(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 October 2013 (31.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/162843 A1

(51) International Patent Classification:
G06F 21/86 (2013.01) *H05K 5/03* (2006.01)

(21) International Application Number:
PCT/US2013/035170

(22) International Filing Date:
3 April 2013 (03.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2012-0042664 24 April 2012 (24.04.2012) KR
13/556,101 23 July 2012 (23.07.2012) US

(72) Inventor; and
(71) Applicant : **LEE, Cheol, Jae** [US/US]; 11254 Key West Ave. Unit 6, Porter Ranch, CA 91326 (US).

(74) Agent: **LEE, Harry, S.**; 660 South Figueroa Street, Suite 2300, Los Angeles, CA 90017 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

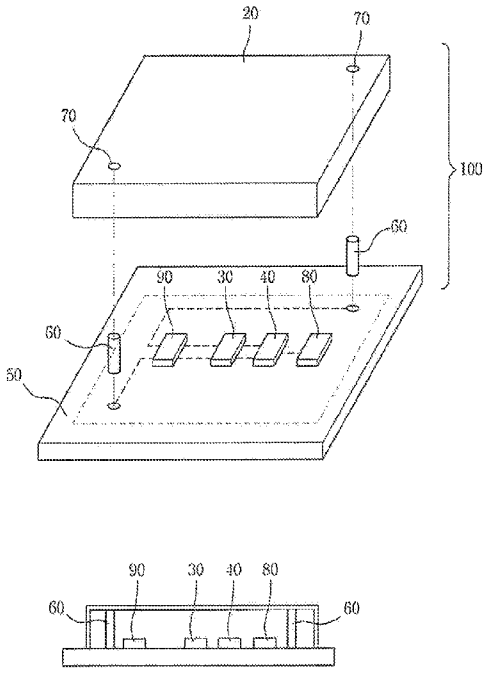
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: TAMPER RESPONDENT COVERING

Fig. 2



(57) Abstract: Disclosed is a tamper respondent covering. The tamper respondent covering has a cover-shaped structure to cover an electronic part which is exposed. This covering protects electronic parts embedded inside or exposed outside a product, such as ICs that contains data concerning security and certification, communication connectors that transmit data, etc. from a tempering operation or an alternating operation. The tamper respondent covering protects data from a tampering operation or an altering operation by erasing the data or disabling operation of the electronic part containing the data in response to an act of attempting to remove the covering from a printed circuit board of the electronic part or to drill a hole in the covering.

WO 2013/162843 A1

TAMPER RESPONDENT COVERING

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of earlier filing date and right of priority to Korean Patent Application No. 10-2012-0042664, filed on April 24, 2012, and U.S. Patent Application No. 13/556,101, filed on July 23, 2012, the contents of which are all hereby incorporated by reference herein in their entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a tamper respondent covering, and, more particularly to a tamper respondent covering that protects data from a tampering operation by covering electronic parts such as, integrated circuits (ICs) that are embedded inside or exposed outside a product and contain data concerning security and certifications, and communication connectors that transmit data, etc. using a cover-shaped structure and by erasing important data stored in the electronic part to be protected or disabling the operation of the electronic part when it detects tampering of the electronic part to be protected, for example, when someone attempts to remove the tamper respondent covering from a printed circuit board (PCB) of the electronic part or to drill a hole in the tamper respondent covering for the purpose of hacking the data in the electronic part.

Description of the Related Art

Enclosures or covers that enclose electronic parts have the form of envelopes and shallow boxes with walls which are formed by folding flexible sheets incorporating tampering detection characteristics. The sheet includes layers of flexible material in which a matrix of semi-conductive lines printed on an insulating film is incorporated. The matrix of semi-conductive lines forms a continuous conductor which breaks if there is an attempt to penetrate the insulating film.

