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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 October 2015 (01.10.2015)

(10) International Publication Number
WO 2015/148607 A1

(51) International Patent Classification: *G08B 13/14* (2006.01)

(21) International Application Number: PCT/US2015/022390

(22) International Filing Date: 25 March 2015 (25.03.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/970,303	25 March 2014 (25.03.2014)	US
14/448,598	31 July 2014 (31.07.2014)	US

(71) Applicant: INTELLIGENT TECHNOLOGIES INTERNATIONAL, INC. [US/US]; 800 West Avenue, Unit 545, Miami Beach, FL 33139 (US).

(72) Inventors: BREED, David; 800 West Avenue, Unit 545, Miami Beach, FL 33139 (US). **JOHNSON, Wendell C.**; 839 S. Beacon Street, #5305, San Pedro, CA 90733 (US).

(74) Agent: ROFFE, Brian; 9206 Avers Avenue, Evanston, IL 60203-1502 (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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,

[Continued on next page]

(54) Title: SECURE TESTING SYSTEM AND METHOD

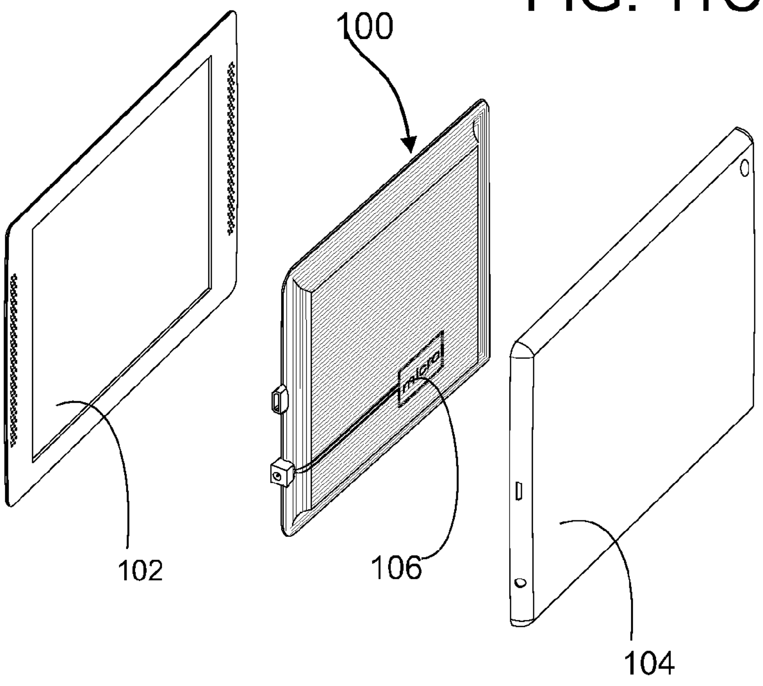


FIG. 11C

(57) Abstract: Method for detecting an attempt to physically alter an electronic device including enclosing the device in a cover component (102, 104), positioning conductive wires (100) in the cover component (102, 104) external to the device, coupling a security assembly (106) to the wires, and then monitoring impedance of the wires (100) by means of the security assembly (106). When a change in impedance is detected by the security assembly (106), a required security code needed for use of the device is deleted.

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SECURE TESTING SYSTEM AND METHOD

TECHNICAL FIELD

The present disclosure relates to the field of a computer-based system and method for taking a test while ensuring that the test-taker is not receiving assistance from another person while taking the test and that the device being used for displaying or taking the test has not been and is not being tampered with or otherwise compromised.

BACKGROUND ART

There has been a great deal of discussion in the press over the past several years relating to MOOCs, Massive Open Online Courses. Through the use of the Internet, education can be freely distributed to anyone who has Internet access. It is now generally recognized that mastery of almost any field taught in colleges and universities can be achieved by a motivated student without actually attending lectures at that college or university. Thus, the technology is in place for a student to obtain the knowledge that has previously only been available to a campus-resident, matriculated student at a college, university or other institution at virtually no cost.

In contrast, the cost of a traditional Massachusetts Institute of Technology (MIT) education, for example, resulting in a bachelor's degree can exceed one hundred thousand dollars. The only impediment which exists from preventing a university such as MIT from granting a degree to such a student is that the university needs to know with absolute certainty that the student did not cheat when taking the various exams required to demonstrate mastery of the coursework. With a degree from MIT, for example, industry will hire such a person at a starting salary approaching or exceeding $100,000 per year. Thus, the value to the student is enormous. Since the information which must be mastered is now available for free on the Internet, the only impediment separating a motivated student from a high starting salary is that a degree-granting university must be certain that the student has demonstrated his mastery of the material through successful completion of examinations.

As generally used herein, a "test" is any type of question-based application that requires analysis by a person taking the test and a response from this person. A test may therefore be considered an examination, a quiz, an assessment, an evaluation, a trial and/or an analysis.

