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

DOMANDA NUMERO	**102008901638806**
Data Deposito	**24/06/2008**
Data Pubblicazione	**24/09/2008**

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	09	F		

Titolo

SIGILLO ELETTRONICO

DESCRIZIONE DELL'INVENZIONE INDUSTRIALE DAL TITOLO:

"SIGILLO ELETTRONICO",

a nome di GIUSEPPE FAZIO codice fiscale FZAGPP51R19F839Z, di nazionalità italiana, nato a Napoli il 19-10-1951 residente in via Vega n. 7, 00012 Guidonia Montecelio; e di DANIELE SACERDOTI codice fiscale SCDDNL59B13H501C di nazionalità italiana, nato a Roma il 13/2/1959, residente in viale Dell'Umanesimo 199, 00144 Roma. Inventore designato: GIUSEPPE FAZIO codice fiscale FZAGPP51R19F839Z, di nazionalità italiana, nato a Napoli il 19-10-1951 residente in via Vega n. 7, 00012 Guidonia Montecelio.

RIASSUNTO

Fin dall'antichità uno dei problemi più sentiti è stato quello di poter verificare la occorrenza di accessi non desiderati sia ad elementi mobili quali pacchi, documenti, container sia ad elementi fissi quali case, armadi, casseforti ecc...

Il problema era risolto applicando dei sigilli difficilmente riproducibili e che si alterassero in modo visibile al momento dell'apertura dell'elemento violato.

Le capacita di contraffazioni oggi presenti elevano la possibilità di rigenerare copie dei sigilli originali sempre più perfette rendendo non efficace il sistema di sicurezza in uso.

Introdurre sistemi innovativi a basso costo che possano proteggere molte delle svariate tipologie di elementi dalla "intrusione" è perciò di grande interesse.

Il sistema inventato ricorre alle nuove tecnologie dell'elettronica e permette di verificare in modo semplice e inequivoco se un "opportuno sigillo" disposto su di un elemento da proteggere sia stato "forzato" ed eventualmente registrare e fornire informazioni aggiuntive circa l'ora della sigillazione, il numero di volte in cui sia stata verificata la sua integrità, informazioni connesse al viaggio del bene.

Il presente trovato fornisce la descrizione di detto dispositivo.

Esso è costituito dai seguenti elementi:

1. Un "Opportuno Sigillo" costituito da elemento fisico caratterizzabile da parametri rilevabili elettronicamente che variano inequivocabilmente il proprio valore in caso di forzatura del sigillo. Un esempio qui proposto è costituito da nastro adesivo realizzato (Nastro sigillante Elettronico) con un particolare dosaggio di colle tali da garantire, una volta applicato, l'impossibilità di poter essere staccato senza alterare le caratteristiche elettriche di alcuni materiali opportunamente posizionati sul nastro o nel nastro medesimo.
2. Un apparato elettronico (d'ora in poi chiamato "Controllore di Sigillo" CS) capace di "leggere" con continuità le caratteristiche elettriche di materiali appartenenti all'"opportuno sigillo" ed in grado di comunicare con un "Sistema Terminale Esterno Sigillo Elettronico" eventualmente in modo "Contact less".
3. Il "Sistema Terminale Esterno Sigillo Elettronico" (d'ora in poi chiamato "terminale STE") è utilizzato per interagire con il

Controllore di Sigillo secondo le modalità di seguito riportate.

4. Opportuni protocolli di utilizzo e comunicazione.

DESCRIZIONE

La descrizione seguente si articola in quattro sezioni separate:

A. Nella prima si descrive il componente denominato "Opportuno Sigillo" nella situazione di cui esso sia costituito da "Nastro Sigillante Elettronico".

B. Nella seconda si descrive il sottosistema elettronico denominato "Controllore di Sigillo".

C. Nella terza si descrive il sottosistema elettronico denominato "Sistema Terminale Esterno Sigillo Elettronico".

D. Nella quarta si descrivono le procedure di utilizzo.

A- OPPORTUNO SIGILLO - NASTRO SIGILLANTE ELETTRONICO

Nella Fig. 1 è schematizzato un prototipo di Nastro Sigillante Elettronico visto dalla parte inferiore in cui sono illustrati i vari strati che lo compongono:

A. Rivestimento protettivo finale.

B. Striscia conduttiva

C. Strato isolante intermedio

D. Isolante superficie contatto

E. Strisce resistive

Nella Fig. 2 è riportata una sezione trasversale del medesimo nastro, in cui i singoli strati sono etichettati come nella Fig. 1 mentre la lettera F rappresenta il contenitore sigillato.

