uno stadio ECM 180 (Ethemet Control Model) e da questo ad un controllore USB 190, il quale trasmette il flusso dati così elaborato su di una porta di comunicazione 130 che benché descritta e rappresentata come porta USB può essere una qualunque porta o interfaccia di comunicazione di dati tra un dispositivo hardware ed un elaboratore elettronico, anche non di tipo cablato ma wireless. Lo stadio ECM 180 può equivalentemente essere sostituito da uno stadio NCM (Network Control Model), anch'esso in grado di gestire sessioni di collegamento Ethernet-over-USB. Il flusso, dati audio è quindi crittografato a priori e fuori dall'elaboratore elettronico 200: una volta che detto flusso è trasmesso all'elaboratore stesso, il compito di quest'ultimo è sostanzialmente solo quello di trasferirlo verso l'altro utente coinvolto nella comunicazione sicura.

[0053] Quando il dispositivo 100 oggetto della presente invenzione è elettricamente connesso ad un elaboratore elettronico 200, il flusso dati trasmesso dal dispositivo 100 oggetto della presente invenzione è inviato ad una cascata di stadi comprendente un controllore USB interno 210, che alimenta un ingresso di un modulo di stack IP 220, il quale a sua volta scambia i dati con uno stadio reiay 230, ancora ad un IP stack 240 e ad uno stadio di interfaccia di rete 250, il quale permette la fuoriuscita dei dati elaborati verso la rete di comunicazione 400, e da questa verso l'elaboratore elettronico dell'altro utente della comunicazione, incontrando dapprima la sua interfaccia di rete 600 e poi gli altri blocchi nella sequenza identica ed opposta rispetto a quanto già descritto.

[0054] Come illustrato in fig. 3, il dispositivo 100 oggetto della presente invenzione, all'atto della connessione con l'elaboratore elettronico 200 si presenta con una pluralità di interfacce. In dettaglio, esse comprendono almeno: un'interfaccia di tipo MSD 100a o Memory Storage Device, che è tipica ad esempio di una chiavetta USB, un'interfaccia di tipo HID 100c ed un'interfaccia di tipo Audio Class 100b. Tale ultima interfaccia audio è selettivamente abilitata da un microcontrollore interno al dispositivo 100 oggetto della presente invenzione, e comprende una prima sottointerfaccia di registrazione ed una seconda sottointerfaccia di riproduzione, ed è in dettaglio configurata per trasmettere un messaggio di segnalazione di intenzione di avvio di una chiamata protetta verso l'altro utente. Attraverso l'interfaccia di tipo Audio Class 100b il software VoIP 500 identifica il dispositivo oggetto della presente invenzione come interfaccia audio. Infatti, l'interfaccia di tipo Audio Class 100b viene presentata all'elaboratore elettronico 200 all'atto della connessione del dispositivo 100 tramite la porta o interfaccia di connessione 130; all'atto della connessione, il dispositivo 100 oggetto della presente invenzione è configurato per fornire ulteriori informazioni a riguardo della presenza o meno dei mezzi trasduttori 300

connessi o meno alla porta o interfaccia di input/output 110. Tale tipo di informazioni fa parte dello standard di gestione di periferiche audio per tutti i tipi di sistemi presenti sul mercato ed è egualmente gestito da tutti i sistemi operativi dei vari elaboratori elettronici. In particolare, all'atto della, connessione del set cuffia/microfono nella porta o interfaccia di input/output 110, l'evento viene notificato dai dispositivo 100 all'elaboratore elettronico 200 e questo causa la commutazione del flusso dati audio da e verso il dispositivo 100 piuttosto che dal precedente mezzo trasduttore utilizzato dall'elaboratore elettronico.

[0055] Il dispositivo oggetto della presente invenzione è caratterizzato dal fatto di potersi interfacciare con software di tipo VoIP 500 di tipo preesistente ed installati sull'elaboratore elettronico presentando se stesso come dispositivo audio di riproduzione e registrazione (ovvero, più semplicemente ma non limitatamente: «cuffia con microfono») al fine di stabilire una comunicazione sicura e crittografata a partire da una comunicazione di tipo tradizionale. Pertanto quando si utilizza il dispositivo 100 per effettuare una comunicazione tra un primo utente A ed un secondo utente B, la struttura complessiva assume la forma illustrata in fig. 4, in cui a partire dal set cuffia/microfono che identifica i mezzi trasduttori 300, il segnale audio è inviato e ricevuto in modo bidirezionale, ed in dettaglio in modalità preferibilmente full-duplex, verso il dispositivo 100 secondo la presente invenzione e da quest'ultimo all'elaboratore elettronico 200, per poi transitare sulla rete di comunicazione 400 verso l'elaboratore elettronico 200 del secondo utente e quindi verso il suo set cuffia/microfono attraverso il rispettivo dispositivo 100. Il tutto mentre il dispositivo 100 continua a mantenere attiva, verso il software VoIP preesistente 500, la propria interfaccia Audio Class in modo che, quest'ultimo, possa a sua volta mantenere attivo il canale di comunicazione in chiaro sul quale verrà veicolato, vantaggiosamente ma non limitatamente, rumore bianco o altri segnali audio generati a partire dal dispositivo 100.

[0056] Per rendere tutto ciò realizzabile, il dispositivo 100 secondo la presente invenzione permette un inizio di comunicazione di tipo tradizionale, utilizzando il software VoIP di tipo preesistente, per poi commutare secondo un. criterio prestabilito su di una comunicazione protetta, che viene inizializzata su di una sessione di trasmissione dati separata rispetto a quella utilizzata dal software VoIP 500 e nella quale la crittografia del flusso di dati viene eseguita esternamente rispetto all'elaboratore elettronico, e cioè proprio all'interno del dispositivo 100 come sopra descritto. La fig. 5 illustra una rappresentazione schematica semplificata di tale commutazione; sostanzialmente è come se in ogni assieme elaboratore elettronico 200-dispositivo 100 vi fosse un commutatore virtuale in grado di fare commutare un flusso audio tra il software VoIP 500 preesistente ed il dispositivo 100 oggetto delia presente invenzione, utilizzando la-medesima rete di comunicazione ma aprendo una sessione di ricetrasmissione dati diversa rispetto a quella precedente.

[0057] Vantaggiosamente, mentre il dispositivo 100 rende sicuro il flusso audio così acquisito in ingresso dal trasduttore 300, il dispositivo 100 stesso continua a mantenere attivo il canale audio in chiaro verso il software preesistente riproducendo rumore bianco e/o altri segnali audio.

