MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA DI INVENZIONE NUMERO	**102021000007808**
Data Deposito	**30/03/2021**
Data Pubblicazione	**30/09/2022**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	N	21	4363

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	N	21	4367

Titolo

DISPOSITIVO E SISTEMA PER LA TRASMISSIONE PROTETTA DI UN SEGNALE VIDEO

UPD007_IT

Descrizione dell'invenzione industriale dal titolo:

"DISPOSITIVO E SISTEMA PER LA TRASMISSIONE PROTETTA DI UN SEGNALE VIDEO"

DESCRIZIONE

Campo dell'invenzione

La presente invenzione riguarda in generale il settore della sicurezza informatica. In particolare, la presente invenzione riguarda un dispositivo per la trasmissione protetta di un segnale video. Secondo un ulteriore aspetto la presente invenzione riguarda un sistema per la trasmissione protetta di un segnale video.

Descrizione dell'arte nota

Oggigiorno la sicurezza informatica ricopre un ruolo importante nella trasmissione e condivisione di dati.

Come noto, numerosi sforzi sono stati compiuti al fine di sviluppare dispositivi e/o algoritmi di protezione per cifrare in modo efficace il contenuto di segnali video.

A titolo di esempio, la domanda di brevetto US20090060182 A1 descrive un dispositivo esterno utilizzato come memoria per chiavi crittografiche.

La domanda di brevetto US20120173877A1 descrive una architettura hardware adatta a stabilire una root-of-trust, tra un dispositivo client ed un dispositivo server, che permette di creare un canale di trasmissione di contenuti video protetti.

Numerosi studi sono inoltre stati effettuati su algoritmi di cifratura, per esempio, l'articolo "Fast and Secure Real-Time Video Encryption," 2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing di C. N. Raju, G. Umadevi, K. Srinathan

and C. V. Jawahar propone un algoritmo per la cifratura di video in tempo reale utilizzando i coefficienti della trasformata discreta del coseno ("*Discrete Cosine Transform*", DCT). L'articolo "SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission," 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), Seoul, 2007, pp. 60-65 di E. Choo, J. Lee, H. Lee and G. Nam, propone uno schema di cifratura veloce che garantisce la sicurezza di una trasmissione di un video senza compromettere la qualità del video stesso. Tale schema di cifratura, denominato SRMT (Secure Real-time Media Transmission), è basato su due trasposizioni di blocchi ed una operazione XOR.

La Richiedente ha notato che i dispositivi e/o gli algoritmi di protezione noti non permettono di ottenere una protezione adeguata da attacchi informatici che colpiscono la trasmissione di segnali video.

In particolare, la Richiedente ha notato che i dispositivi e/o algoritmi di protezione noti sono vulnerabili ad attacchi informatici del tipo *Man in the Middle*, MITM.

Breve descrizione dell'invenzione

La Richiedente ha percepito il bisogno di fornire un dispositivo ed un sistema per la trasmissione protetta di un segnale video che superino i suddetti problemi.

In particolare, scopo della presente invenzione è fornire un dispositivo ed un sistema adatti a proteggere la trasmissione di un segnale video in caso di un attacco informatico del tipo M*an in the Middle*.

Secondo un primo aspetto la presente invenzione fornisce un sistema per la trasmissione protetta di un segnale video comprendente:

- un elaboratore;

- un dispositivo di visualizzazione;
- un canale di trasmissione video;

in cui detto canale di trasmissione video è collegato a:

- un encoder configurato per:
  - ricevere in input un segnale video generato da detto elaboratore;
  - criptare detto segnale video ottenendo un segnale video criptato; e
  - trasmettere, per mezzo di detto canale di trasmissione video, detto segnale video criptato ad un decoder;
- detto decoder essendo configurato per:
  - ricevere detto segnale video criptato da detto canale di trasmissione video;
  - decriptare detto segnale video criptato, ottenendo detto segnale video;
  - trasmettere detto segnale video a detto dispositivo di visualizzazione;

in cui detto canale di trasmissione video è un canale di collegamento fisico;

in cui detto encoder e detto decoder sono collegati fisicamente in corrispondenza di una rispettiva estremità di detto canale di trasmissione video.

Preferibilmente, detto encoder e detto decoder sono configurati per eseguire una criptazione simmetrica del segnale video generato dall'elaboratore.

Preferibilmente, detto encoder e detto decoder sono configurati per eseguire una criptazione asimmetrica del segnale video generato dall'elaboratore.

Preferibilmente, detto encoder è collegato fisicamente all'elaboratore e detto decoder è collegato fisicamente all'elaboratore.