Immaginiamo di avere un nastro adesivo tale che la colla che lo fissi sia più robusta della struttura del nastro medesimo, questo già rende molto difficile se non impossibile rimuovere il nastro dopo un primo posizionamento senza distruggerlo.

Immaginiamo di depositare una o più strisce, conduttive (Fig. 1 e Fig. 2 E) estremamente fragili sulla parte inferiore adesiva per la cui intrinseca tipologia di deposizione risultino non esattamente prevedibili le loro caratteristiche (Esempio conduttore costituito da elementi quali una striscia di polvere di carbone). Agendo in questo modo risulta impredicibile indicare a priori il valore preciso della resistenza (e/o di altri parametri elettrici quali capacità induttanza ecc.) finale che si otterrà agli estremi della striscia così ottenuta.

Nella deposizione della colla, per ulteriore precauzione, si possono alternare dei piccoli tratti in cui la grafite della striscia conduttiva sia incollata più saldamente al nastro ad altri in cui detta colla sia più forte verso la superficie dell'elemento su cui è applicato, questa modalità di incollaggio facilita la possibilità di distruzione delle strisce nel caso di un tentativo di effrazione.

Come ulteriore precauzione è pure possibile posizionare le strisce resistive, sopra descritte, con percorsi casuali rispetto ai margini del nastro adesivo ed eventualmente più strisce sotto il medesimo nastro (Fig. 1 e Fig. 2 E).

Risulta immediato che sarà estremamente complicato, se non impossibile alterare o riposizionare il nastro senza variare le caratteristiche elettriche

della striscia conduttiva così realizzata.

Ovviamente se la superficie dell'elemento da sigillare fosse completamente conduttiva sarà necessario interporre tra la striscia conduttiva così realizzata e l'involucro un ulteriore nastro isolante (Fig. 1 e Fig. 2 D) estremamente fragile e dotato di una colla estremamente salda verso il contenitore, mentre verso l'insieme nastro / striscia conduttiva col sistema di incollaggio differenziale (tratti ad alta aderenza intervallati a tratti ad aderenza ridotta) precedentemente illustrato. La fragilità di questo strato è necessaria per evitare che si possa staccare tutto il nastro di sigillo senza alterare le caratteristiche elettriche dei componenti interni al nastro.

Un ulteriore strato composto da materiale conduttivo (Fig. 1 e Fig. 2 B), dovrà essere posizionato sopra il nastro precedentemente descritto.

Infine vi sarà uno strato isolante finale a protezione del nastro (Fig. 1 e Fig. 2 A).

Eventualmente si può realizzare una struttura analoga con la sovrapposizione di vari nastri che realizzino solo uno o più degli strati precedentemente descritti, ricordiamo inoltre che lo strato identificato dalla lettera D è indispensabile solo se la superficie del contenitore da sigillare è conduttrice.

Prestazioni analoghe si possono comunque ottenere alterando il numero e la composizione degli strati purché si seguano i concetti illustrati.

Risulta immediato capire che se si applica un nastro, realizzato secondo i principi sopraesposti, e si misura ad esempio la resistenza finale delle

strisce resistive inglobate (Fig. 1 e Fig. 2 E) risulta estremamente improbabile riuscire ad alterare il nastro o sostituirlo con resistenze equivalenti senza che un sistema di misura ripetitiva e continua della resistenza possa rilevarlo e generare un allarme.

La possibilità di effettuare tale alterazione senza venir rilevati dai sistemi di misura, si riduce ulteriormente se in contemporanea si misurassero anche altre caratteristiche del nastro applicato, quali la capacità tra le strisce resistive (Fig. 1 e Fig. 2 E) e lo stato conduttore (Fig. 1 e Fig. 2 B), od anche altri parametri quali induttanze ecc..

Ulteriori "variazioni sul tema" si potrebbero operare inglobando nel nastro altri componenti elettronici di cui rilevare in modo continuo i parametri, tra cui anche componenti attivi.