As generally used herein, a "laptop computer" is a portable computing device that includes hardware and software for conventional functionality for outputting questions (visually and/or audibly) and receiving via one or more user interfaces, responses to the questions. A laptop computer is an example of a preferred implementation of the disclosure but the disclosure may also be implemented in other types of computers, e.g., desktops, tablets, notebooks, notepads, and the like.

SUMMARY OF THE INVENTION

The present disclosure is directed at solving the problem of guaranteeing with a high degree of certainty that a student taking a test is acting alone without the aid of a consultant or otherwise cheating.

A method for detecting an attempt to physically alter an electronic device in accordance with the invention is a type of chassis intrusion detector. In the method, the device, such as a laptop used for test-taking, is enclosed a cover component that may comprise a front cover and a back cover, conductive wires are positioned in the cover component external to the device (i.e., not part of the internal wiring of the device), a security assembly to the wires, e.g., to their ends, and then impedance of the wires is monitored by means of the security assembly (e.g., resistance and/or mutual inductance between a pair of wires). When a change in impedance is detected by the security assembly, a required security code needed for use of the device is deleted. In a preferred embodiment, the device is a laptop being used for test-taking and thus with the method incorporated into the device, secure test taking is provided.

The security assembly includes a processor, a power source for providing power to the processor and a RAM assembly containing a required security code for use of the device for test-taking purposes. The security assembly is configured such that any attempt to disassemble the security assembly will break one or more wires connecting the power source to the processor and such that a change in impedance relative to a threshold will cause the security code to be erased from the RAM assembly. The security assembly may be coupled to the device using a port of the device and with the security assembly within films around or within the cover component. Apertures are provided in the envelope defined by the films in which the device is placed, the apertures having a size and location aligning with power and USB ports of the device. The films are preferably transparent at portions that overlie a display of the device.

A method for limiting viewing of content on a display includes changing images being displayed on the display at a high rate at which viewing the display does not provide a discernible image to a viewer, equipping a person with a viewing device having lenses that are selectively opaque or transparent, and controlling the lenses to cause the lenses to be transparent only when determined content, e.g., a test, is being displayed on the display to enable only a lenses- equipped person to correctly view the predetermined content. The image frames containing the predetermined content are preferably randomized and an indication of the randomization provided only to the viewing device. The viewing device preferably incorporates a chassis intrusion detection system.

BRIEF DESCRIPTION OF DRAWINGS

The following drawings are illustrative of embodiments of the system developed or adapted using the teachings of at least one of the embodiments disclosed herein and are not meant to limit the scope of the disclosure as encompassed by the claims.

FIG. 1 is a schematic view of a tower for placement in proximity to a computer used for test taking.

FIG. 2 is an outline of a fisheye lens for use with the tower shown in FIG. 1.

FIG. 3 is an outline of a dual camera assembly for use with the tower shown in FIG. 1.

FIG. 4 is a view of a transducer board for the tower shown in FIG. 1.

FIG. 5 is a view of a processor board for the tower shown in FIG. 1.

FIG. 6 is a side view of the boards shown in FIGS. 4 and 5 connected together.

FIG. 7 is a schematic showing a test-taking arrangement with a head-mounted apparatus.

FIG. 8A illustrates the arrangement where the tablet is mounted on ledge of the tower.

FIG. 8B illustrated the case of FIG. 8A only with the tower and the tablet separated.

FIG. 9 is a similar illustration to FIG. 7 but with use of display glasses similar to Google Glass.

FIG. 10 is a view where the spherical camera is separated into two camera halves to eliminate the low resolution band.

FIG. 11A illustrates the addition of a chassis Intrusion detector system using transparent conductive films encapsulating the entire tablet computer, FIG. 11B illustrates the case where the film encapsulation film in inside of the housing and FIG. 11C illustrates the case where a matrix of thin printed wires replaces the conductive films of FIGS. 11A and 11B.

FIG. 12 is a schematic of the operation of the chassis intrusion detector of FIG. 11C.

FIG. 13 illustrates the use of liquid crystal glasses which are sequenced with the display to allow the student to see the test but not an observer of the tablet display.

BEST MODE FOR CARRYING OUT INVENTION

Referring now to FIGS. 1-7, this embodiment of the disclosure does not require a special laptop computer to facilitate secure test-taking. Rather, in this embodiment, the test-taker can use a tablet computer or other non-specialized computing device. However, other components are required including a head-mounted apparatus and an equipment tower 20.

Tower 20 may be generally considered a structure that provides an elevated platform above the computer being used for test-taking, not shown in FIG. 1. As shown in FIG. 1, the tower 20 includes a vertically oriented support 22 into which a processing unit 24 is mounted. The tower also has a camera assembly 26. The processing unit 24 controls the testing process, in a similar manner as described above. The support 22 may be a tripod configured to rest on a horizontal surface such as a table, or the floor in the vicinity of the computer being used for test-taking. When placed on the floor, the support 22 may be configured to be collapsible, in the same or a similar manner in which a camera tripod is collapsible, and the support may be from about 5 to about 6 feet high. When configured for table-top placement, the height of the support 22 would be less.