Secondo un ulteriore aspetto la presente invenzione fornisce un

encoder comprendente:

- un corpo scatolare dotato di un primo connettore video ed un secondo connettore video;
- una unità di elaborazione, alloggiata in detto corpo scatolare, configurata per:
  - ricevere in input un segnale video da detto primo connettore video;
  - criptare detto segnale video ottenendo un segnale video criptato;
  - inviare detto segnale video criptato a detto secondo connettore video;

in cui detto primo connettore video è un connettore maschio adatto ad essere inserito, in modo removibile, in una rispettiva uscita video di un elaboratore;

in cui detto secondo connettore video è un connettore adatto ad impegnare, in modo removibile, un cavo di trasmissione video.

Preferibilmente, detto primo connettore video è un connettore maschio del tipo HDMI o VGA o DVI o USB-c.

Preferibilmente, detto secondo connettore video è un connettore femmina del tipo HDMI o VGA o DVI o USB-c.

Preferibilmente, detto encoder comprende inoltre una memoria fisica in cui è memorizzata una chiave crittografica.

Secondo un ulteriore aspetto la presente invenzione fornisce un decoder comprendente:

- un corpo scatolare dotato di un primo connettore video ed un secondo connettore video;
- una unità di elaborazione alloggiata nel corpo scatolare;

in cui detto elaboratore è configurato per:

- ricevere in input un segnale video criptato da detto primo connettore video;
- decriptare detto segnale video criptato ottenendo un segnale video;

- inviare detto segnale video a detto secondo connettore video;

in cui detto primo connettore video è un connettore adatto ad impegnare, in modo removibile, un cavo di trasmissione video;

in cui detto secondo connettore video è un connettore maschio adatto ad essere inserito, in modo removibile, in una rispettiva entrata video di un dispositivo di visualizzazione.

Preferibilmente, detto primo connettore video è un connettore femmina del tipo HDMI o VGA o DVI o USB-c.

Preferibilmente, detto secondo connettore video è un connettore maschio del tipo HDMI o VGA o DVI o USB-c.

Preferibilmente, detto decoder comprende una memoria fisica; in cui detta memoria fisica contiene una chiave crittografica

Breve descrizione dei disegni

L'invenzione apparirà maggiormente chiara dalla descrizione dettagliata che segue, fornita a puro titolo esemplificativo e non limitativo e da leggersi con riferimento ai disegni allegati, in cui:

- la Figura 1 mostra in generale un attacco informatico del tipo *Man in the Middle*;
- la Figura 2 mostra un attacco del tipo *Man in the middle* in cui un dispositivo hardware è collegato tra un calcolatore ed un monitor;
- la Figura 3 è uno schema esemplificativo di un sistema per la trasmissione protetta di un segnale video secondo la presente invenzione;
- la Figura 4 è uno schema a blocchi di un dispositivo per la trasmissione protetta di un segnale video secondo la presente invenzione;
- la Figura 5 è uno schema a blocchi di un encoder secondo la

presente invenzione;

- la Figura 6 è uno schema a blocchi di un decoder secondo la presente invenzione;
- la Figura 7 mostra il principio di funzionamento di una coppia di dispositivi per la trasmissione protetta di un segnale video secondo la presente invenzione.

Nel seguito, facendo riferimento alle Figure di cui sopra, elementi e/o oggetti che svolgono la medesima funzione saranno indicati mediante lo stesso numero di riferimento.

Descrizione dettagliata delle forme di realizzazione preferite

Secondo la presente invenzione è fornito un sistema per la trasmissione protetta di un segnale video. Tale sistema è indicato nel seguito con il numero di riferimento 100.

In particolare, il sistema 100 è adatto a proteggere la trasmissione di un segnale video nel caso di un attacco informatico del tipo *Man in the Middle*. Tale tipo di attacco informatico è denominato nel seguito *Man in the Video,* MITV.

Facendo riferimento alle Figure 1 e 2, un attacco informatico del tipo *Man in the Video*, MITV consiste nell'intercettare un segnale video trasmesso da un elaboratore 10 e diretto ad un dispositivo di riproduzione video 20.

Per esempio, l'elaboratore 10 può essere un personal computer ed il dispositivo di riproduzione video 20 può essere un monitor esterno o un proiettore. Come noto i monitor esterni sono utilizzati come interfacce per interagire con dispositivi informatici fornendo un feedback visivo delle operazioni svolte. Un attacco del tipo *Man in the Video,* MITV consiste nell'intercettare il segnale video in uscita dal laptop o dal computer, modificarlo e mostrarlo all'utente che non ha modo di accorgersi di vedere delle immagini rielaborate e modificate.

In particolare, facendo riferimento ad un attacco MITV come mostrato in Figura 1 e 2, l'attaccante può prendere il controllo del canale video 30 tra l'elaboratore 10 ed il monitor 20. Quando l'utente utilizza l'elaboratore 10, per esempio, per controllare la sua casella di posta elettronica, accedere al proprio internet banking o altre operazioni di uso comune, i suoi input sono elaborati dall'elaboratore 10 che genera un flusso video che viene inviato al monitor 20 per mezzo del canale video 30.