[0058] Durante la trasmissione dei dati crittografata, la comunicazione con il software VoIP preesistente viene mantenuta aperta, e sulla sessione gestita dal software di VoIP viene trasmesso – preferibilmente quantunque non limitatamente – un rumore bianco.

[0059] Più in dettaglio, è proprio attraverso il software VoIP 500 preinstallato sull'elaboratore elettronico 200 che è possibile trasmettere il codice identificativo utilizzato per selezionare la corretta chiave crittografica utilizzata dai dispositivi 100 coinvolti nella comunicazione; inoltre, l'avvio di una comunicazione «in chiaro» attraverso il software VoIP preinstallato sugli elaboratori elettronici 200 è necessaria, in quanto in alternativa non sarebbe possibile - da parte dell'utente chiamato – sapere chi lo sta chiamando e quando avviare la sessione di comunicazione crittografata. In particolare il termine «in chiaro» qui sopra riportato non deve essere inteso come riferito ad un software VoIP che non crittografi in alcun modo il flusso dati inviato sulla propria sessione di comunicazione, ma un flusso dati crittografato da mezzi di crittazione software all'interno dell'elaboratore elettronico 200 stesso, che per quanto detto prima non sono purtroppo in grado di assicurare la corretta protezione da attacchi di virus e malware.

[0060] Infine, il dispositivo 100 oggetto della presente invenzione può comprendere preferibilmente una memoria interna 195, controllata da un microprocessore, contenente una pluralità di messaggi audio preregistrati, tra i quali un messaggio di attesa di instaurazione di comunicazione sicura M2, un messaggio di richiesta di chiamata sicura MI, un messaggio di risposta alla richiesta di chiamata sicura M3 e un messaggio di mantenimento della comunicazione VoIP preesistente M4 che vengono utilizzati dal dispositivo stesso e trasmessi all'elaboratore elettronico 200 attraverso la porta o interfaccia di comunicazione 130 durante il processo di inizializzazione della sessione di comunicazione sicura e durante l'effettuazione della detta comunicazione sicura. Ulteriori dettagli di tali messaggi verranno descritti in seguito.

[0061] Per semplicità di rappresentazione memoria e microprocessore sono raggruppati entro un unico blocco, e sono elettricamente connessi sia con lo stadio di codifica 150 (al fine di poter quantizzare e/o comprimere i messaggi predefiniti prima dell'invio all'elaboratore elettronico) sia con il controllore USB 190, in quest'ultimo caso per mezzo di uno stadio di interfaccia audio 197 che è configurato per permettere di presentare all'elaboratore elettronico l'interfaccia di tipo Audio Class 100b allorché il dispositivo 100 viene connesso all'elaboratore elettronico 200.

[0062] Il dispositivo oggetto della presente invenzione si configura come in grado di operare correttamente sia che i due elaboratori elettronici 200 siano in una configurazione di tipo peer-to-peer, sia che essi abbiano una configurazione di tipo client/server. Al fine di chiarire al meglio la logica di funzionamento del dispositivo oggetto della presente invenzione, verrà qui di seguito descritto un esempio di chiamata tra un primo utente A ed un secondo utente B utilizzanti ognuno un

dispositivo 100, dapprima secondo una configurazione di tipo P2P come quella raffigurata in fig. 4 e successivamente con una configurazione di tipo client/server, rappresentata invece in fig. 7.

[0063] Preferibilmente, nella configurazione P2P almeno uno tra i due utenti A e B dispone di un elaboratore elettronico 200, avente caratteristiche di connettività ad Internet quali ad esempio e non limitatamente possibilità di download ed upload di dati, latenza minima, capacità di accettare connessioni in entrata tali da poter operare come server temporaneo nella comunicazione.

[0064] In un primo momento, il primo utente A connette il proprio dispositivo 100 ai suo elaboratore elettronico 200, e la propria cuffia/microfono direttamente nel dispositivo 100. A questo punto il primo utente A attiva il software VoIP preinstallato sull'elaboratore elettronico, andando a verificare se il secondo utente B che vuole chiamare è o meno in linea. In caso affermativo, lo chiama seguendo la tradizionale procedura di chiamata definita dal software VoIP. Fin qui, il dispositivo 100 - essendo visto dall'elaboratore elettronico 200 come interfaccia audio – riceve il flusso di dati audio proveniente dal computer come se fosse semplicemente un buffer, in altre parole, per il momento esso non apporta nessun'elaborazione di cifratura, effettuando solamente la codifica e decodifica del flusso dati e la sua conversione tra dominio analogico e dominio digitale.

[0065] L'utente B, che ancora non ha il dispositivo 100 connesso con il proprio elaboratore elettronico 200, vede che il proprio software VoIP squilla, e decide di rispondere. Fino a questo punto l'utente B non sa se il primo utente A lo stia chiamando «in chiaro» o meno, in quanto quest'informazione non è gestita dal software VoIP. Nondimeno, il dispositivo 100 del primo utente A non sa assolutamente con quale ulteriore dispositivo 100 si dovrà connettere.

[0066] Il secondo utente B risponde alla chiamata tramite il proprio software VoIP, e tramite gli altoparlanti del proprio computer o una qualsiasi altra periferica audio attiva, riceve il messaggio di richiesta di chiamata sicura MI precedentemente citato che è trasmesso dal dispositivo 100 del primo utente A; tale messaggio può essere ad esempio un messaggio vocale che recita: «Chiamata VoIP crittografata in ingresso; si prega di connettere il proprio dispositivo di cifratura all'elaboratore elettronico».

[0067] A questo punto il secondo utente B connette attraverso la porta o interfaccia di connessione 130 il proprio dispositivo 100 all'elaboratore elettronico 200, introducendo preferibilmente e non limitatamente un codice o credenziale di accesso che nella forma di realizzazione preferita qui descritta è rappresentato da una coppia username/password oppure da una singola master password/pin.

[0068] Durante questo intervallo di tempo tra il primo utente A ed il secondo utente B non è ancora presente una comunicazione «sicura», e l'utente A riceve sul proprio mezzo trasduttore 300 un segnale di chiamata in attesa o alternativamente il messaggio di risposta alla richiesta di chiamata sicura M3 proveniente dal dispositivo 100 in dotazione al secondo utente B, ad esempio: «Si prega di attendere; il vostro contatto sta completando il collegamento di comunicazione sicura» come anche, a sua volta, eventualmente il messaggio MI stesso inviato dall'utente B.

[0069] E' da notare che fintanto che il secondo utente B non connette al proprio dispositivo 100 un set cuffia/microfono, il dispositivo 100 non presenta la sua interfaccia audio verso l'elaboratore elettronico; di conseguenza, l'audio viene gestito dall'interfaccia audio preventivamente selezionata come predefinita dall'elaboratore elettronico stesso, e nessun flusso dati audio viene indirizzato verso il dispositivo 100 oggetto della presente invenzione, fintanto che il set cuffia/microfono non verrà attivato tramite l'inserimento nella porta o interfaccia di input/output 110.