Since a circuit in the enclosures or covers has a conductor, the circuit is monitored by opening the conductor and measuring the resistance between the two ends of the circuit. The flexible sheets are folded and overlapped to create a wedge-, cuboid-, or cube-shaped enclosure as disclosed in GB 258 075 A in which a laminate is folded about a plurality of fold lines to form an enclosure. US Patent No. 05,858,500 discloses an envelope- or a box-shaped flexible sheet which is set in a settable material.

The enclosure is intended to surround an item to be protected, such as an electronic device which may be an encryption module, a chip, or a circuit for processing which stores or carries potentially valuable information. As noted above, all attempts to penetrate the enclosure result in damaging to one or more of the lines, which is detected by the change in the electrical characteristics of the conductor. Upon detecting such a change, the valuable information stored in the item is typically erased or destroyed, and an alarm may be activated.

It may however be relatively time-consuming and expensive to enclose and surround the item with such an enclosure. Also, the provision of an enclosure which completely surrounds an item restricts the manner in which the item may be located and positioned within a larger device and is likely to, for example, preclude conventional surface mounting.

US Patent Application Publication No. US2002/0002683 Al by Benson, et al. discloses a Security Module System that comprises a cover which encloses the components to be protected and abuts against the substrate, on which the components are mounted, using a ball grid array connection system. The cover comprises a serpentine pattern of metallic conductors which may be interconnected with a pattern of metallic conductors embedded in the substrate by a system of plated through-holes and blind vias to form a three dimensional array of conductors surrounding the components to be protected. To prevent the pattern and location of the metallic conductors from being detected by non-destructive techniques such as X-rays, back panels made of X-ray opaque material are laminated on the cover and the substrate.

Furthermore, to deter a chemical attack on the system, additional elements such as conductive ink fuses are provided on the substrate. The system disclosed has a number of

shortcomings in relation to resistance to intrusive attacks, for example, the X-ray opaque back planes can be easily located and could be ground away or electrochemically etched, allowing the underlying pattern of metallic conductors to be exposed to X-rays or other non-destructive techniques. Areas of the metallic conductors could then be effectively bridged by attaching wire links to the serpentine pattern of conductors and the cover or substrate which was breached, without triggering the tamper respondent circuit.

Similarly, the vias in the side wall of the cover could be located and similarly bridged without triggering the tamper respondent circuit. The side walls are not protected by the pattern of serpentine conductors and therefore present an area susceptible to attack, as does the system of ball grid array interconnections.

It would also be possible by similar techniques to locate the positions of the conductive ink fuses on the circuit board and to direct a chemical attack at locations far away from the fuses without triggering a tamper response.

Fig. 1 illustrates a tamper respondent covering disclosed in PCT Publication No. WO2005/098950. In this patent document, the tamper respondent covering 10 is adapted for mounting on a surface having at least one item 3 and 4 disposed thereon, and the tamper respondent covering 10 includes a cover member defining a recess 7 and at least one non-metallic detecting element having an electrical characteristic disposed on the cover member. That is, the cover member is adapted for mounting on the surface and covering and protecting the at least one item 3 (and 4) on the surface such that damage to the at least non-metallic detecting element results in a detectable variation in the electrical characteristics.

The inventor of the present application invented a device that can reliably detect an external shock or attack even when the device is applied to any type of product by improving the technology disclosed in PCT Publication No. WO2005/098950.

SUMMARY OF THE INVENTION

Accordingly, the present invention has been made keeping in mind the above problems occurring in the related art, and is intended to provide a tamper respondent covering which protects data from tampering or altering by covering exposed electronic parts, such as ICs embedded inside or exposed outside a product and containing data concerning security and certification, and communication connectors that transmit data, using a cover-shaped structure so that the electronic parts can be protected from tampering and alteration, and by erasing important data or disabling the operation of the electronic part, in response to an attempt to remove the covering from a printed circuit board of an electronic device or drilling a hole in the covering for the purpose of hacking the data.