La Richiedente osserva che il canale video 30 è l'unico componente con cui l'attaccante deve interagire al fine di effettuare un attacco informatico MITV. In particolare, l'attaccante non ha bisogno di interagire direttamente con il protocollo di comunicazione, ha solo bisogno di adattare il suo hardware 31 con connettori e/o driver di input/output specifici.

Per esempio, nell'attacco MITV di Figura 2, l'attaccante intercetta il canale video 30, per esempio, utilizzando un hardware 31 in grado di intercettare e modificare un flusso di immagini contenuto in un segnale video. Una volta intercettato il flusso di immagini, l'attaccante può modificarlo in modo da indirizzare l'utente a sua insaputa, per esempio, su siti web di phishing convincendolo a fornire informazioni personali, dati finanziari o codici di accesso, semplicemente mostrando una URL di un sito web ritenuto affidabile per mezzo dell'hardware 31.

Facendo riferimento a Figura 3, il sistema 100 comprende un primo dispositivo 110, nel seguito indicato come "encoder", ed un secondo dispositivo 120, nel seguito indicato come "decoder".

L'encoder 110 ed il decoder 120 sono collegati tra loro per mezzo di un canale di trasmissione video 30. Per esempio, il canale di trasmissione video 30 è un cavo HDMI o VGA o DVI.

L'encoder 110 è collegato all'elaboratore 10 ed il decoder 120 è collegato al dispositivo di visualizzazione 20. L'encoder 110 è configurato per eseguire una crittografia simmetrica o una

crittografia asimmetrica del segnale video Sv_in generato dall'elaboratore 10; il decoder 120 è configurato per decriptare tale segnale video criptato Sv_c e renderlo disponibile al dispositivo di visualizzazione 20.

Considerando la crittografia simmetrica, l'encoder 110 è configurato per utilizzare una chiave crittografica per criptare il segnale video Sv_in; il decoder 120 utilizza la medesima chiave crittografica per decriptare il segnale video criptato Sv_c.

In altre parole, il decoder 110 e l'encoder 120 condividono una stessa chiave crittografica. Tale chiave crittografica è utilizzata per criptare/decriptare il segnale video generato dall'elaboratore 10 e mostrato dal dispositivo di visualizzazione 20.

Considerando la crittografia asimmetrica, l'encoder 110 ed il decoder 120 sono configurati per criptare/decriptare il segnale video per mezzo di una coppia di chiavi crittografiche complementari. In particolare, una prima chiave è utilizzata dall'encoder 110 per criptare il segnale video; una seconda chiave, complementare alla prima chiave, è utilizzata dal decoder 120 per decriptare il segnale video.

Gli algoritmi di crittografia simmetrica e di crittografia asimmetrica sono noti e non verranno descritti nel dettaglio nel seguito.

Preferibilmente, l'encoder 110 ed il decoder 120 utilizzano un algoritmo di crittografia simmetrica. Per esempio, l'encoder 110 ed il decoder 120 utilizzano un algoritmo AES256.

Secondo la presente invenzione, come mostrato in Figura 4 e 5, l'encoder 110 comprende un corpo scatolare 111. Il corpo scatolare 111 presenta un primo connettore video 112 ed un secondo connettore video 113.

Preferibilmente, il primo connettore video 112 ed il secondo connettore video 113 sono disposti su superfici opposte del corpo scatolare 111.

Preferibilmente, il primo connettore video 112 è un connettore maschio. Per esempio, il primo connettore video 112 è un connettore maschio a scelta tra: un connettore HDMI, un connettore USB-c, un connettore VGA o un connettore DVI.

Preferibilmente, il secondo connettore video 113 è un connettore femmina. Per esempio, il secondo connettore video 113 è un connettore femmina a scelta tra: un connettore HDMI, un connettore USB-c, un connettore VGA o un connettore DVI.

L'encoder 110 comprende una unità di elaborazione 115. L'unità di elaborazione 115 è alloggiata nel corpo scatolare 111. L'unità di elaborazione 115 è configurata per:

- ricevere in input un segnale video Sv_in da detto primo connettore video;
- criptare detto segnale video Sv_in ottenendo un segnale video criptato Sv_c;
- inviare detto segnale video criptato Sv_c a detto secondo connettore video.

Per esempio, l'unità di elaborazione 115 comprende un System-on-a-Chip (SoC) 118. In particolare, il SoC 118 è un circuito integrato comprendente una central processing unit (CPU) e una memoria di calcolo (RAM). Il SoC 118 è configurato per:

- ricevere un segnale video Sv_in dal primo connettore video 112 (input)
- criptare tale segnale video Sv_in ottenendo un segnale video criptato Sv_c (preferibilmente, per mezzo di un algoritmo di criptazione simmetrico);
- inviare tale segnale video criptato Sv_c al secondo connettore video 113 (output).

Il SoC 118 è collegato ad una memoria fisica 119. La memoria fisica 119 contiene preferibilmente un sistema operativo, funzioni utilizzate per la cifratura del video e la chiave crittografica.