[0070] E' importante quindi che in fase di ricezione di una chiamata, il dispositivo 100 oggetto della presente invenzione non esponga immediatamente all'elaboratore elettronico l'interfaccia audio o, comunque, anche se la esponesse questa non risulti attiva per l'elaboratore elettronico; se così fosse, e se l'utente B non avesse già il set cuffia/microfono connesso al dispositivo 100 attraverso la porta o interfaccia di input/output 110, esso non riuscirebbe più a sentire nulla.

[0071] A questo punto, il secondo utente B connette al dispositivo 100 il proprio set cuffia/microfono, il dispositivo 100 rileva tale connessione e comanda il proprio microcontrollore per trasmettere in chiaro, verso il detto software VoIP, un flusso dati audio che contiene un messaggio di identificazione di instaurazione di una chiamata VoIP sicura, in cui cioè la crittografia è eseguita esternamente all'elaboratore elettronico 200. Tale messaggio di attesa di instaurazione di comunicazione sicura M2 può essere ad esempio: «Chiamata sicura in fase di inizializzazione, attendere mentre si completa l'instaurazione della chiamata».

[0072] Proprio attraverso i messaggi audio predeterminati trasmessi tramite il software VoIP, messaggi che possono essere puramente vocali e/o contenenti un codice a toni ad esempio DTMF udibile, ogni dispositivo 100 connesso alla chiamata apprende quale è l'altro dispositivo chiamante attraverso la ricezione di un codice identificativo univoco (ID). In particolare, i due dispositivi 100 coinvolti nella chiamata, riescono a rilevare automaticamente l'avvio della chiamata VoIP grazie alle segnalazioni di start e di stop ricevute dal sistema operativo del proprio elaboratore elettronico 200. Sostanzialmente, quindi, quando il secondo utente B risponde alla chiamata, entrambi i software VoIP (sia del primo che del secondo utente) avviano l'endpoint o sottointerfaccia di registrazione dell'interfaccia audio presentata dal dispositivo 100 e, rilevato questo evento, entrambi i dispositivi 100 iniziano a riprodurre il messaggio audio aggiungendovi un proprio identificativo univoco.

[0073] Se il codice identificativo ID del dispositivo 100 del primo e/o secondo utente è trasmesso in uno dei messaggi audio predefiniti in modo offuscato, si utilizza una tecnica di steganografia applicata a flussi audio vocali; viceversa, se il codice identificativo ID è trasmesso con una tecnica di modulazione di tipo standard DTMF, si avrà una pluralità di valori

predeterminati (tipicamente ma non limitatamente da 0 a 15) che vengono introdotti all'interno del flusso dati prima della sua codifica tramite lo stadio di codifica audio 150, modulando segnali a diverse frequenze sintetizzati appositamente in modo artificiale dal dispositivo 100 oggetto della presente invenzione.

[0074] Viene quindi aperta una seconda sessione di comunicazione sicura, nella quale dapprima i due dispositivi 100 coinvolti nella comunicazione si scambiano i propri codici seme (seed) utilizzati a loro volta per derivare la chiave di crittografia univoca della sessione di comunicazione sicura, che si sta instaurando a partire da un segreto comune già noto a priori contenuto in entrambi i dispositivi e selezionato grazie all'identificativo univoco precedentemente ricevuto.

[0075] In tal modo, entrambi i dispositivi 100 commutano la comunicazione su di una sessione sicura distinta da quella utilizzata dal software VoIP, e provvedono a convertire, codificare e crittografare lo stream audio di origine utilizzando l'intera catena di stadi descritta in precedenza e rappresentata in fig. 2, inviando pacchetti dati digitali contenenti il detto messaggio audio crittografato verso l'elaboratore elettronico 200 e di conseguenza il dispositivo 100 dell'utente opposto.È' da notare che la comunicazione instaurata è di tipo full duplex. Il programma software VoIP continua a ricevere un flusso audio in chiaro, preferibilmente ma non limitatamente rumore bianco, e nel contempo un eventuale malware, virus o trojan presente nell'elaboratore elettronico non è minimamente in grado di accedere al contenuto della comunicazione sicura stabilita grazie alla crittografia apportata dal dispositivo oggetto della presente invenzione. Allorché i due elaboratori elettronici 200 sono connessi su di una rete internet, nella configurazione P2P essi si scambiano i pacchetti di dati contenenti il flusso dati crittografati basandosi sul protocollo di rete UDP con un flusso dati gestito secondo il protocollo di livello applicazione RTP (Real-time Transport Protocol, ISO/OSI application layer), che rappresenta lo standard più comunemente usato per la trasmissione di flussi di dati di tipo stream audio o video; l'uso del protocollo UDP per il supporto dell'RTP non deve essere considerato limitativo; esso può infatti essere supportato anche da un protocollo di tipo TCP o di altra tipologia, benché quest'ultimo sia più orientato al mantenimento di una integrità dei pacchetti a discapito del loro allineamento temporale.

[0076] Durante tutta la sessione di comunicazione sicura, la precedente sessione di comunicazione aperta dal software VoIP viene mantenuta aperta, e pertanto si hanno contemporaneamente due sessioni di comunicazione, come illustrato in fig. 6, nella quale una prima è quella standard, gestita dal programma software VoIP. Su tale sessione può essere ad esempio e non limitatamente trasmesso un rumore bianco o un altro flusso dati non correlato alla comunicazione tra i due utenti A e B, come ad esempio un messaggio di mantenimento di comunicazione VoIP che venga ripetuto ad intervalli di tempo regolari.

[0077] E' da notare come, nel caso esemplificativo e non limitativo rappresentato nelle figure annesse alla presente descrizione, la comunicazione sicura avvenga tra due utenti connessi tramite rispettivi elaboratori elettronici 200 su di una rete di comunicazioni 400 Internet. In tale soluzione i pacchetti di dati che contengono il segnale audio crittografato, viaggiano sulla rete Internet direttamente verso l'elaboratore elettronico destinatario o passano in alternativa in relay su di un server esterno. Tale passaggio aggiuntivo, che è opzionale e dipende dalla struttura o configurazione della rete, rende necessario che nel caso gli elaboratori elettronici 200 (che rappresentano gli endpoint) non riescano a stabilire una comunicazione diretta tra loro come potrebbe essere un peer-to-peer, si deve ricorrere ad un servizio di «rilancio» intermedio, che generalmente, è affidato ad un server dedicato; tale server dedicato, nei sistemi VoIP, è il cosiddetto «conference server».