The camera assembly 26 may be composed of 4 imagers in a tetrahedron arrangement or two hemispherical imagers when the entire room is to be monitored. Each of the imagers would have a special lens such as a fisheye lens, as illustrated at 28 in FIG. 2 and at 30 in FIG. 3, in order to capture the maximum field of view. Other configurations using more imagers can be used to accomplish full room coverage. It is also possible that for some implementations where full rom coverage is not desired, other imager configurations are possible. When the tetrahedron camera assembly is provided, it can have its corners removed since there is no reason for them to extend beyond the camera. Instead of associating a fisheye lens with the imager 28, other types of lens may be used. Indeed, since a square imager may be used in the disclosure and fisheye lens are often round, accommodations to address this shape different will be utilized.

In addition to camera assembly 26, other cameras may be arranged on the support 22 to view the area around the computer being used for test-taking and/or the test-taker. One camera might be optimized for viewing the computer while another might be optimized for viewing the test-taker. The specific camera location of these other cameras may depend on the structure of the support 22 or the camera on the computer may be used. However, as shown in FIG. 1, the camera assembly 26 is preferably mounted at a top of the support 22.

The dual camera 30, the outline of which is shown in FIG. 3, may be used instead of the tetrahedron camera assembly. Such a dual camera 30 could likely provide a full spherical image. Details of this aspect are set forth in U.S. Pat. No. 7,161,746.

The processing unit includes a connection port to enable a cable to extend from the processing unit 24 to the computer being used for test-taking. This cable may the only connection between the processing unit 24 on the tower 20 and the test-taking computer. The cable may extend through an aperture 32 in a transducer board 34 shown in FIG. 4. Transducer board 34 may be part of the processing unit 24. This cable may be a USB cable with appropriate connectors placed on the computer and the transducer board 34 to enable correct engagement. Another USB cable may also be provided to connect to an ultrasonics board 36 shown in FIG. 5. The ultrasonic transducers making up the sensor array are connected to the ultrasonics board 36. The ultrasonic sensor array is an example of a motion sensor that may be used to monitor movement in the vicinity of the test-taker, and other motion sensors of course may be used. Instead of cables, wireless connections may be considered.

FIG. 6 shows the connection of the transducer board 34 and the ultrasonics board 36 via mating 12 pin connectors 38, 40. The support 22 can also include an angle sensor (not shown). In combination, the camera 26, ultrasonic sensor array and angle sensor monitor the environment surrounding the test-taker. Other types and combinations of environment monitoring systems and sensors may be used in accordance with the invention. The support 22 may also include one or more sound sensors and/or one or more sensors for detecting RF communications that can reach the test-taker. These sensors may alternatively be provided on another unit.

Use of this embodiment would involve the test-taker accessing the test-providing website, as described above, and proceed to take the test using their computer in the vicinity of the tower 20. The tower 20 would monitor the presence of other people in the vicinity of the test-taker, some communications toward the test-taker, verify the identity of the test-taker, etc., basically a subset or all of the features performed by the computer and arrangement described above with respect to FIGS. 1-5. One or more biometric sensors or other identity-verification sensors or systems may be coupled to the processing unit 24, and may even be integrated into the computer.

Although this configuration essentially provides all of the same features as the special laptop implementation, it has the feature of not requiring the purchase of the special computer. Instead, the test-taker can use his or her own computer and purchase a less expensive tower which contains all of the decryption and security features which were added to the laptop computer. The tower 20 can be protected using a chassis intrusion detection system as described below, but a display is still needed, unless the test-taker's computer is a tablet computer which is docked to the tower as described below. If the monitor is separate from the tower, then the problems related to securing the display signal described above come into play. Even if it is docked to the tower 20, it too would need chassis intrusion detection or the tablet can be modified to transmit the display image to another room. Alternatively, the display can be made an integral part of the tower 20 and the vulnerable parts of the total assembly properly protected with a chassis intrusion detector (CID).

Another embodiment of the invention which may be used in combination with the tower 20 or without the tower 20 is to use a frame that is worn by the test-taker on their head, i.e., head-mounted, and provides a screen, not shown, in front of the test-taker's eyes. As shown in FIG. 7, this frame includes a housing 44 that has the screen and a strap 42 that straps the housing 44 around the user's head. Such a device is commercially available as an Oculus Rift™. An advantage of the use of a frame that is worn by the test-taker is that only the test-taker can view the material being displayed. As such, it is virtually assured that no one else can provide assistance to the test-taker after viewing the display screen that displays the test, providing the decryption is accomplished within the device and the electronics are protected with a chassis intrusion detector as described below. The tower 20 with the RF communication sensors and microphones are thus not as important and can potentially be eliminated if a frame-based test-taking system is used. However, since the test-taker may still speak and try to communicate with a consultant, the sound-sensors or microphones 46, whether incorporated into the tablet computer and accessed via a cable connection or incorporated into another structure such as the frame itself, will still be beneficial.