Preferibilmente, la memoria fisica 119 è una memoria Flash. Per esempio, una scheda microSD.

L'encoder 110 comprende una unità di alimentazione 116. L'unità di alimentazione 116 alimenta il primo connettore video 112 il secondo connettore video 113 e l'unità di elaborazione 115.

Preferibilmente, l'unità di alimentazione 116 è implementata come una porta USB o una porta micro-USB o una porta USB-C. Alternativamente, l'unità di alimentazione 116 è implementata come una porta Lightning o una porta Thunderbolt.

Preferibilmente, la prima chiave è memorizzata nella memoria fisica 119.

Preferibilmente, l'algoritmo crittografico, simmetrico o asimmetrico, è disponibile nel pacchetto crittografico associato al sistema operativo del SoC 118.

Alternativamente, l'algoritmo crittografico simmetrico o asimmetrico è memorizzato nella memoria fisica 119.

Facendo riferimento alle Figure 4 e 6, il decoder 120 comprende un corpo scatolare 121. Alternativamente, il decoder 120 può essere alloggiato all'interno del dispositivo di visualizzazione 20.

Il corpo scatolare 121 presenta un primo connettore video 122 ed un secondo connettore video 123. Preferibilmente, il primo connettore video 122 ed il secondo connettore video 123 sono disposti su superfici opposte del corpo scatolare 121.

Preferibilmente, il primo connettore video 122 del decoder 120 è un connettore femmina. Per esempio, il primo connettore video 122 del decoder 120 è un connettore femmina a scelta tra: un connettore HDMI, un connettore USB-c, un connettore VGA o un connettore DVI.

Preferibilmente, il secondo connettore video 123 del decoder 120 è un connettore maschio. Per esempio, il secondo connettore video 123 del decoder 120 è un connettore maschio a scelta tra: un connettore HDMI, un connettore USB-c, un connettore VGA o un connettore DVI.

Il decoder 120 comprende una unità di elaborazione 125. L'unità di elaborazione 125 è alloggiata nel corpo scatolare 121 del decoder 120. L'unità di elaborazione 125 è configurata per:

- ricevere in input il segnale video criptato Sv_c da detto primo connettore video;
- decriptare detto segnale video criptato Sv_c ottenendo il segnale video Sv_in;
- inviare detto segnale video Sv_in a detto secondo connettore video.

Per esempio, l'unità di elaborazione 125 comprende un System-on-a-Chip (SoC) 128. Il SoC 128 è sostanzialmente analogo al SoC 118 dell'encoder 110. Il SoC 128 del decoder 120 è configurato per:

- ricevere il segnale video criptato Sv_c dal primo connettore video 122 (input)
- decriptare tale segnale video criptato Sv_c ottenendo il segnale video decriptato (segnale video Sv_in), preferibilmente, per mezzo di un algoritmo di decriptazione simmetrico, ossia, decripta il segnale video criptato utilizzando la stessa chiave utilizzata dall'encoder 110);
- inviare tale segnale video decriptato al secondo connettore video 123 (output).

Il SoC 128 del decoder 120 è collegato ad una memoria fisica 129. La memoria fisica 129 del decoder 120 contiene il sistema operativo, le funzioni utilizzate per la cifratura del video e la chiave crittografica.

Preferibilmente, la memoria fisica 129 del decoder 120 è una memoria flash, per esempio, una scheda microSD.

Il decoder 120 comprende una unità di alimentazione 126. L'unità di alimentazione 126 alimenta sia il primo connettore video 122 sia il secondo connettore video 123 sia l'unità di elaborazione 125 del decoder 120.

Preferibilmente, l'unità di alimentazione 126 del decoder 120 è implementata come una porta USB o una porta micro-USB o una porta USB-C. Alternativamente, l'unità di alimentazione 126 è implementata come una porta Lightning o una porta Thunderbolt.

Preferibilmente, la seconda chiave è memorizzata nella memoria fisica 129 del decoder 120.

Preferibilmente, l'algoritmo crittografico simmetrico o asimmetrico è disponibile nel pacchetto crittografico associato al sistema operativo del SoC 128. Alternativamente, l'algoritmo crittografico simmetrico o asimmetrico è memorizzato nella memoria fisica 129 del decoder 120.

Facendo riferimento a Figura 7, nel seguito è descritto quali sono le fasi eseguite su un segnale video generato da un elaboratore 10 prima di essere mostrato su un dispositivo di visualizzazione.

Secondo la presente invenzione un segnale video viene codificato. In particolare, una uscita video dell'elaboratore 10 è collegata fisicamente all'encoder 110, per esempio, per mezzo del connettore maschio 112 dell'encoder 110. L'encoder 110 riceve il segnale video generato dell'elaboratore 10 tramite il connettore maschio 112, lo cripta utilizzando preferibilmente un algoritmo di criptazione simmetrico e trasmette il segnale video criptato lungo il canale di trasmissione video 30 tramite il secondo connettore 113.