In order to achieve an object of the invention, according to one aspect of the present invention, there is provided a tamper respondent covering that protects data stored in an electronic part so that the data will not be illegally leaked by an external attack by erasing the data stored in the electronic part to be protected from an external shock or attack, or by disabling the operation of the electronic product, the tamper respondent covering including: a power supply that supplies power; a cover having a predetermined shape and covering a device to be protected; a substrate on which the device to be produced is mounted; the device to be protected, which is mounted on the substrate; a metallic portion that forms a external surface of the cover; a conductive coating layered on an internal surface of the cover; an insulating coating, interposed between and electrically isolating the metallic portion and the conductive coating from each other; a contact formed at a predetermined portion of the conductive coating; a connector electrically connected to the contact and formed between the cover and the substrate; a tamper detecting device that detects the electrical disconnection of the connector from the contact; and a controller that erases data of the device or disables operation of the device in response to a signal transmitted from the tamper detecting device.

According to the present invention, when the tamper covering of the present invention is provided for an electronic device equipped with an important electronic part to be protected, a tampering operation wherein it is attempted to remove the covering from the substrate or to drill a

hole in the covering is detected, and then the operation of the electronic part to be protected is disabled or data is erased. Accordingly, the covering of the present invention has the advantage of preventing the electronic device to be protected from being illegally used.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and further advantages of the present invention will be more clearly understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a cross-sectional view illustrating a tamper respondent covering according to a related art;

Fig. 2 is a perspective view illustrating a tamper respondent covering according to a first embodiment of the present invention;

Fig. 3A is a cross-sectional view illustrating a cover portion according to the first embodiment;

Fig. 3B is a cross-sectional view illustrating a cover portion according to a second embodiment;

Fig. 3C is a diagram illustrating an internal structure of the covering according to the first embodiment; and

Figs. 4A and 4B are perspective views illustrating various shapes of the tamper respondent covering according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Hereinbelow, a tamper respondent covering according to an embodiment of the present invention will be described in detail with reference to the accompanying drawings. Throughout the drawings, elements that are substantially the same or similar are denoted by the same or

similar reference signs.

Fig. 2 is a perspective view illustrating a tamper respondent covering according to a first embodiment of the present invention.

A temper respondent covering 100 includes a cover 20, devices 30 and 40 mounted on a Printed Circuit Board (PCB), a connector 60 made of a conductive rubber or a metal, a contact connected to the connector 60, and a controller 80. The covering 100 further includes a power supply unit 90 to supply power because the covering 100 is a portable part. The power supply unit 90 may be provided as a battery. The battery may be, but is not limited to, a lithium battery or a lithium ion battery. Any type of battery can be used as long as these have the same or equivalent function as the exemplary batteries.

The device 30 detects a tampering operation, and the device 40 is a storage device in which data concerning security or certification is stored. When an external shock is applied to the covering, for example, when someone attempts to remove the substrate 50 from the covering 20 or to drill a hole in the covering 20, the following operation is performed: the connector 60 is disconnected from the contact 70; at the same time, a change in an electrical characteristic attributable to the disconnection is detected by the device 30 for detecting the tamper; a signal is transmitted from the tamper detecting device 30 to the controller 80; and finally the controller 80 erases the data stored in the device 40 to be protected or disables the operation of the device 40. The cover 20 and the substrate 50 are coupled to each other using screws or other locking means. The cover 20 and the substrate 50 can be separated by unscrewing the screw or unlocking the locking means.

Fig. 3A is a cross-sectional view illustrating a cover according to the first embodiment, Fig. 3B is a cross-sectional view illustrating a cover according to a second embodiment, and Fig. 3C is a diagram illustrating an internal structure of the cover according to the first embodiment.

Referring to Fig. 3A, the cover 20 includes a metallic portion 110 made of rigid material, a conductive coating 130 of a strip shape made of conductive material, and an insulating coating 120 that is interposed between the metallic portion 110 and the conductive coating 130 to

electrically isolate the conductive coating 130 and the metallic portion 110 from each other.