Although the computer being used for test-taking does not require all of the accessories described in the embodiment above with reference to FIGS. 1-5, it can contain a camera or other imaging device and a biometric device, such as a fingerprint sensor. More generally, since the camera can be used for one biometric measurement, the computer can contain at least two systems that enable two biometric measurements 52, 54 to confirm the identity of the test-taker. These two biometric measurements may be obtained via the camera, e.g., a facial scan or an iris scan, and the finger print sensor or by any other combination of two or more biometric measurement devices or sensors. Among others, a palm scanner may be incorporated into the computer, or may be connected to the tower 20 and its processing unit 24 if present. Representation of biometric sensors 52, 54 apart from the processing unit 50 and the housing 44 and strap 42 does not imply that these must be separate therefrom and indeed, they may be arranged, as desired, on any of these components. Also, in some cases when the tower 20 is used, the processing unit 50 may be the same as the processing unit 24 arranged on the tower 20.

The facial scan obtained via a camera used as biometric sensor system 52 may be used to image the pattern of blood vessels in the test-taker's face, in which case, an infrared illuminator should also be used (not shown). The illuminator would be mounted on the support 22. The illuminator could also be used to aid in the facial recognition, if so desired.

Accordingly, one embodiment of a frame in accordance with the disclosure includes, in addition to the housing 44 with the screen and a strap 42, one or more microphones 46 or other sound sensors that sense sound in the vicinity of the frame. Of course, the test-taker might be talking to himself and this talking detected. However, the processor 50 associated with the frame could be configured to require the test-taker to speak to initiate the system and then compare any other subsequently detected sounds to the voice of the test-taker. Detection of a voice other than that of the test-taker would be a good indication of the test-taker cheating by receiving assistance from someone else. This problem is at least partially solved by requiring the test-taker to be quite when taking a test.

A particularly useful arrangement is to incorporate the microphones and RF sensors into the strap 42 or preferably into a device which at least partially covers each of the test-taker’s ears as shown at 46, 48. Two microphones, one at each ear, can additionally locate the source of sound coming to the test-taker as lying in a plane perpendicular to a line passing through both microphones. If a third microphone is provided at the top of the test-taker’s head, also 46, then the location of the source of a sound can be determined. This can be helpful in differentiating sound from a consultant from road noise in a city, for example. Similarly, the use of three RF sensors can pinpoint the source of the RF transmission and if that source is located on the body of the test-taker, then this becomes significant evidence that there is another device being worn by the test-taker which is communicating with a consultant. Such devices are available today to assist students in cheating on tests.

Another way for the test-taker to cheat while wearing the frame would be to type questions onto a smartphone or a second tablet or other type of computer, or provide this smartphone or computer with voice-recognition that converts the test-taker's speech into a communication. To prevent this type of cheating, the tower 20 or tablet computer being used for test-taking should be configured to detect communications. He or she might use another device to type in questions such as a smartphone hidden from the cameras.

More importantly, for the reasons described above, in order to guarantee that the biometric measurements have not been compromised, at least one of the measurements should be accomplished on a secure device which is CID protected and which contains the private key. Since the private key should be adjacent to the display which is on the frame, the biometrics measurement system also should be housed on the frame. If a camera is mounted on the frame so that it has a clear view of one of the test-taker’s eyes, then an iris scan can be easily accomplished. Since the iris scan is among the most reliable of the biometric measurements, this may be sufficient. If a second biometric measurement is desired, then the same or different camera can perform a retinal scan or a scan of the blood vein pattern around the eye. Also a second camera can be provided to check the second eye. This eliminates the need for this hardware to be part of the computer or a tower. Now, any computer can be used by the test-taker for test taking. The test is decrypted just as it enters the display and the display can only be seen by the test-taker. The private key and test-taker’s biometrics are stored in a CID-protected assembly on the frame adjacent to the display. Microphones are provided to detect any talking by the test-taker and a sound creator to test the microphones. Two problems remain which will be addressed below. A camera can be mounted within the frame which captures the images and transmits them to another room and the test taker can be typing messages to the consultant on the keyboard or other device.

The foregoing reveals that while a test-taker's tablet computer could be used for secure test-taking, it must be CID-protected and configured to improve detection of possible cheating. Some tablet computers are dual-mode tablets that allow for a limited operating system, which limited operating system could be used for test-taking, whether solely for test-taking or for test-taking and other purposes. In such a limited operating system, Internet access is restricted, among other things. Such tablet computers would ordinarily include a camera and software capable of performing a photographic-based fingerprint and an iris scan (and/or facial vein pattern or retinal scans) to provide a biometric analysis to confirm the identity of the test-taker. As long as the tablet display is not seen by a consultant then this can be a good system. However, as discussed above, it is almost impossible to prevent the display from being observed. Also, no tablets are believed to be on the market with CID-protection, so this will need to be a specially designed device. It has been proposed to attach this to the tower as shown in FIG. 8A.