Il segnale video criptato viene ricevuto dal decoder 120. In particolare, il canale di trasmissione video 30 è collegato con il primo connettore 122 del decoder 120.

Per esempio, il canale di trasmissione video 30 è un cavo HDMI in cui una prima estremità è inserita nel connettore femmina 113 dell'encoder 110; la seconda estremità del cavo HDMI è inserita nel connettore femmina 122 del decoder 120.

Il segnale video criptato, una volta ricevuto dal decoder 120, viene decodificato ed inviato, per mezzo del secondo connettore 123,

al dispositivo di visualizzazione 20. Per esempio, considerando un monitor esterno, il secondo connettore 123 del decoder 120 è un connettore maschio adatto ad essere inserito in una entrata video del monitor esterno.

La presente invenzione comporta importanti vantaggi.

Il sistema 100 per la trasmissione protetta di un segnale video secondo la presente invenzione garantisce una tutela da attacchi informatici del tipo Man in the Video, MITV.

L'encoder 110 ed il decoder 120 sono dispositivi di semplice utilizzo per l'utente. Infatti, è sufficiente collegarli in corrispondenza di una rispettiva estremità di un canale di trasmissione 30 per ottenere una protezione da attacchi del tipo MITV.

Vantaggiosamente, è possibile integrare il decoder 120 in un dispositivo di visualizzazione 20.

Vantaggiosamente, l'encoder 110 ed il decoder 120 sono retro-compatibili con tutti i computer che utilizzano connettori video del tipo HDMI, VGA, DVI, USB-C o comunque altri connettori video attualmente disponibili in commercio. La Richiedente osserva che, vantaggiosamente, i produttori di computer e monitor non devono modificare la loro catena di produzione per integrare l'encoder 110 ed il decoder 120 in quanto sono componenti plug-and-play.

RIVENDICAZIONI

1. Un sistema (100) per la trasmissione protetta di un segnale video (Sv_in) comprendente:
   - un elaboratore (10);
   - un dispositivo di visualizzazione (20);
   - un canale di trasmissione video (30);

   in cui detto canale di trasmissione video (30) è collegato a:
   - un encoder (110) configurato per:
     - ricevere in input un segnale video generato da detto elaboratore (10);
     - criptare detto segnale video (SV_in) ottenendo un segnale video criptato (Sv_c); e
     - trasmettere, per mezzo di detto canale di trasmissione video (30), detto segnale video criptato (Sv_c) ad un decoder (120);
   - detto decoder (120) essendo configurato per:
     - ricevere detto segnale video criptato (Sv_c) da detto canale di trasmissione video (30);
     - decriptare detto segnale video criptato (Sv_c), ottenendo detto segnale video (Sv_in);
     - trasmettere detto segnale video (Sv_in) a detto dispositivo di visualizzazione (20);

   in cui detto canale di trasmissione video (30) è un canale di collegamento fisico;
   in cui detto encoder (110) e detto decoder (120) sono collegati fisicamente in corrispondenza di una rispettiva estremità di detto canale di trasmissione video (30).

2. Il sistema (100) secondo la rivendicazione precedente in cui detto encoder (110) e detto decoder (120) sono configurati per eseguire una criptazione simmetrica del segnale video generato

dall'elaboratore (10).

3. Il sistema (100) secondo la rivendicazione 1 in cui detto encoder (110) e detto decoder (120) sono configurati per eseguire una criptazione asimmetrica del segnale video generato dall'elaboratore (10).

4. Il sistema (100) secondo una qualsiasi delle rivendicazioni precedenti in cui detto encoder (110) è inoltre collegato fisicamente all'elaboratore (10) e detto decoder (120) è collegato fisicamente all'elaboratore (10).

5. Un encoder (110) comprendente:
   - un corpo scatolare (111) dotato di un primo connettore video (112) ed un secondo connettore video (113);
   - una unità di elaborazione (115), alloggiata nel corpo scatolare (111), configurata per:
     - ricevere in input un segnale video (Sv_in) da detto primo connettore video (112)
     - criptare detto segnale video (Sv_in) ottenendo un segnale video criptato (Sv_c);
     - inviare detto segnale video criptato (Sv_c) a detto secondo connettore video (113);

   in cui detto primo connettore video (112) è un connettore maschio adatto ad essere inserito, in modo removibile, in una rispettiva uscita video di un elaboratore (10);
   in cui detto secondo connettore video (113) è un connettore adatto ad impegnare, in modo removibile, un cavo di trasmissione video (30).

6. L'encoder (110) secondo la rivendicazione precedente in cui detto primo connettore video (112) è un connettore maschio del tipo HDMI o VGA o DVI o USB-c.

7. L'encoder (110) secondo una qualsiasi delle rivendicazioni 5 o 6 in cui detto secondo connettore video (113) è un connettore femmina del tipo HDMI o VGA o DVI o USB-c.