[0078] Infine in fig. 7 è illustrata una configurazione della comunicazione tra il primo utente A ed il secondo utente B secondo uno schema di tipo client/server. In dettaglio, in tale configurazione il metodo di instaurazione della sessione di comunicazione crittografata è del tutto simile a quello precedentemente descritto per il caso della configurazione peer-to-peer; tuttavia, in questo caso l'invio dei pacchetti di dati sfruttando il protocollo di rete UDP (o TCP, come sopra descritto) e il protocollo di trasporto RTP non è effettuato direttamente tra i due elaboratori elettronici 200 sulla rete Internet, ma questi vengono inviati ad un server 800 di controllo centralizzato, che gestisce per ognuno dei due elaboratori elettronici 200 sia i flussi di dati entranti sia i flussi di dati uscenti, e li smista poi al corretto destintatario. Nella configurazione client/server diviene quindi più facile implementare delle sale conferenza virtuali nelle quali una pluralità di utenti, anche molto maggiore rispetto a due, possa parlare avendo la sicurezza che nessun malware, virus o trojan presente sugli elaboratori elettronici possa intervenire in modo maligno, captando la loro conversazione privata.

[0079] Allorché la comunicazione tra il primo ed il secondo utente termina, vengono chiuse entrambe le sessioni di comunicazione precedentemente instaurate, e ognuno degli utenti è a questo punto libero di arrestare il software VoIP 500 e disconnettere il dispositivo 100, oggetto della presente invenzione dal proprio elaboratore elettronico. Altresì, allorché uno dei due utenti termini la sessione di comunicazione agendo direttamente sul software VoIP preesistente, l'architettura del dispositivo crittografico oggetto della presente invenzione consente di chiudere automaticamente le sessioni di comunicazione sicura precedentemente instaurate.

[0080] I vantaggi del dispositivo 100, oggetto della presente invenzione sono chiari alla luce della descrizione che precede. Esso infatti permette all'utenza di effettuare delle comunicazioni sicure utilizzando software tradizionalmente conosciuti, senza che l'utente debba effettuare complicate operazioni per instaurare una comunicazione sicura. In particolare, il dispositivo descritto nella presente descrizione non è limitato all'utilizzo con specifici software, potendosi adattare senza modifiche a qualunque software o programma per elaboratore in grado di instaurare una comunicazione di tipo multimediale e, nello specifico ma non limitatamente, di tipo VoIP.

[0081] Vantaggiosamente, qualora l'utente desideri interrompere la detta comunicazione sicura, egli potrà ritornare in modo semplice e rapido direttamente sulla comunicazione in chiaro utilizzando il software di comunicazione VoIP che –

per tutta la durata della comunicazione sicura – può rimanere aperto e quindi attivo. Parimenti l'utente può fare anche il contrario, ovvero passare da una comunicazione in chiaro instaurata e già attiva tramite il software di comunicazione VoIP a una comunicazione crittografata e protetta semplicemente inserendo il proprio dispositivo crittografico con relativa periferica audio locale ad esso collegata.

[0082] Vantaggiosamente, il dispositivo secondo la presente invenzione è di piccole dimensioni, è esterno all'elaboratore elettronico e pertanto può essere facilmente trasportato ed utilizzato su elaboratori elettronici come precedentemente definito indipendentemente dal loro produttore o dal sistema operativo da essi utilizzato. Questo vantaggio è dato in particolare dal fatto che il dispositivo oggetto della presente invenzione sia dotato di una porta di comunicazione di tipo USB, che ad oggi è la porta di comunicazione standard più largamente usata nel mondo dell'elettronica informatica. Il dispositivo oggetto della presente invenzione può essere tuttavia dotato di altre tipologie di interfacce verso l'elaboratore elettronico sia di tipo elettromeccanico, sia wireless.

[0083] Vantaggiosamente, il dispositivo secondo la presente invenzione non permette a malintenzionati di accedere facilmente alla comunicazione sicura, proprio perché sia le chiavi crittografiche, sia la procedura di cifratura sono contenute al sicuro al proprio interno, ai di fuori dell'elaboratore elettronico. In tal modo, i tradizionali malware, Spyware, virus o trojan eventualmente in esecuzione nell'elaboratore elettronico non possono avervi accesso. Cosa ben diversa dai comuni sistemi di protezione software di dati e voce dove sia la chiave di cifratura, sia l'eventuale algoritmo crittografico risiedono totalmente nell'elaboratore elettronico in esecuzione nella pozione di memoria RAM in cui è in esecuzione il software di comunicazione utilizzato dall'utente.

[0084] In particolare, il dispositivo fin qui descritto fa si che anche avendo l'elaboratore elettronico infettato da programmi maligni in grado di catturare flussi audio e/o audio e video, e pur l'utente stesso continui ad utilizzare il proprio software di comunicazione preesistente, la comunicazione venga automaticamente e totalmente protetta a livello hardware non più dal software di comunicazione preesistente, in esecuzione nella memoria dell'elaboratore elettronico, bensì dal dispositivo esterno oggetto della presente invenzione.

[0085] Vantaggiosamente, infine, il dispositivo oggetto della presente invenzione può essere utilizzato con un qualunque tipo di cuffia dotata di microfono o essere equivalentemente collegato ad un set di altoparlanti e microfono del tipo tradizionalmente disponibile sul mercato.

[0086] Vantaggiosamente, il dispositivo secondo la presente invenzione può proteggere anche comunicazioni di tipo video o di tipo audio e video mediante la medesima logica di funzionamento e il collegamento alle proprie porte di comunicazioni di dispositivi esterni eterogenei come webcam USB, webcam Ethernet, telecamere e sistemi di videoconferenza in grado di comunicare su reti IP e collegate a tali reti e/o direttamente al dispositivo stesso tramite interfacce cablate o wireless e così via.

[0087] E' infine chiaro che al dispositivo 100 fin qui descritto possono essere applicate aggiunte o varianti ovvie per un tecnico del ramo senza per questo fuoriuscire dall'ambito di tutela fornito dalle rivendicazioni annesse.