A first configuration for an arrangement for secure test-taking using a dual-mode tablet computer therefore includes configuring the dual mode tablet computer 56 for use for test taking while having the limited operating system. The tower 20 is provided in a room or other area in the vicinity of the tablet computer 56, and the tower 20 is provided with the ultrasonic sensor array embodied by ultrasonics board 36, or comparable ultrasonic unit, and the camera 26, e.g., a spherical camera. In addition, a head-mounted frame is provided to the test-taker and includes one or more communication-detecting sensors 48 on the housing 44 and/or strap 42 and one or more sound-detecting sensors 46 on the housing 44 and/or strap (see FIG. 7). A fingerprint biometric sensor 52 is also provided, e.g., as an attachment to the tablet computer 56 or connected to the processing unit 50. Finally, a biometric sensor 54 capable of detecting and analyzing an iris scan (and/or facial vein pattern or retinal) to provide a biometric analysis to confirm the identity of the test-taker is also included. This may be an attachment of the tablet computer 56 or an attachment to the processing unit 50 which is inside of tower 20.

Advantages of this configuration include the limited required modification, if any, to the tablet computer 56 of the test-taker (since the hardware can be implemented in the tower 20 or connected by cable of the tower 20), and the relatively low cost. Also, the equipment to construct the tower 20 is readily available. Disadvantages include the difficulty in monitoring the test taker's peripheral vision and the ability for a consultant to view the display of the tablet computer 56.

A second configuration involves use of a more specialized frame worn by the test taker, such as the headgear referred to as the Oculus Rift™. This headgear is significantly more complicated and expensive relative to the simple frame including the communication-detecting and sound-detecting sensor(s) in the first configuration. Yet, the Oculus Rift™ could be modified, if necessary, to include one or more communication-detecting sensors 48, if desired, and one or more sound detecting sensors 46. The communication-detecting sensors 48, as well as any other communication detecting sensors or systems disclosed herein, may be radio frequency communication detecting sensors or systems The tower 20 can also be used in this embodiment with the ultrasonics capability and camera 26. The fingerprint biometric sensor can be used as well. Finally, either the iris scan sensor is used before the Oculus Rift™ is put on, or a separate biometric sensor is used to validate the identity of the test-taker, e.g., a voice print, typing pattern, palm scan, and face recognition-based system.

Advantages of this configuration include the ability to combine it with gaming hardware (the primary development purpose of the Oculus Rift™), thereby reducing combined system cost and increasing market potential, the inability for a consultant to the test-taker to view the display (which is inherently only visible to the test-taker wearing the Oculus Rift™), visual input from the consultant is effectively eliminated and a tower 20 is optional. Disadvantages include the fact that the Oculus Rift™ is currently expensive, touch typing skill is required for textual input and some students will experience nausea from use of the Oculus Rift™. Another product with similar properties is The Vuziex Wrap 1200 video eyewear as described at http://www.vuzix.com/consumer/products_wrap_1200/.

Yet another configuration includes a Google Glass™ type display. In this case, the frame worn by the test-taker is Google Glass™ which can be equipped with one or more radio frequency communication-detecting sensors 48, if desired, and one or more sound-detecting sensors 46.

Advantages of this configuration include the fact that a consultant cannot view the display as only the wearer of Google Glass™ can see the display, the frame has other uses than just test-taking (any other uses for Google Glass™) and thus reducing system cost and increasing market potential, eye tracking is available to control student's peripheral vision, gesture input can be an option for answering questions on the test being taken, and a tower is optional. A disadvantage is that Google Glass™ is currently expensive.

Yet another configuration is possible in which the strap 42 and/or housing 44 include a total of four cameras with fish eye lens or comparable lens that are positioned to provide the same field of view as the cameras 26 mounted on the tower 20. In this case, again, the tower 20 can either be eliminated or its components reduced since the optical imaging hardware is now provided on the head-mounted apparatus of the test-taker.

Let us now consider in detail some of the components of the invention and variations thereof. FIG. 8A illustrates the use of the tower 20 to hold and position a tablet and to serve as a docking station for the tablet 56. The tablet 56 when inserted into the holding ledge 52 automatically connects a USB hub to the micro USB port on the tablet. This hub is used for attaching a cable from the goggles or glasses, a mouse and a keyboard if provided.

Although the spherical camera is shown as comprising two imagers and lenses, an alternate approach is to provide a linear array which rotates in order to capture the spherical image. Whichever camera is used, it can be vertically positioned using a small motor which moves the camera vertically upward and downward in order to provide the optimum camera location.

FIG. 8B illustrates an alternate approach where the tablet 50 is placed on a table 54 and connected by a wire to the tower 20.