B- CONTROLLORE DI SIGILLO (CS)

L'apparato è costituito da un dispositivo elettronico in grado di generare parametri randomici (o chiavi di cifratura); scambiare infomazioni con terminali STE esterni; misurare in modo continuo i parametri elettrici dell'Opportuno Sigillo di cui sopra trattato; memorizzare parametri randomici generati; registrare se il caso ulteriori informazioni quali il numero di interrogazioni ricevute, l'ora delle stesse e del sigillo iniziale ecc...

Funzionamento dell'apparato:

Dopo l'accensione o Reset l'apparato attende alcuni secondi e quindi aspetta di riconoscere una situazione "stabile" per alcuni secondi della misura dei parametri elettrici monitorati. La situazione stabile indica che è

stato finito il posizionamento fisico del "Opportuno Sigillo".

Il dispositivo rimane in attesa di un comando dal terminale di controllo STE di "attiva Sigillo" recepito solo se le condizioni di stabilità di misura parametri sono verificate.

Dopo il riconoscimento del comando, se i parametri del nastro sono stabili, vengono generati e inviati al terminale STE (o generati dal STE ed acquisiti dal SC) specifici codici randomici. La operazione di invio sarà non ripetuta fino ad un successivo comando di "attiva Sigillo" nel qual caso i parametri saranno, ovviamente nuovi e riferiti alla successiva operazione di sigillazione in quanto il precedente sigillo risulta rotto. Nel caso che il CS. sia dotato all'interno di un orologio (opzionale) o sia in grado di avere la informazione dal STE si potrà registrare anche l'ora di sigillazione..

All'interno dell'apparato rimangono perciò memorizzati i codici randomici di cifratura / decifratura (di cui codici opportuni inviati in copia al terminale STE) ed eventuali ulteriori informazioni quali l'ora di sigillazione.

All'interno dell'apparato rimane memorizzato il valore dei parametri di misura al momento in cui essi sono misurati dopo il recepimento del comando di attivazione.

Un volta attivato e scambiate le informazioni con il terminale, il dispositivo legge in continuazione i parametri di controllo rilevandone le variazioni significative. In caso di variazione dei valori registrati l'apparato riconosce il tentativo di intrusione e cancella definitivamente tutte le celle di memoria interne ove sono stati memorizzati i precedenti codici (rottura del sigillo).

L'interrogazione esterna di stato del sigillo avviene inviando al CS. tramite

il terminale STE opportuno comando facendo uso dei codici randomici generati in fase di sigillatura (diversi possono essere il numero e le modalità di uso dei codici generati come diversi possono essere i generatori (STE o SC), si potrebbe pensare di generare due copie di chiavi pubbliche e private di cui lasciare sul SC una chiave privata personale (denominata PKPRSC) a la chiave pubblica relativa (denominata PKPUSTE) alla seconda chiave privata che rimane al STE (denominata PKPRSTE) assieme alla chiave pubblica del STE (denominata PKPUSC), si potrebbe pensare di far girare nei punti lettura la PKPUSC con cui rileggere l'ora di sigillazione criptata con la PKPRSC si potrebbe usare l'altra coppia di chiavi per abilitare comandi ricevuti dal SC solo se riconosciuti criptati con PKPRSTE)

A fronte dell'interrogazione il sistema S.E. può fornire informazioni a garanzia dell'integrità del sigillo quali:

1. l'ora e data di sigillazione.
2. numero delle precedenti interrogazioni
3. codice di integrità criptato da decriptare con PKPUSC.

Il codice di integrità è un codice che può essere unico o variare ad ogni interrogazione esterna ed è generato come cifratura effettuata tramite PKPRSC.

Le logiche di evoluzione dei codici di integrità ed altre informazioni p derivare da necessità addizionali di registrare ulteriori informazioni che supportano la tracciabilità di beni viaggianti, verificare interrogazioni da parte dei servizi di sicurezza che debbono fare ispezioni periodiche per

verificare intrusione in locali ecc.. monitorare, verificare tentativi di "ispezioni" del dispositivo da parte di terzi per verificarne il funzionamento.

Il motivo di generare differenti ad ogni interrogazione, risiede nella necessità di evitare possibili registrazioni "pirata" dello scambio dati per scopi fraudolenti.

Se presente l'orologio l'utilizzo dell'ora e data nella generazione del codice di integrità, annulla comunque qualsiasi tentativo di utilizzo di registrazioni "pirata" tra S.E. e terminale. Questa caratteristica risiede nel fatto che l'unica via per generare il codice corretto all'orario di controllo è quella di avere i codici criptati di partenza, l'ora e l'algoritmo di calcolo. Altri codici generati precedentemente, al cambiare dell'orario di controllo diventano in questo modo automaticamente inattivi.