Rivendicazioni

1. Metodo di ricetrasmissione di flussi multimediali crittografati tra almeno un primo ed un secondo utente, il detto metodo essendo caratterizzato dal fatto di comprendere l'utilizzo di un dispositivo (100) di ricetrasmissione di flussi multimediali connesso ad un rispettivo elaboratore elettronico (200) da parte sia del primo che del detto secondo utente; il detto metodo comprendendo un primo passo di attivazione preventiva di una sessione di comunicazione in chiaro tra detto primo e detto secondo utente attraverso un software per l'effettuazione di chiamate (500) nella quale il detto dispositivo (100) opera in una prima configurazione di trasmissione in chiaro, e un secondo passo di instaurazione di una comunicazione crittografata, nella quale il detto dispositivo (100) opera in una seconda configurazione di ricetrasmissione cifrata per mezzo di uno stadio o motore crittografico (120);
   detto metodo comprendendo un passo in cui il detto dispositivo (100) causa l'apertura di una sessione per trasferimento dati crittografati tra gli elaboratori elettronici (200) del detto primo utente e detto secondo utente distinta dalla sessione di comunicazione in chiaro utilizzata dal detto software per l'effettuazione di chiamate, ed in cui un flusso dati almeno audio ricetrasmesso tra i due utenti durante la loro comunicazione è selettivamente commutato tra detta sessione di comunicazione in chiaro e detta sessione di trasferimento dati crittografati sulla base di un criterio predefinito.
2. Metodo secondo la rivendicazione 1, in cui la detta sessione di comunicazione di dati in chiaro utilizzata dal detto software per l'effettuazione di chiamate (500) è mantenuta aperta durante la detta sessione di trasferimento di dati crittografati.
3. Metodo secondo la rivendicazione 2, in cui il detto criterio predefinito comprende la trasmissione di un codice identificativo, eseguita alternativamente da uno dei due dispositivi (100) coinvolti nella detta comunicazione tra detto primo e secondo utente; la detta trasmissione del detto codice seme avvenendo mediante una sessione di comunicazione preventivamente aperta mediante il detto software per l'effettuazione di chiamate (500).
4. Metodo secondo la rivendicazione 3, in cui il detto codice seme causa la selezione di un codice di cifratura preventivamente memorizzato all'interno di una memoria (120) di entrambi Ì detti dispositivi (100); detto codice di cifratura

essendo mantenuto segreto su ognuno dei detti dispositivi (100) ed essendo utilizzato per eseguire la crittografia del detto flusso di dati audio.

5. Metodo secondo una qualsiasi delle precedenti rivendicazioni, in cui la detta sessione di trasferimento di dati crittografati causa una ricetrasmissione dei detti dati crittografati su di una rete di trasmissione dati (400) suscettibile permettere la connessione tra detto primo e detto almeno secondo utente.

6. Metodo secondo una qualsiasi delle precedenti rivendicazioni 1–5, in cui l'instaurazione della detta sessione di comunicazione in chiaro comprende un passo di collegamento i un mezzo trasduttore audio (300) su di una porta o interfaccia di ingresso/uscita (110) del detto dispositivo (100) di ricetrasmissione di flussi multimediali preventivamente all'instaurazione della detta sessione di comunicazione di trasferimento di dati crittografati, e comprende inoltre un passo di connessione del detto dispositivo (100) di ricetrasmissione di flussi media ad un elaboratore elettronico (200) attraverso una porta di comunicazione (130), la detta connessione causando la presentazione di un'interfaccia audio al detto elaboratore elettronico (200), suscettibile di selezionare il detto dispositivo (100) di ricetrasmissione di flussi media come periferica di input/output di stream multimediali ricevuti, trasmessi o direttamente elaborati dal detto elaboratore elettronico (200).

7. Dispositivo (100) di ricetrasmissione di flussi multimediali crittografati, il detto dispositivo comprendendo:
– almeno un porta o interfaccia di ingresso/uscita (110) per flussi di dati almeno di tipo audio suscettibili di essere trasmessi e/o ricevuti in chiaro da/verso mezzi trasduttori (300),
– almeno una porta o interfaccia di connessione (130) con un elaboratore elettronico (200), detta porta o interfaccia di connessione (130) essendo configurata per permettere almeno di trasmettere e/o ricevere un flusso di dati almeno audio crittografato rispettivamente da e/o verso il detto elaboratore elettronico (200);
– uno stadio o motore crittografico (120), elettricamente connesso a detta porta o interfaccia di ingresso uscita (110) e a detta porta o interfaccia di connessione (130), e configurato per fornire e rispettivamente ricevere a/da detta porta o interfaccia di connessione (130) un flusso dati crittografato contenente almeno dati di tipo audio;
ed in cui il detto dispositivo (100) è configurato per presentare al detto elaboratore elettronico (200) un'interfaccia di ricetrasmissione di dati almeno audio; il detto dispositivo (100) inviando al detto elaboratore elettronico (200), secondo un criterio predeterminato, un comando per la commutazione della ricetrasmissione del detto flusso dati almeno audio ricetrasmesso da/verso detta almeno una porta o interfaccia di ingresso/uscita (110).

8. Dispositivo secondo la rivendicazione 7, configurato per permettere la trasmissione del detto flusso dati audio e/o video attraverso la detta interfaccia di ricetrasmissione di dati audio e/o video in chiaro verso un software di comunicazione (500) preesistente, preferibilmente di tipo. VoIP, suscettibile di interconnettere in una comunicazione almeno un primo utente con un secondo utente; detto dispositivo essendo configurato per ricevere un comando di commutazione verso una sessione di comunicazione crittografata; detto stadio o motore crittografico (120) essendo attivato da detto comando o segnale di commutazione.

9. Dispositivo secondo una qualsiasi delle precedenti rivendicazioni 7, 8, in cui la detta interfaccia di ricetrasmissione di dati audio e/o video è un'interfaccia di tipo Audio Class.

10. Dispositivo secondo la rivendicazione 7 o la rivendicazione 9 allorché dipendente dalla rivendicazione 8, in cui il detto stadio o motore crittografico (120) esegue la crittografia del detto flusso di dati audio e/o video con una chiave utilizzata una sola volta, selezionata sulla base di un segnale di codifica di seme condiviso con un secondo utente del medesimo dispositivo (100) e generata a partire dal un mutuo scambio di dati specifici tra il detto dispositivo (100) ed un altro dispositivo (100) coinvolto nella comunicazione.

11. Dispositivo secondo le rivendicazioni 8 e 10 in cui i detti dati specifici comprendono almeno un codice di identificazione (ID) scambiato con un altro dispositivo (100) prima dell'instaurazione della detta sessione di comunicazione crittografata, in cui lo scambio del detto codice di identificazione (ID) avviene su di una sessione preventivamente instaurata da software di comunicazione (500), ed in cui il detto dispositivo (100) è configurato per trasmettere una richiesta di apertura della detta sessione crittografata per la ricetrasmissione ciati a pacchetto verso un altro elaboratore elettronico (200), detti dati a pacchetto comprendendo il detto flusso dati crittografato scambiato tra detto dispositivo (100) e detto elaboratore elettronico (200) attraverso la detta porta o interfaccia di comunicazione (130).