FIG. 9 illustrates the use of a Google Glass™ type device 60 in place of the Oculus Rift™ device of FIG. 7. The Google Glass™ device 60 contains a head camera 62 as described elsewhere. One problem with the Oculus Rift™ implementation is that it would be relatively easy to mount a camera and transmitter inside the housing 44 which could view the display and transmit its contents to a remote location. This would be quite difficult with the Google Glass™ implementation. On the other hand, the monitoring of the environment in the room becomes more important in the event that the consultant has somehow gained access to the contents of the test and is displaying answers on the floor or ceiling, for example. The microphones and RF sensors are shown here as 64 and 65 respectively.

When a spherical camera comprises two hemispherical cameras, there is likely to be a dead spot in line with the joints between the two cameras. Although this can be made quite small, nevertheless, sometimes it is desirable to eliminate this completely. This can be accomplished as shown in FIG. 10 by displacing the two hemispherical cameras, 72, horizontally as shown in the drawing. They are showing mounted on towers 70. Naturally these cameras can be displaced vertically or in any other configuration that is easy to implement and which provides the best view of the room and test taker.

If the room is dark, it is conceivable that a consultant can be positioned in the room in such a manner that his presence is not detected by the spherical camera. In such a case, the consultant might be positioned in such a location that he or she has a view of the display. In order to prevent the camera from not seeing the consultant in this situation, a small amount of illumination may be provided in conjunction with the spherical camera. This illumination can be in the visual spectrum or, more likely, in the near IR portion of the spectrum. It is expected that if the consultant moves, his presence will be detectable by the ultrasonic motion detector, however if the consultant is very still, this might not occur. Another approach is to provide imagers with long wave IR sensing capability, in which case, the presence of an object whose temperature is above that of ambient can be detected. This system can be defeated when the environment is at a temperature which is at or slightly higher than the temperature of the human body.

Thermal IR motion sensors could of course be used as an alternative to the ultrasonic sensors described above. Such sensors can be fooled by strong sunlight heating a surface in the room, a cup of coffee, and, as mentioned above, when the ambient temperature approaches body temperature. Ultrasonic motion sensors provide an easier method of locating the source of motion in a room, estimating its size, and permitting pattern recognition systems to identify the object causing the motion. Although these can also be accomplished with thermal IR sensors, the cost and complexity is considerably higher.

A further solution is to require that the room where the test is being taken have adequate lighting. Even it that case, there may be areas which are shaded from the light.

Consider now the camera which is worn by the test-taker 62. This camera can be designed to snap on to any appropriate glasses frame allowing the student which normally wears glasses to apply the camera to his or her glasses frame. The head camera typically will have a field of view which is substantially less than the field of view which the student can see by moving his eyes to one side or the other or up or down. Thus, the student may be able to observe signals which are not seen by the head camera. This requires that the head camera be designed to have a wide field of view and may also require that the glasses worn by the students contain shades which prevent the student from observing areas which exceed the field of view of the head camera. The tablet-mounted camera can be used to ascertain that the student is properly wearing his or her glasses so as to prevent momentary displacement of the glasses and head camera to allow for a temporary peripheral glance by the student.

As mentioned above, the glasses containing the head camera can also contain RF sensors 65 and microphones 64. Normally, two RF sensors and two microphones will be used; however, if it is desirable to locate the direction of a source of sound or radio frequency, then a third microphone and a third RF sensor can be provided at a convenient locations such as on top of the headset, as discussed above, of the student but connected to the glasses where the other sensors are located. By triangulation, therefore, the source of either sound or radio frequency at a particular sensed frequency can be located. The sound, for example, may be coming from immediately behind the student where a consultant has positioned himself in such a way as to not be observable by the cameras and yet still have the ability to see the display and therefore to help the student with the correct answer. Similarly, the RF source may reside on the student’s body as used in a commercially available cheating system. All of the devices which make up a headset can be multiplexed into a single USB cable which then can be plugged in to the tower as provided.

Previously, secure test taking apparatus employing an inexpensive tablet have not been available. What follows will now discuss a preferred embodiment of such a secure tablet. A tablet geometry has advantages over alternates such as a desktop or laptop computer as will become evident.

A fingerprint sensor may or may not part of the tablet and thus a separate fingerprint sensor peripheral may be required as a first biometric device. If the second biometric device is an iris scanner, face recognition scanner, hand geometry scanner, or other system utilizing a camera, the tablet resident web camera may be sufficient for any of these biometric information gathering purposes. For example, the student may be requested to place his iris within 3 inches of the tablet resident camera for the purpose of obtaining an iris or retinal scan or hold his hand 6 to 8 inches from the camera.

The fingerprint scanner may be a conventional system where the student swipes his finger across an aperture and the number and spacing of the ridges in the scanned area are recorded and processed typically by counting the ridges. This has been found to be relatively easy to fool by using a picture of a fingerprint, for example, or by merely trying a large number different fingerprint pictures. Also, if access to the computer can be obtained the recorded fingerprint can be hacked or the fingerprint can be obtained when the student allows it to be measured by another computer and then a photograph produced and used in the testing computer. If access to the internal circuitry of the computer is permitted or even just to the fingerprint scanner, then a previously recorded signal reprehensive of the student can be substituted for the actual scan.