Ulteriori raffinamenti del dispositivo possono prevedere meccanismi quali la cancellazione dei codici e delle informazioni interne dopo aver superato un numero prefissato di verifiche di integrità o dopo un tempo prefissato senza verifiche o altre a secondo dell'uso e della capacità elaborativa tipica del SC.

Ulteriore precauzione può essere posta realizzando i registri, ove il sistema memorizza i codici randomici, adoperati come base per la generazione dei codici di integrità, in celle di memorie dinamiche, in modo che qualsiasi malfunzionamento del sistema porti alla automatica distruzione dei codici in modo irreversibile. La soluzione delle celle di memoria dinamica per la memorizzazione dei codici prevede, ovviamente, la presenza di un sistema di "refesh" delle informazioni in esse contenute,

condizionando l'esecuzione di detto "refresh" alla verifica della invarianza dei parametri del nastro otteniamo un ulteriore innalzamento del grado di "sicurezza" dell'apparato.

Il sistema C.S. è realizzato in modo molto compatto ed ha i terminali per la misura dei parametri del "Opportuno Sigillo" posti sul lato superiore in modo da semplificare il corretto collegamento del nastro.

Gli elettrodi possono essere realizzati in modo da forare automaticamente gli strati isolanti inferiori del nastro.

Con una accurata scelta delle dimensioni e del posizionamento, lo stesso nastro può fissare il sistema CS al contenitore e contemporaneamente stabilire il corretto contatto.

Il sistema è realizzato in modo che il nastro possa ricoprire integralmente il sistema S.E. in modo da proteggerlo automaticamente da tentativi di effrazione.

Nel caso lo "Opportuno Sigillo" sia costituito da "Nastro Sigillante Elettronico" può risultare utile realizzare degli attrezzi idonei per il taglio del nastro, capaci pure di eliminare l'ultimo tratto delle piste o dello strato conduttivo.

Il sistema CS può anche fornire un modo non criptato un numero identificativo in modo da poter essere adoperato per seguire la movimentazione dei contenitori e poter più facilmente individuare quello di cui bisogna verificare l'integrità del sigillo.

Il sistema CS può essere realizzato in modo da generare autonomamente un allarme in caso di rottura del sigillo.

C- SISTEMA TERMINALE ESTERNO SIGILLO ELETTRONICO (STE)

Il sistema STE viene usato in fase di sigillatura, verifica del sigillo, aggiunta di informazioni sul SC (ad esempio per beni in transito).

Composto da un terminale, da un'interfaccia video (LCD) o equivalente, sistema di comunicazione verso CS, da possibile comunicazione verso rete.

Fornisce il comando di "sigillatura" / reset, recepisce o invia al CS le parole di cifratura, l'ora di sigillatura o di lettura, altre informazioni ritenute utili.

In fase di interrogazione dello stato del sigillo legge informazioni quali la data sigillatura e numero di interrogazioni precedenti ed il codice di integrità.

Ha una memoria in cui possono essere mantenuti i codici randomici e ha un software analogo a quello con cui il sigillo CS può generare il codice di integrità a partire dai codici randomici.

Può disporre di un collegamento ad una rete per ricevere da essa, in modo criptato, i codici generati all'atto della sigillazione e registrati da un altro terminale.

D-PROCEDURE DI UTILIZZO

Dopo aver applicato il sistema CS sull'elemento da sigillare (busta, scatola, container, porta, macchina etc.) si posiziona l'Opportuno Sigillo. Nel caso si tratti ad esempio di Nastro Sigillante Elettronico si avrà cura di ricoprire con il nastro il sistema CS e si porrà attenzione che le piste resistive e conduttive poste sul nastro facciano gli opportuni contatti con gli appositi elettrodi di misura parametri posti sulla parte superiore del

sistema CS. e nel caso che lo schermo conduttore sia realizzato con un secondo nastro si applica anche esso.

Si inizializza il sistema CS con la contestuale generazione dei parametri randomici (o chiavi di cifratura) e registrazione dell'ora su CS e STE.

Si comunicano in modo sicuro e criptato detti valori agli enti preposti alla ricezione e al controllo o traking (in caso di elementi mobili).

Nel momento del controllo o della apertura del sigillo si verificano le eventuali effrazioni o informazioni di servizio.