Referring to Fig. 3B, this embodiment is different from the embodiment of Fig. 3A in that a conductive coating 130 and an insulating coating 120 each have a multilayered structure. With this structure, it is possible to more reliably detect the tampering operations of drilling a hole in the covering or separating the cover 20 and the substrate 50 from each other. Fig. 3B illustrates the multilayered structure composed of two layers. However, the multilayered structure is not limited to the one with two layers but may be a one with three or more layers.

Fig. 3C illustrates the conductive coating 130 in detail. As described above, the conductive coating 130 has a strip shape and a pattern of rectangular waves, but may not be limited thereto. For example, if a hole is drilled through the conductive coating 130, the pattern of the conductive coating 130 is disrupted such that electrical change is detected due to the disruption of the pattern of the conductive coating 130.

Figs. 2 and Figs. 3A to 3C illustrate a structure in which the cover and the substrate are combined. However, a power supply device, a detecting device, a connector, and a controller may be embedded in the cover, so that the cover may be used alone without being combined with the substrate.

Figs. 4A and 4B are perspective views illustrating tamper respondent covers of various shapes.

As illustrated in the drawings, the tamper respondent covering of the present invention has a rectangular shape as illustrated in Fig. 4A, or an inverted T shape as illustrated in Fig. 4B. However, such shapes are presented only by way of example but may be modified into various forms.

As described above, when the tamper respondent covering of the present invention is applied to an important electronic part to be protected, tampering operations such as removing the cover from the substrate or drilling a hole in the covering is detected, and then the electronic part to be protected will be disabled or data in the electronic part will be erased. Accordingly, it is possible to protect the device to be protected from being used illegally.

The covering of the present invention can be applied, but not limitedly, to communication connectors, payment card slots, circuit boards, magnetic strip card reader heads, products used under certification, card reader terminals, PIN input devices, Automatic Teller Machines (ATMs), card reader terminals for gas stations, etc. The covering of the present invention can be applied to equivalents of the above examples.

Although embodiments of the tamper respondent covering according to the present invention have been described with reference to the accompanying drawings for illustrative purpose, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.

WHAT IS CLAIMED IS:

1. A tamper respondent covering that prevents data, which is stored in an electronic part, from being accessed as a result of an external shock or attack by erasing the data stored in the electronic part to be protected or by disabling operation of the electronic part, the tamper respondent covering comprising:

a power supply device which supplies power;

a cover of a predetermined shape, the cover covering a device to be protected;

a substrate, on which the device to be protected is mounted;

the device to be protected, the device being mounted on the substrate;

a metallic portion, which forms an external surface of the cover ;

a conductive coating, which has a multilayered structure and is coated on an internal surface of the cover;

an insulating coating, interposed between the metallic portion and the conductive coating, to electrically isolate the metallic portion and the conductive coating from each other;

a contact formed at a portion of the conductive coating;

a connector electrically connected to the contact and formed between the cover and the substrate;

a tamper detecting device that detects an electrical disconnection between the connector and the contact; and

a controller that erases data stored in the device to be protected or disables operation of the device to be protected in response to a signal transmitted from the tamper detecting device.

2. The tamper respondent covering according to claim 1, wherein each of the insulating coating and the conductive coating has a multilayered structure.

3. The tamper respondent covering according to claim 1, wherein the cover has a shape

corresponding to that of the device to be protected.

4. The tamper respondent covering according to claim 1, further comprising a fixing unit that combines the cover and the substrate with each other.

5. A tamper respondent covering that protects data stored in an electronic part to be protected from an external shock or attack so that the data is not illegally accessed by erasing the data stored in the electronic part or disabling operation of the electronic part, the tamper respondent covering comprising:

a power supply device that supplies power;

a cover that covers a predetermined shape of an electronic part to be protected;

a metallic portion that forms an external surface;

a conductive coating layered on an internal surface of the cover;

an insulating coating interposed between the metallic portion and the conductive coating so that the metallic portion and the conductive coating are electrically isolated from each other;

a contact formed at a portion of the conductive coating;

a connector electrically connected to the contact and formed in the cover;

a tamper detecting device, installed in the cover, to detect an electrical disconnection between the connector and the contact; and

a controller, installed in the cover, to erase data in the electronic part or disable operation of the electronic part in response to a signal transmitted from the tamper detecting device.