An alternate and preferred design makes use of the tablet rear camera and the student places his or her finger at a directed position and the finger is photographed. This theoretically could also be fooled by the use of a picture so the finger can be monitored over a few seconds to determine that a pulse is present using methods such as amplifying the motion or the color of the finger as disclosed in: “Software Detects Motion that the Human Eye Can't See”, Conor Myhrvold, MIT Technology Review, July 24, 2012; “Seeing the human pulse”, Larry Hardesty, MIT News Office, June 19, 2013; and, “Guha Balakrishnan, Fredo Durand, John Guttag, Detecting Pulse from Head Motions in Video, presented at the IEEE Computer Vision and Pattern Recognition conference, 2013. More of the finger print can be captured by this method making it more accurate and difficult to fool than the fingerprint scanner. Also multiple fingerprints can be simultaneously acquired.

Due to the high stakes involved in the granting of degrees by prestigious universities, it can be expected that attempts will be made to alter the tablet so as to permit information which normally resides only within the tablet to be transferred elsewhere. This will require breaching the chassis of the tablet. Several chassis intrusion sensors have been developed such as a light sensing sensor which records an incident if the cover of the tablet has been removed and any light is present, or a mechanical switch or other electrical connection that is disrupted upon removal of the tablet back. Although in some cases, these chassis intrusion sensor will be difficult to defeat, in all cases a conventional chassis intrusion sensor can be defeated. For example, if a light sensor is used then the cheater can buy one laptop and locate the light sensor and then in a second laptop he can remove the cover in a dark room and place tape or spray black paint over the light sensor thereby defeating it.

The first and easiest step in preventing chassis intrusion is to replace the screws, when screws are used to attach the back, with fasteners which cannot be readily removed. This can be done in the case of screws by removing the present screws and replacing them with screws that when screwed in and a threshold torque is obtained, then the screw breaks off of the driving shaft. Secondly, a tape can be securely attached to the joint between the cover and the remainder of the tablet with an adhesive such that the tape must be broken in order to remove the cover. If the tape has encoded within the tape a complicated code which can be read by the tablet and if this code cannot be read or otherwise hacked and is destroyed during the removal of the tape, then intrusion by cover removal can be detected and thus prevented. There still remains the possibility of slicing through the cover without moving the screws or disturbing the tape. In this extreme intrusion method, therefore, the entire back of the tablet can be covered with a film which contains a distributed code in such a way that the breach of any portion of the film alters the code and can be detected by the tablet.

Another such area wide chassis intrusion detector (CID) device is depicted in FIG. 11A which illustrates a film which contains two closely spaced conductive films. The capacitance between these films is measured and monitored by the tablet. If any attempt is made to breach this film, it is likely that one of the conductive layers will be shorted to the other which even if it happens momentarily, can be detected. If one of the films is carefully removed, which would be extremely difficult, then again the capacitance between the two films would be detectably altered. The two films can reside within a thicker plastic assembly such that damage to the films through normal handling of the laptop would not be likely to occur.

A key complement of the chassis intrusion detection systems described below is the use of a small microprocessor and RAM assembly along with a small battery. The battery is connected to the microprocessor through small diameter wires. This assembly is potted such that any attempt to disassemble the assembly will break one or more of the wires connecting the battery to the microprocessor. The microprocessor interrogates the capacitance of the intrusion protection film such as once per second. The battery has sufficient stored energy to power the microprocessor for a long period such as 10 years. The assembly can also be connected to the laptop battery which would then maintain the 10 year battery fully charged. If the volatile RAM loses power, which can happen either through a command from the microprocessor if the capacitance of the film has changed or if the ten-year battery has been disconnected, the contents of the RAM memory will be erased. This RAM memory upon construction of the laptop for test taking purposes would contain the private key associated with that laptop.

Starting with a standard off-the-shelf tablet computer such as the Tegra note. http://www.newegg.com/Product/Product.aspx?Item=N82E16834099001, the RAM, microprocessor and battery assembly is built into a small assembly hereinafter call the security assembly (SA) as shown at 114 in FIG. 12, which plugs in to one of the available ports such that it can be accessed by the tablet CPU. This assembly is also inside of a film envelope and connected to the leads of the conductive layers of the film. Assembly of this system to the tablet is as follows, as illustrated in FIG 16A:

1. Place the tablet inside the envelope and plug in the SA.
2. Fold over the flap of the envelope and make sure that power and micro USB ports are adjacent an opening in the envelope provided for that purpose.
3. Activate the SA using available wires to load the private key and burn the fuse links.
4. Fold over the envelope flap so that it overlaps with a portion of the rest of the envelope.
5. Apply heat to shrink the envelope around the tablet.