Il codice di integrità può essere fornito differente ad ogni lettura per evitare di poterlo captare con apparati pirata e riprodurlo tramite un falso sigillo.

Qualora l'"Opportuno Sigillo" sia costituito da "Nastro Sigillante Elettronico" che lavora su parametri resistivi si possono adattare due filosofie differenti di posizionamento:

- La prima, consigliabile per elementi di dimensioni contenute, consiste nell'avvolgere completamente l'elemento col nastro. In questo caso converrà verificare i parametri monitorati con collegamenti agli estremi del nastro.
- La seconda, consigliabile nel caso di voler applicare il nastro Sigillante solo su una zona "apribile" dell'elemento si potrà adoperare il Nastro Sigillante con due "strisce resistive" cortocircuitate all'estremo opposto rispetto al lato dove è applicato il sistema CS.

In questo caso il corto circuito può essere realizzato tramite appositi adesivi progettati ad hoc che incollati sulla superficie del contenitore presentito dei terminali sulla parte superiore tali da creare il cortocircuito

su un nastro posizionato sopra di esso.

Come prima variante di questo secondo caso si possono realizzare Nastri Sigillanti di lunghezza prefissata con le due "strisce resistive" cortocircuitate ad uno degli estremi.

Come ulteriore variante di questo caso si può pensare di sostituire il cortocircuito con resistenze abbastanza elevate e poste ad intervalli costanti lungo il nastro. Questo fa sì che dal punto di vista elettrico visto dall'estremo di applicazione del sistema CS il circuito appaia come una serie di anelli resistivi in cascata. E per un numero non elevato di questi una manomissione di un qualsiasi anello può essere rilevata dall'estremo dove è applicato il sistema CS. Questa soluzione permette di avere un nastro continuo e decidere la lunghezza del sigillo semplicemente tagliandolo al momento dell'applicazione.

Il posizionamento del Nastro Sigillante nelle due modalità sopra descritte, ad anello o a circuito aperto, può richiedere due tipi di sistemi CS differenti per il posizionamento degli elettrodi.

CONCLUSIONI

Si è descritto un sistema costituito da più elementi interoperanti che in modo certo possa fornire delle prestazioni comprendenti ma superiori (sono possibili ulteriori verifiche e memorizzazione di informazioni) a quelle che precedentemente erano offerti dai sistemi di sigillatura con ceralacca e consimiliari.

Questo sistema permette una facile applicazione a qualsiasi tipo di contenitore dalle piccole buste per documenti ai grandi container alle case

alle porte ecc...

Il sistema descritto risponde alle crescenti esigenze di sicurezza che si hanno in varie aree.

Il principio di funzionamento si basa sul disporre di una struttura, da applicare sul contenitore da sigillare, inglobante dei materiali le cui caratteristiche elettriche variano in modo evidente nel caso vi sia il più piccolo tentativo di separazione tra detta struttura e la superficie ove é stata applicata, la variazione di queste caratteristiche elettriche è monitorata da un sistema elettronico, che ove riscontri una variazione significativa distrugga dei codici randomici al suo interno (apertura sigillo).

E stata progettata una struttura esemplificativa realizzata tramite un semplice ed economico nastro adesivo a più strati, che si distrugge ad ogni tentativo di manomissione.

E' stato progettato il sistema elettronico "CS" in modo tale da poter essere applicato sotto il nastro in modo da essere anche esso protetto da tentativi di manomissione.

Particolare cura è stata posta nell'ipotizzare un esempio di codici di integrità del sigillo in modo che essendo variabili di volta in volta e con l'orario, non siano clonabili a valle di eventuali registrazioni "pirata" di interrogazioni di integrità del Sigillo.

Sono state presentati, a scopo esemplificativo, dei possibili protocolli di utilizzo.

****

Particolare cura è stata posta nello studiare il sistema per un uso semplice che non richiedesse personale qualificato e con costi contenuti.