Fig. 1

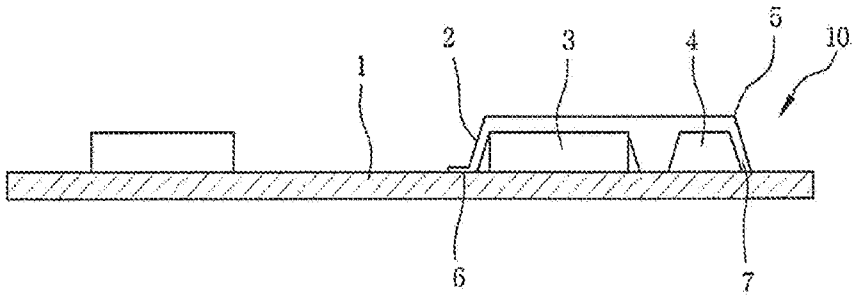


Fig. 2

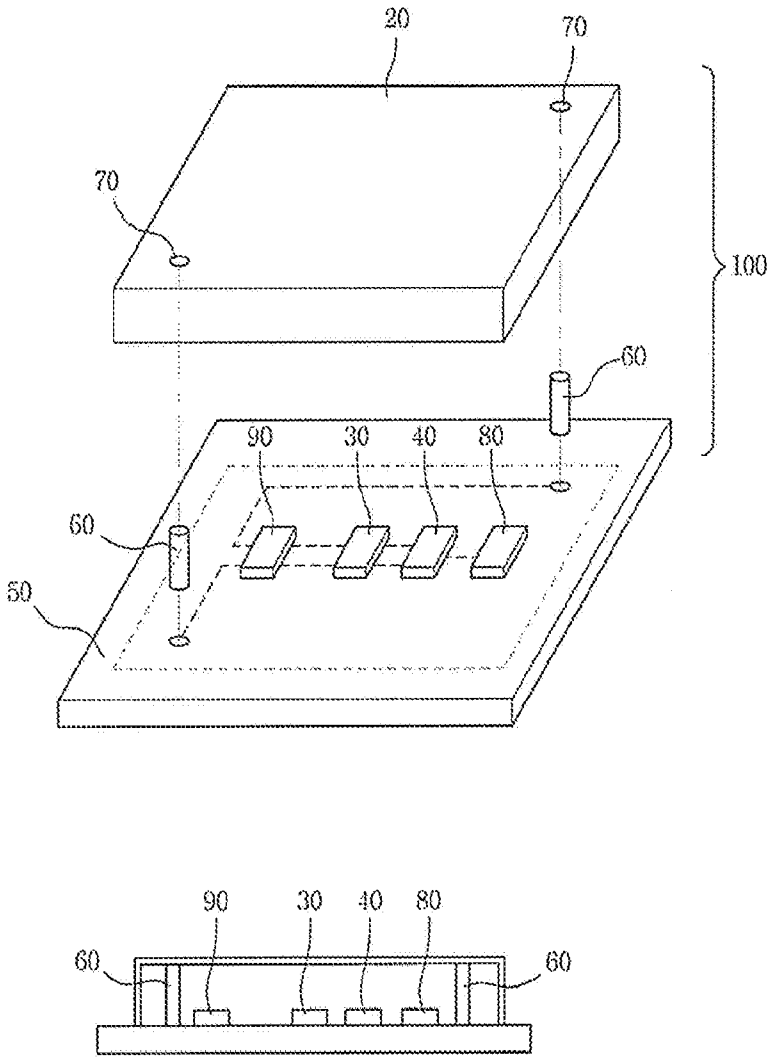


Fig. 3A

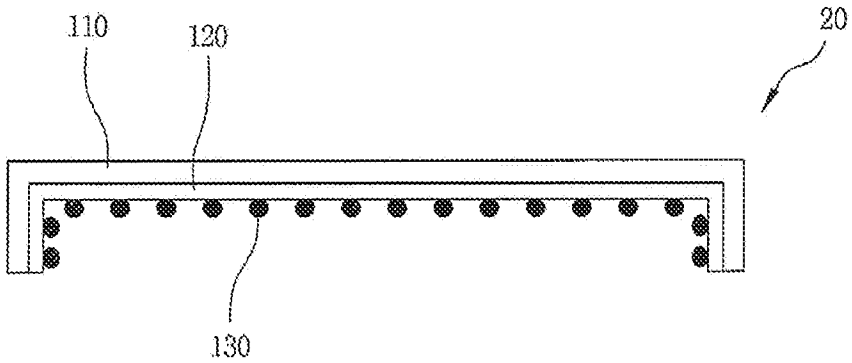


Fig. 3B