12. Dispositivo secondo la rivendicazione 11, in cui la detta sessione di ricetrasmissione di dati a pacchetto è una sessione basata su di un protocollo di comunicazione di tipo UDP.

13. Dispositivo secondo la rivendicazione 11, configurato per causare il mantenimento dell'apertura di una sessione di comunicazione preventivamente aperta mediante il detto software per la comunicazione (500) durante la trasmissione del detto flusso dati crittografato su detta sessione crittografata per la ricetrasmissione di dati a pacchetto.

14. Dispositivo secondo la rivendicazione 13, configurato per causare la trasmissione di un segnale fittizio verso detto software per la comunicazione (500).

15. Dispositivo secondo la rivendicazione 14, in cui il detto segnale fittizio è un rumore bianco e/o detto codice seme.

16. Dispositivo secondo una qualsiasi delle precedenti rivendicazioni 7-15, comprendente uno stadio di codifica audio (150), avente un ingresso alimentato con un flusso di dati numerico comprendente almeno un flusso di dati audio

(101) ricevuto da mezzi trasduttori audio (300) elettricamente connessi alla detta porta di input/output (110); detto stadio di codifica audio (150) comprendendo mezzi di codifica e/o decodifica e/o compressione/decompressione audio specificatamente configurati per eseguire un'elaborazione numerica dei detti dati basata sulla codifica del parlato.

17. Dispositivo secondo la rivendicazione 16, in cui i detti mezzi di codifica sono vocoder del tipo o derivati del Code-Excited Linear Predictor, Mixed-Excitation Linear Prediction o Algebraic Code-Excited Linear Prediction.

18. Dispositivo secondo una qualsiasi delle rivendicazioni 16 o 17, comprendente inoltre uno stadio di conversione analogico/digitale (140) ricevente avente un ingresso alimentato dalla detta porta o interfaccia di input/output (110) e un'uscita alimentante il detto ingresso del detto stadio di codifica audio (150) con il detto flusso dati numerico comprendente una trasformazione nel dominio digitale del detto stream audio.