RIVENDICAZIONI

Sistema di "**SIGILLO ELETTRONICO**",

1. Sistema di "SIGILLO ELETTRONICO" descritto nelle sue componenti e varianti di implementazione nel presente documento;
2. Soluzione antieffrazione per elementi Mobile e Immobili basato sulla memorizzazione sul sistema elettronico solidale all'elemento "protetto" di codici e della loro cancellazione laddove si riscontri una variazione del valore di parametri misurati sull'elemento fisico di sigillo "Opportuno Sigillo" costantemente monitorato.
3. Misura dei parametri elettrici quali resistenze capacità, induttanze, relativi all'Opportuno Sigillo al fine di verificare la manomissione del Opportuno Sigillo stesso per l'utilizzo di cui alla prima rivendicazione
4. Codifica variabile ad ogni interrogazione dello stato del Sistema realizzata tramite apposito algoritmo a partire dai codici nascosti ed eventualmente dall'orario finalizzato a proteggere il messaggio da registrazioni indesiderate e a fornire informazioni circa la "vita" dell'elemento inerente la anti effrazione per l'utilizzo nel contesto di cui alla prima rivendicazione.
5. Cancellazione definitiva di uno o più codici interni ed eventuali ulteriori dati registrato nel caso di forzatura dell'Opportuno Sigillo e/o qualora si verifichino tentativi di interrogazione o lettura al di fuori di quelli

Particolare cura è stata posta nello studiare il sistema per un uso semplice che non richiedesse personale qualificato e con costi contenuti.

RIVENDICAZIONI

Sistema di "**SIGILLO ELETTRONICO**",

1. Sistema di "SIGILLO ELETTRONICO" descritto nelle sue componenti e varianti di implementazione nel presente documento;
2. Soluzione antieffrazione per elementi Mobile e Immobili basato sulla memorizzazione sul sistema elettronico solidale all'elemento "protetto" di codici e della loro cancellazione laddove si riscontri una variazione del valore di parametri misurati sull'elemento fisico di sigillo "Opportuno Sigillo" costantemente monitorato.
3. Misura dei parametri elettrici quali resistenze capacità, induttanze, relativi all'Opportuno Sigillo al fine di verificare la manomissione del Opportuno Sigillo stesso per l'utilizzo di cui alla prima rivendicazione
4. Codifica variabile ad ogni interrogazione dello stato del Sistema realizzata tramite apposito algoritmo a partire dai codici nascosti ed eventualmente dall'orario finalizzato a proteggere il messaggio da registrazioni indesiderate e a fornire informazioni circa la "vita" dell'elemento inerente la anti effrazione per l'utilizzo nel contesto di cui alla prima rivendicazione.
5. Cancellazione definitiva di uno o più codici interni ed eventuali ulteriori dati registrato nel caso di forzatura dell'Opportuno Sigillo e/o qualora si verifichino tentativi di interrogazione o lettura al di fuori di quelli

considerati accettabili per rappresentare la situazione nel contesto di cui alla prima rivendicazione.

6. Memorizzazione dei codici ed eventuali altri dati interni su memorie dinamiche il cui rinfresco è condizionato dalla invarianza dei parametri elettrici del nastro sigillante elettronico nel contesto di sistemi di cui alla prima rivendicazione.
7. Opportuno Sigillo costituito da Nastro Sigillante Elettronico che incorpora strisce di materiale elettricamente monitorabile (resistenza, capacità.) e superfici conduttive da potersi utilizzare nel sistema antieffrazione di cui ai fini delle precedenti rivendicazioni o altri sistemi si sicurezza.
8. Posizionamento del sistema elettronico CS sotto l'Opportuno Sigillo (Nastro Sigillante Elettronico) per proteggerlo automaticamente da possibili effrazioni in contesti di cui alla precedente rivendicazione.
9. Dosaggio della colla in modo differente in vari tratti e strati del nastro di cui ai punti precedenti per avere la certezza di alterare i componenti e materiali di cui si misurano i parametri elettrici e non elettrici in caso di tentativo di effrazione per i fini di cui alle precedenti rivendicazioni.
10. Misura dei parametri elettrici, di elementi attivi incorporati in Nastri o superfici adesive al fine di verificare la manomissione di pacchi, plichi etc. per contenitori vari per l'utilizzo ai fini delle precedenti rivendicazioni.