8. L'encoder (110) secondo una qualsiasi delle rivendicazioni da 5 a 7 in cui detto encoder (110) comprende inoltre una memoria fisica (119) in cui è memorizzata una chiave crittografica.

9. Un decoder (120) comprendente:
   - un corpo scatolare (121) dotato di un primo connettore video (122) ed un secondo connettore video (123);
   - una unità di elaborazione (125) alloggiata nel corpo scatolare (121); in cui detto elaboratore (125) è configurato per:
     - ricevere in input un segnale video criptato (Sv_c) da detto primo connettore video (122)
     - decriptare detto segnale video criptato (Sv_c) ottenendo un segnale video (Sv_in);
     - inviare detto segnale video (Sv_in) a detto secondo connettore video (123);

   in cui detto primo connettore video (122) è un connettore adatto ad impegnare, in modo removibile, un cavo di trasmissione video (30);

   in cui detto secondo connettore video (123) è un connettore maschio adatto ad essere inserito, in modo removibile, in una rispettiva entrata video di un dispositivo di visualizzazione (20).

10. Il decoder (120) secondo la rivendicazione precedente in cui detto primo connettore video (112) è un connettore femmina del tipo HDMI o VGA o DVI o USB-c.

11. Il decoder (120) secondo una qualsiasi delle rivendicazioni 9 o 10 in cui detto secondo connettore video (123) è un connettore

maschio del tipo HDMI o VGA o DVI o USB-c.

12. Il decoder (120) secondo una qualsiasi delle rivendicazioni da 9 a 11 in cui detto decoder (120) comprende una memoria fisica (129); in cui detta memoria fisica (129) contiene una chiave crittografica.

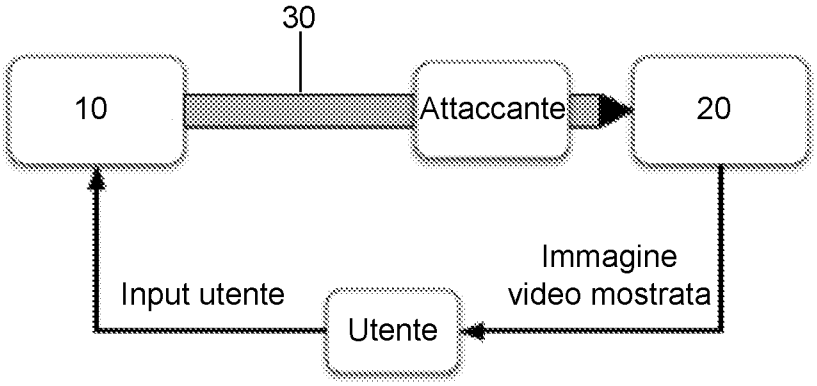
30
10
Attaccante
20
Immagine
video mostrata
Input utente
Utente

Fig. 1

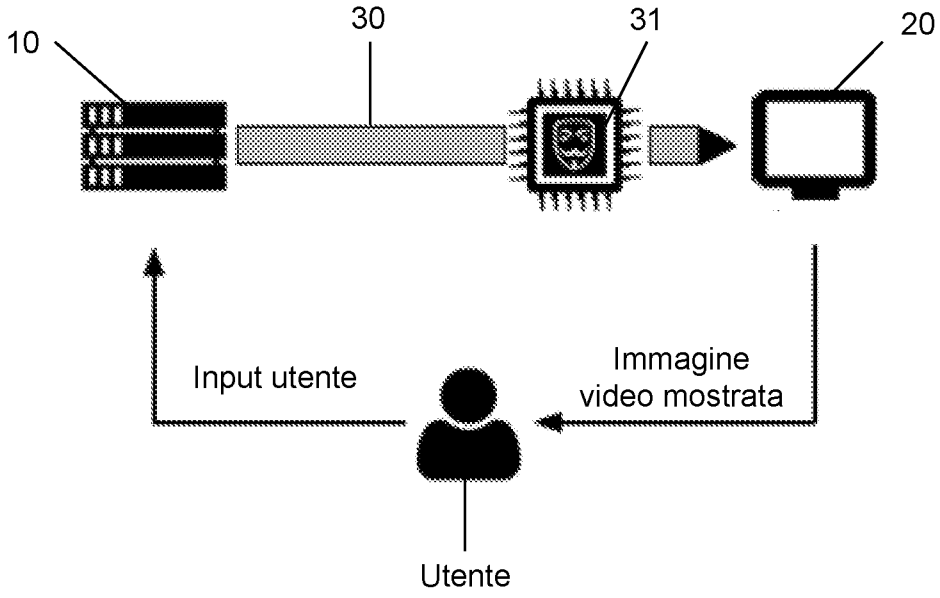
10
30
31
20
Input utente
Immagine
video mostrata
Utente