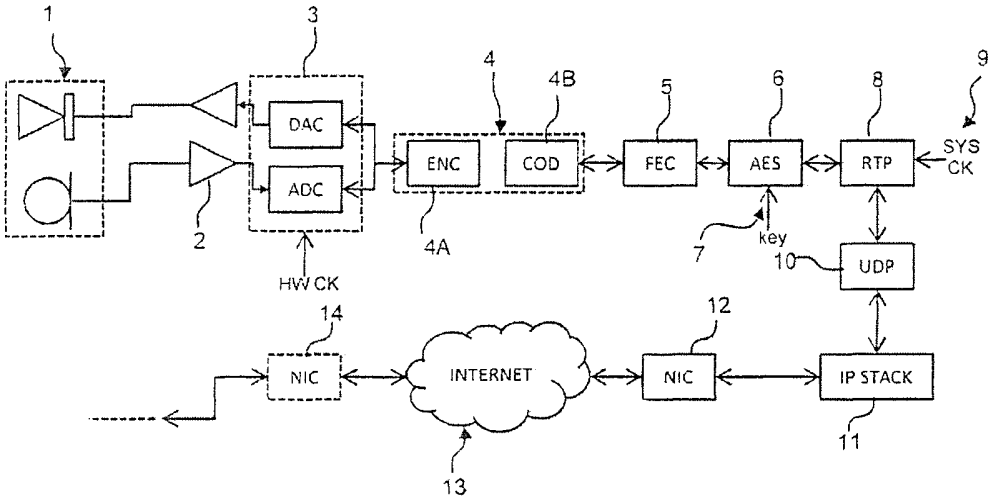

1
3
4
4B
5
6
8
9
DAC
ADC
ENC
COD
FEC
AES
RTP
SYS CK
2
4A
key
7
10
UDP
HW CK
14
12
NIC
INTERNET
NIC
IP STACK
11
13

Fig.1

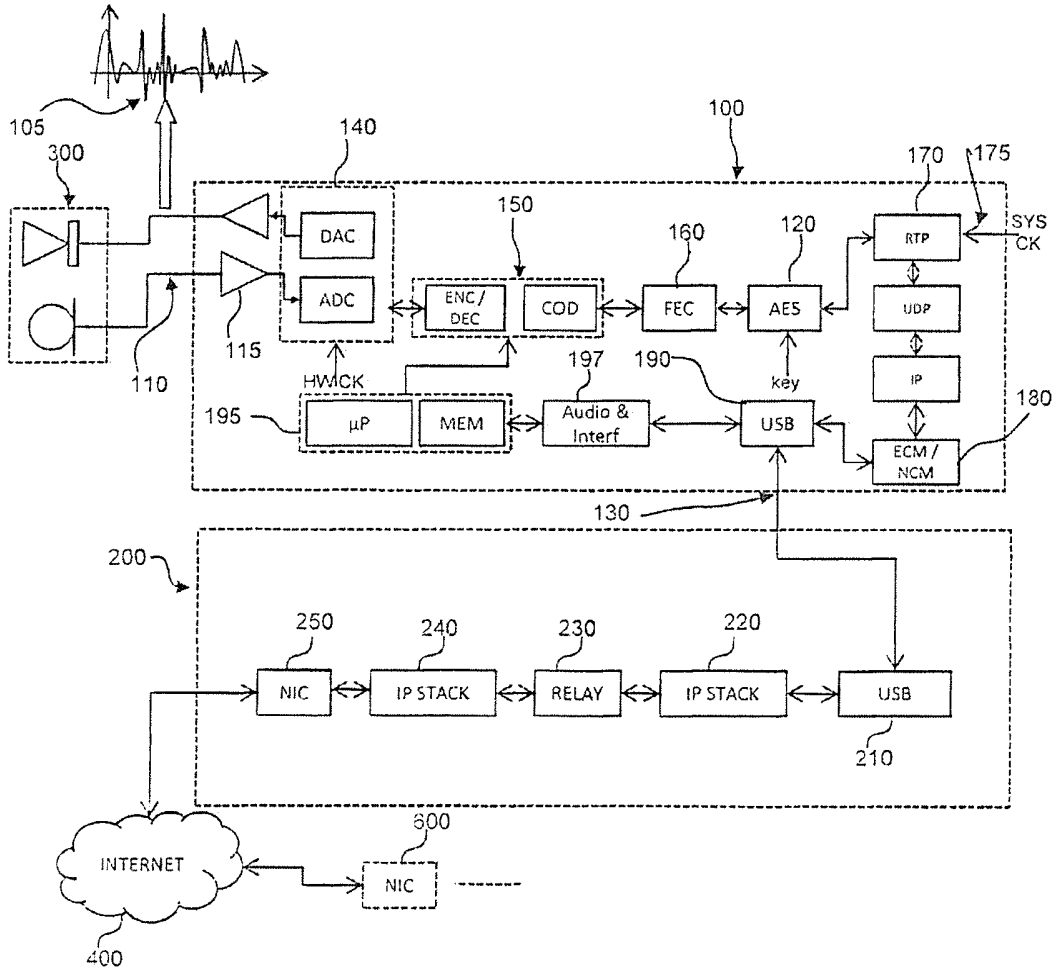

105
300
140
100
170
175
150
160
120
DAC
ADC
ENC / DEC
COD
FEC
AES
RTP
SYS CK
UDP
IP
115
110
HW CK
197
190
key
195
µP
MEM
Audio & Interf
USB
ECM / NCM
180
130
200
250
240
230
220
NIC
IP STACK
RELAY
IP STACK
USB
210
600
INTERNET
NIC
400