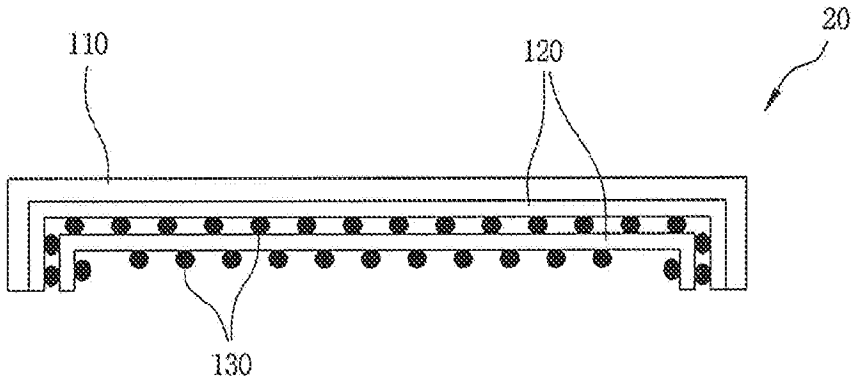


Fig. 3C

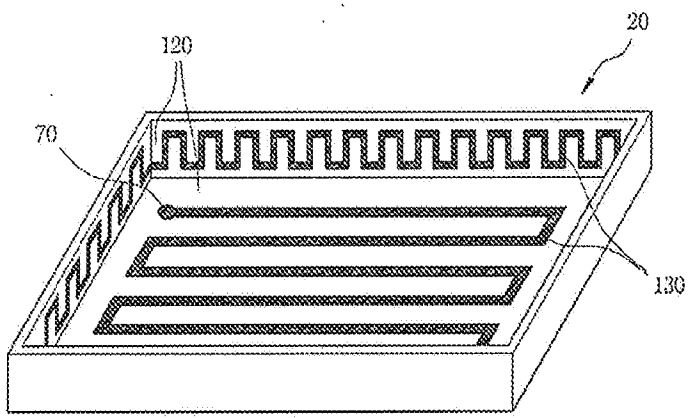


Fig. 4A

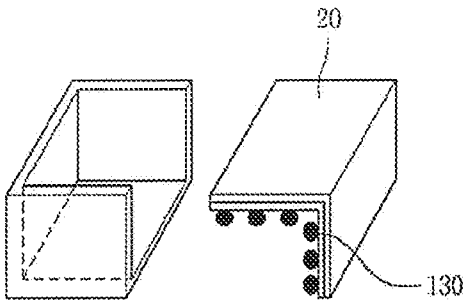
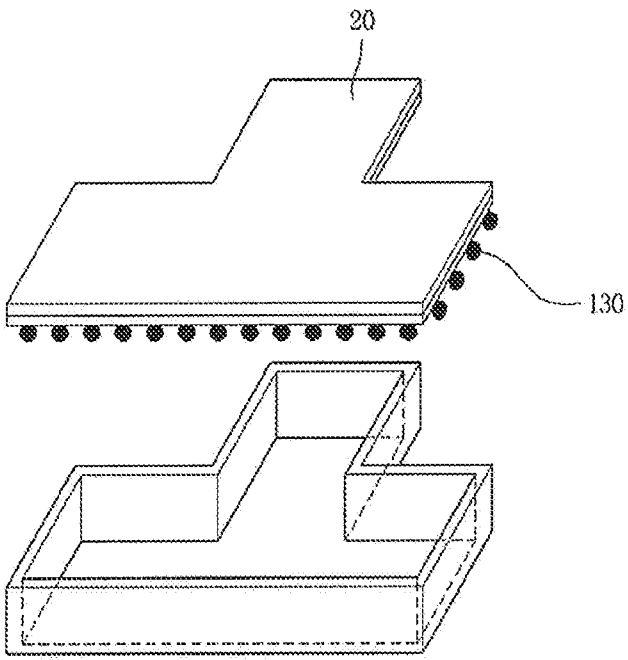