Fig. 2

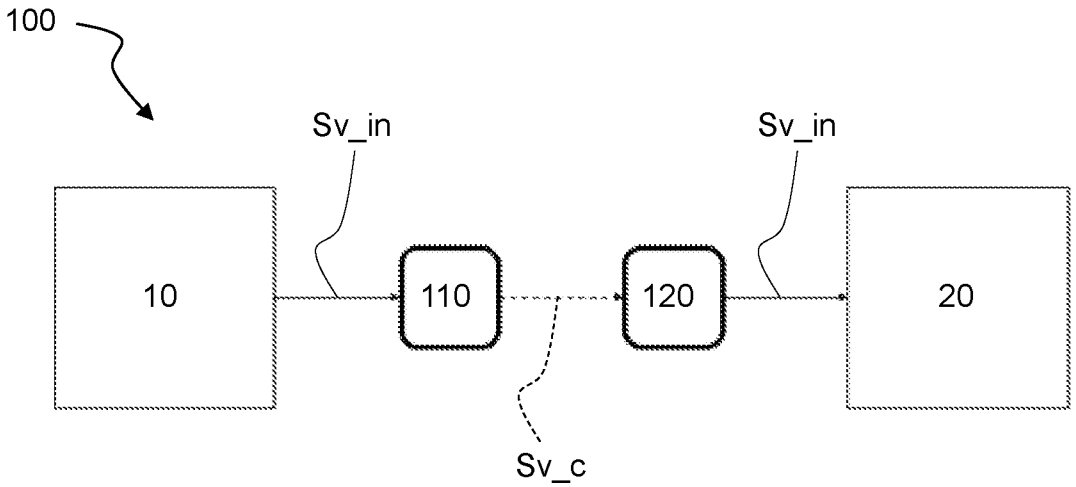
100
Sv_in
Sv_in
10
110
120
20
Sv_c

Fig. 3

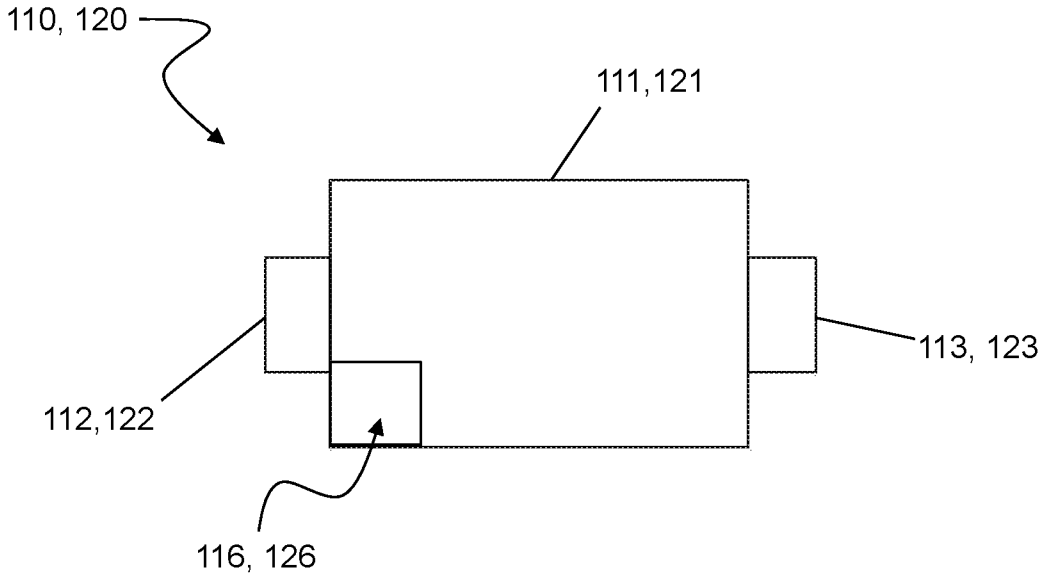
110, 120
111,121
113, 123
112,122
116, 126

Fig. 4

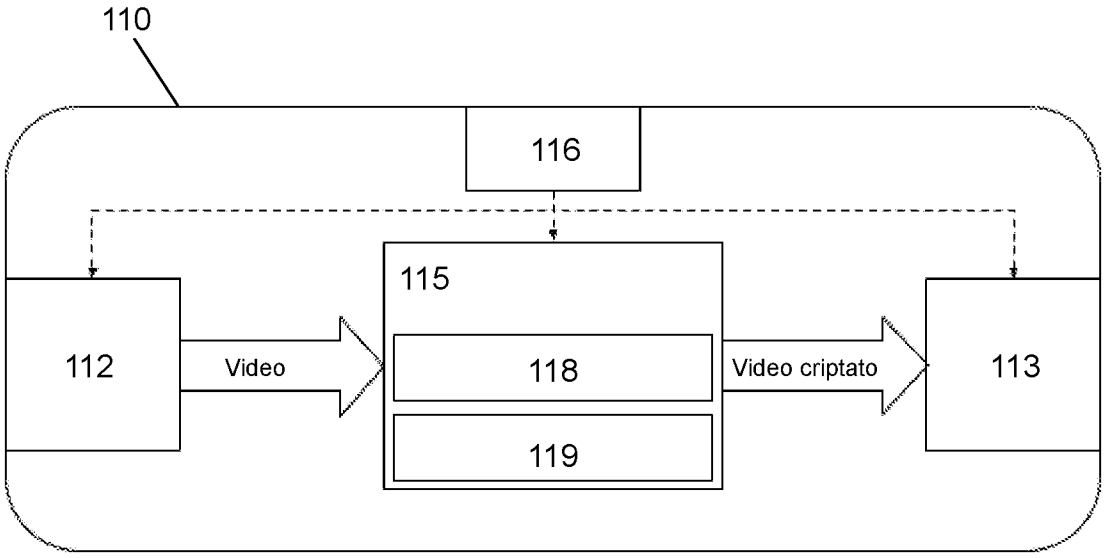
110
116
115
112
Video
118
Video criptato
113
119