Fig.2

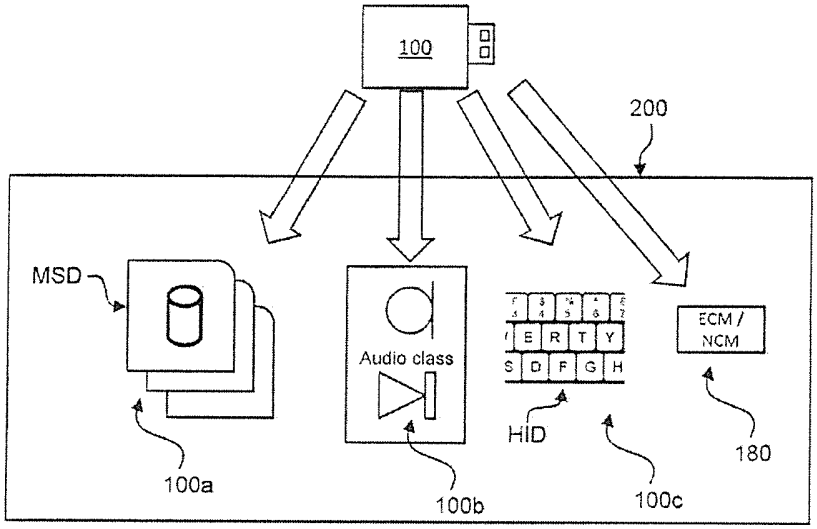

100
200
MSD
Audio class
E R T Y
S D F G H
ECM / NCM
HID
180
100a
100b
100c

Fig.3

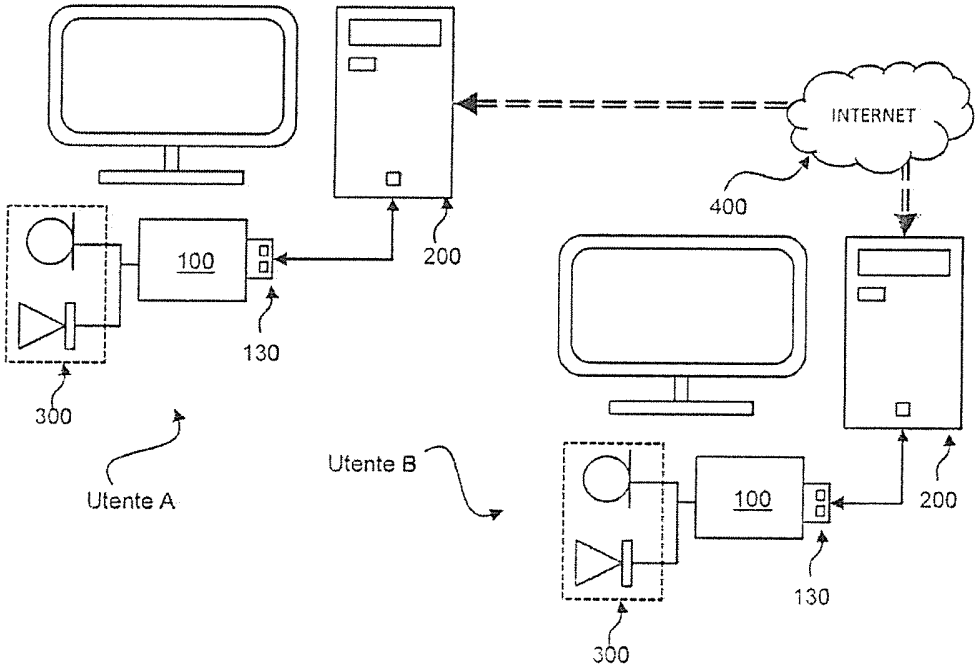

INTERNET
400
100
200
130
300
Utente A
Utente B
100
200
130
300

Fig.4

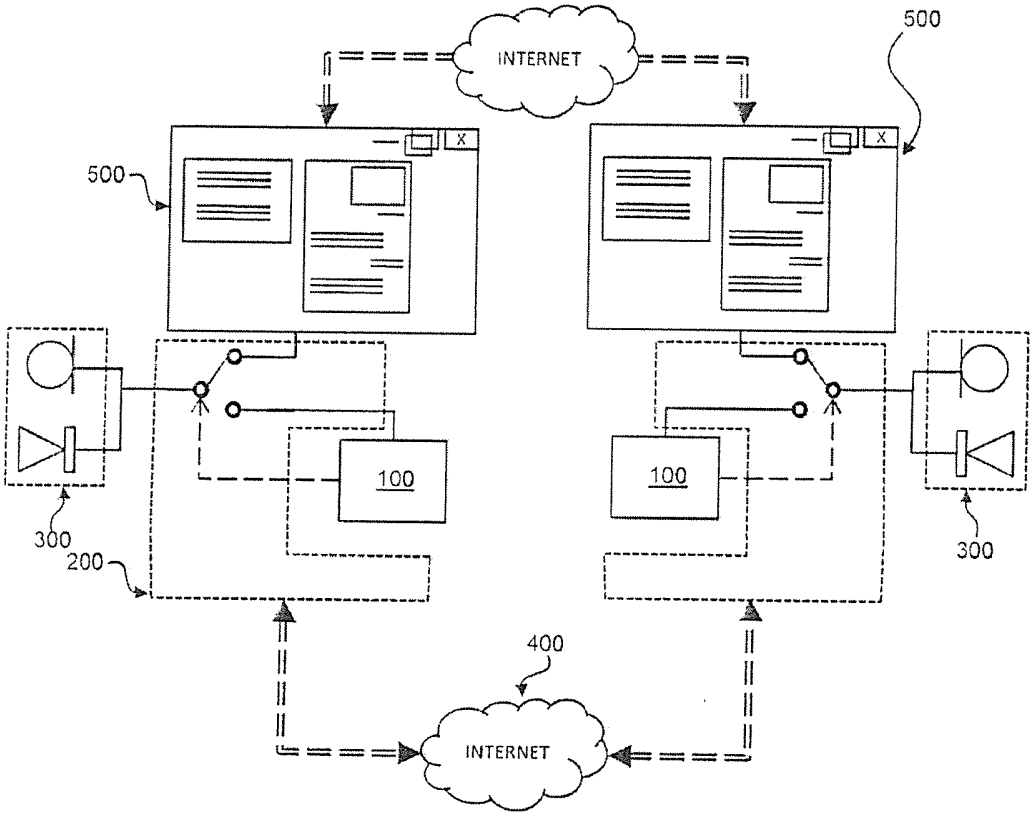

INTERNET
500
500
100
100
300
200
300
400
INTERNET

Fig.5

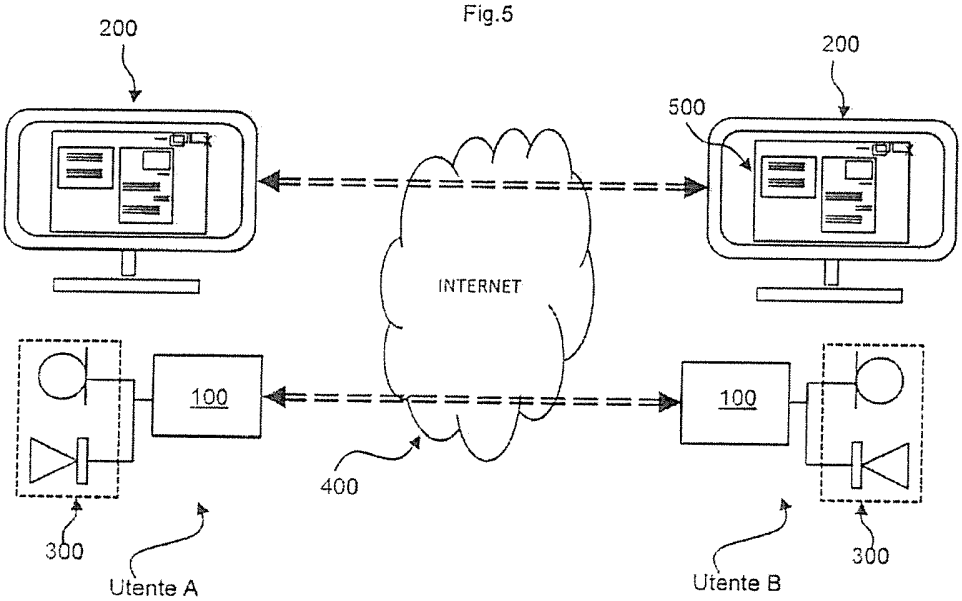

200
200
500
INTERNET
100
100
400
300
300
Utente A
Utente B

Fig.6

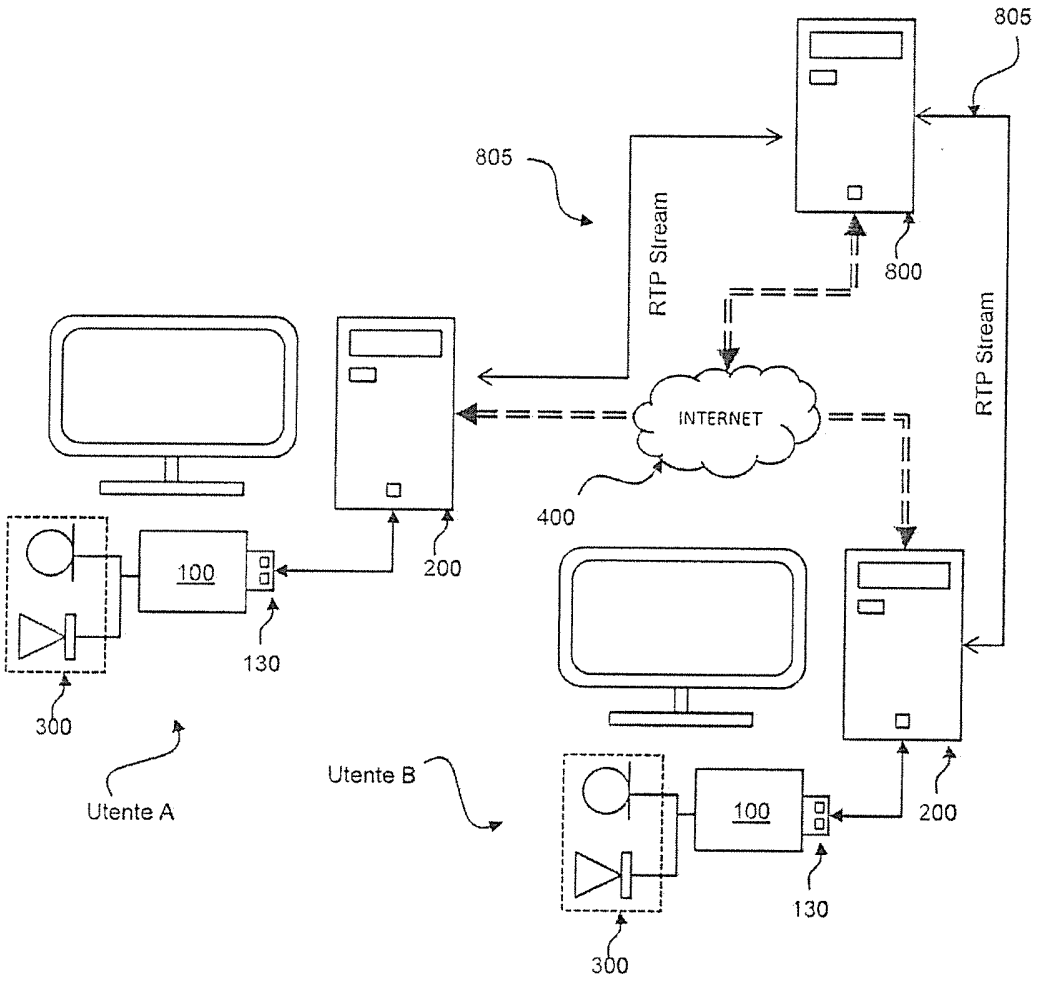

805
805
RTP Stream
800
RTP Stream
INTERNET
400
200
100
130
300
Utente A
Utente B
100
200
130
300

Fig.7