Fig. 4B



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/035170

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/86(2013.01)i, H05K 5/03(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/86; G08B 21/00; B41M 3/14; H05K 1/16; H05K 3/00; H05K 1/00; H05K 1/14; G08B 13/08; H05K 5/03

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords:tamper respondent, conductive, insulate, metal, erase.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006-0049941 A1 (STEVE B. HUNTER et al.) 09 March 2006 See paragraphs [0035]-[0039], [0048], [0098], [0105]; claims 25, 53; and figure 9.	1-5
Y	US 2008-0284610 A1 (STEPHEN B. HUNTER) 20 November 2008 See paragraphs [0019], [0027], [0054]-[0055]; and claims 36, 98.	1-5
A	US 2011-0090658 A1 (CHRISTIAN ADAMS et al.) 21 April 2011 See abstract; paragraphs [0008], [0015], [0019]-[0020]; claims 1-2; and figures 4A-4C.	1-5
A	US 2009-0040735 A1 (KARL CHAN et al.) 12 February 2009 See paragraphs [0032]-[0035]; claims 1-5; and figures 1A-1B.	1-5
A	US 2010-0177487 A1 (NAUMAN ARSHAD et al.) 15 July 2010 See paragraphs [0041], [0043]-[0044]; and claims 5-10.	1-5

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 July 2013 (09.07.2013)	**09 July 2013 (09.07.2013)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
BYUN Sung Cheal
Telephone No. +82-42-481-8262

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/035170

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0049941 A1	09/03/2006	EP 1784800 A1	16/05/2007
		EP 1784800 A4	15/04/2009
		US 7323986 B2	29/01/2008
		WO 2006-028665 A1	16/03/2006
US 2008-0284610 A1	20/11/2008	AU 2005-231051 A1	20/10/2005
		AU 2005-231051 A2	20/10/2005
		AU 2005-231051 B2	09/06/2011
		CA 2563240 A1	20/10/2005
		CA 2563240 C	12/03/2013
		CN 1998080 A	11/07/2007
		CN 1998080 B	08/05/2013
		EP 1751798 A1	14/02/2007
		EP 1751798 B1	26/12/2012
		GB 0407972 D0	12/05/2004
		GB 2412996 A	12/10/2005
		GB 2412996 B	12/11/2008
		JP 2007-533129 A	15/11/2007
		JP 4965430 B2	06/04/2012
		US 7978070 B2	12/07/2011
		WO 2005-098950 A1	20/10/2005
US 2011-0090658 A1	21/04/2011	EP 2489072 A1	22/08/2012
		US 2011-0120764 A1	26/05/2011
		US 2012-0091456 A1	19/04/2012
		WO 2011-046769 A1	21/04/2011
		WO 2011-046770 A1	21/04/2011
US 2009-0040735 A1	12/02/2009	EP 2186036 A1	19/05/2010
		JP 2010-541028 A	24/12/2010
		US 7787256 B2	31/08/2010
		WO 2009-023075 A1	19/02/2009
US 2010-0177487 A1	15/07/2010	US 2013-058052 A1	07/03/2013
		US 8325486 B2	04/12/2012