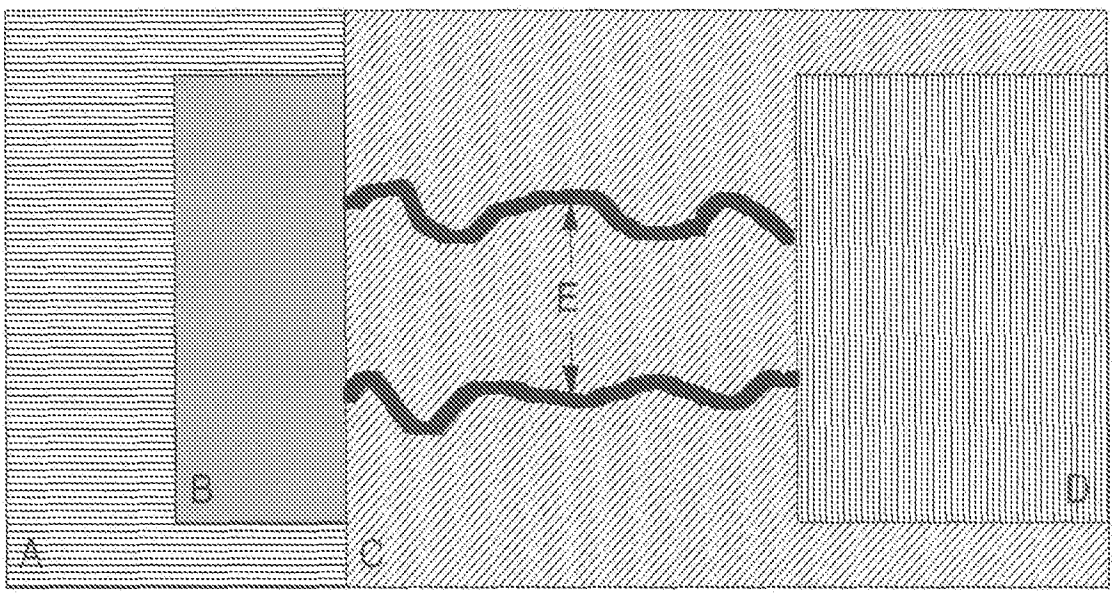

Fig. 1

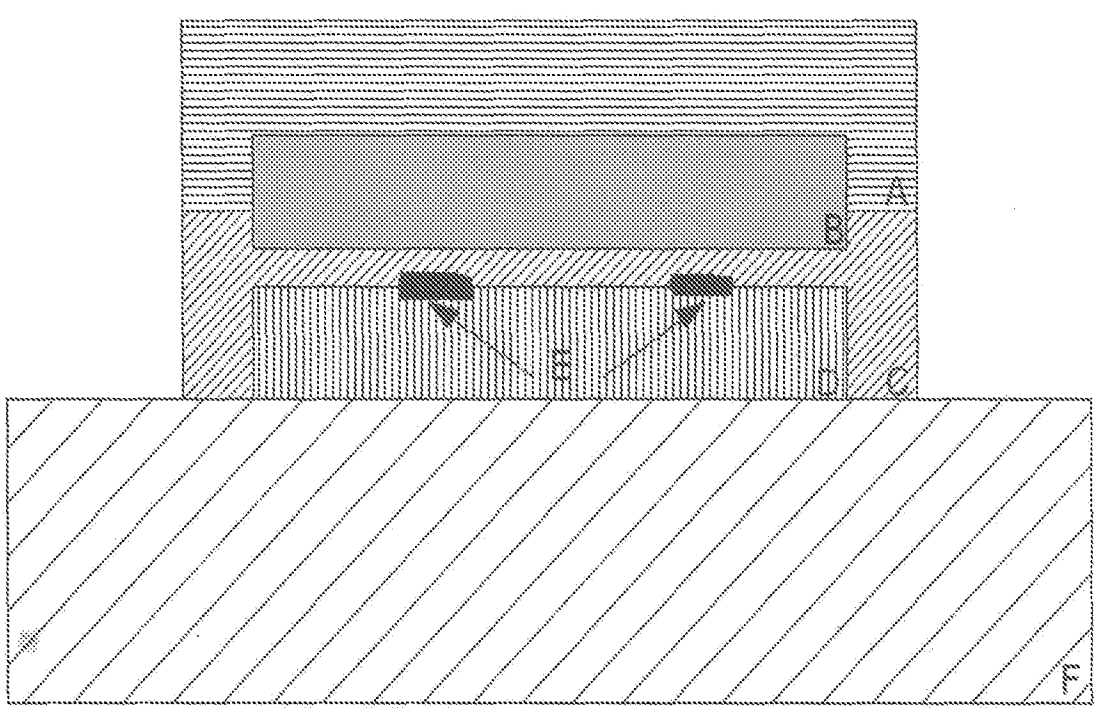

Fig. 2