Fig. 5

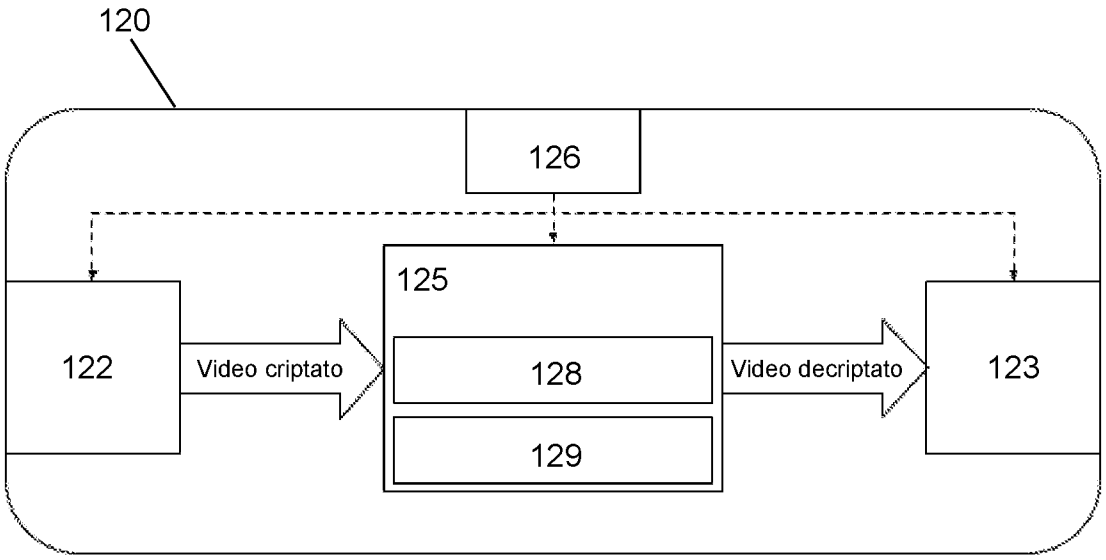
120
126
125
122
Video criptato
128
Video decriptato
123
129

Fig. 6

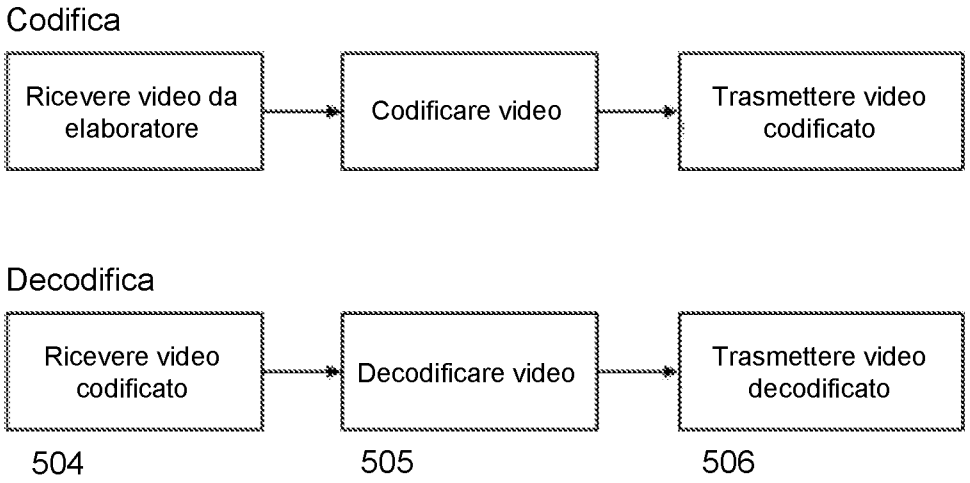
Codifica
Ricevere video da elaboratore
Codificare video
Trasmettere video codificato
Decodifica
Ricevere video codificato
Decodificare video
Trasmettere video decodificato
504
505
506

Fig. 7