The final assembly can therefore be totally encapsulated with the film and the only openings to the outside world would be the power and micro USB ports provided. Some care should be exercised to make sure that these ports cannot be compromised. Special operating system software can be loaded and designed so that it cannot be compromised. The key to this system is to have a film which is transparent so that it does not interfere with viewing the screen. This can be eventually done using graphene but for now indium tin oxide can be used to form the conductive film layers.

http://en.wikipedia.org/wiki/Transparent_conducting_film.

In FIG. 11A, the tablet computer prior to assembly of the encapsulating film is shown at 80. The two layer conductive film is embedded in the plastic film envelope 82. The SA is depicted at 86. In reality, the SA will be quite small such as occupying a volume of 10 mm^3 or less. The final assembly is depicted at 84.

FIG. 11B illustrates the back cover 96, the motherboard and display assembly 92 and the front cover 94 of a standard off-the-shelf tablet computer as illustrated in FIG. 11A. In this case, the SA 86 is packaged with the tablet cover but inside of the CID film. The film 82 is glued to the entire back cover of the tablet and extends slightly outside of the area of the cover as depicted at 90 and in more detail at 90A. The SA 86 is attached to the film and plugs into the motherboard. When the cover is attached to the remainder of the tablet, it is firmly glued or heat sealed in place so that once attached, the cover cannot be removed from the remainder of the tablet without destroying the cover as shown at 96. The film is arranged so that it is also glued to the interface and partially to the area above the interface. Thus any attempt to breach the tablet will damage the film. In FIG. 11B, the glue is depicted at 99.

In FIGS. 11A and 11B, the film 82 contains two layers of conductive film arranged in close proximity to each other with approximately a spacing of 0.001 inches and covered by a thicker plastic film of approximately 0.02 inches on each side resulting in a total thickness of approximately 0.043 inches. An alternate construction is to use a pattern of small conductive wires which can, for example, be 0.005 inches wide with a similar spacing between the wires as shown in FIG. 11C. In FIG. 11C, the front cover is depicted at 102, the interior circuitry at 100, the SA at 106 and the back cover at 104. Typically, these wires will appear in pairs and will meander throughout the film. The SA 106 will be connected to the ends of these wires and continuously monitor their resistance and mutual inductance. If there is any change in the geometry of these wires in the mash after assembly of the cover to the tablet, then this will be sensed by the SA and the RAM memory will be erased thereby destroying the private key. The mesh of wires depicted in FIG. 11C can be economically produced by xerographic techniques resulting in a very low cost chassis intrusion detector system.

To summarize, any disruption of the mash or conductive film in either of the above described examples will destroy the private key making it impossible to decode the test questions. After the assembly is completed, the computer can be powered on and the first step would be to measure the inductance, resistance, and capacitance of the mash or films. Thereafter, if any of these measurements significantly change, then the circuit in the SA would remove power from the RAM thereby destroying the private key. Since the private key cannot be reloaded, the assembly would need to be returned to the factory for remanufacture.

The electronic circuit which powers the CID system of FIGS. 11A-11C is illustrated in FIG. 12. An embedded microprocessor is powered by a 10 year battery and contains a RAM memory. The RAM memory contains the private key encryption code needed to decrypt the test questions. The microprocessor continuously monitors the wires on the CID and if there is any change in the resistance, mutual inductance or capacitance in the circuit, the microprocessor disconnects power from the RAM and the private key is erased.

FIG. 12 is a schematic of the system of FIG. 11C shown generally at 110. Power is supplied from the tablet at 120, the fine wire maze at 116, the SA at 114 the long life battery at 118 and the RAM memory at 112.

A determined cheater still has one route open for getting the assistance of a consultant. Since the tablet display can be observed optically, a consultant may position a camera with a telephoto lens somewhere in the room or on or through a wall that can view the tablet screen. Alternatively, the student may wear a hidden camera, which is not observable by either the spherical camera or the tablet Web camera, which can monitor the tablet display. Such a camera, for example, may be worn around the neck of the student and view the screen through a very small opening in the shirt or blouse worn by the student. These two types of cameras can be disguised in such a manner that it is virtually impossible for the system monitoring cameras to detect their presence. Nevertheless, either of these cameras can transmit the contents of the tablet screen to a consultant in another room, for example. A solution to this final problem rests in scrambling the display and providing the student with a special pair of glasses which descrambles the display. Many techniques are available for accomplishing this task and one will now be explained.

Modern displays refresh the screen at 240 Hz. Since the text on a test changes very slowly only a small portion of this information need be seen by the student. For example, if the screen displays constantly changing images which are very similar to the text on the test wherein only 5%, for example, of the images represent the actual test, then anyone observing the screen through one of the aforementioned cameras would see a blur of constantly changing text. If the student wears a set of glasses illustrated at 130 in FIG. 13 where the lenses are made opaque through liquid crystal technology, then the lenses can be made transparent only during the 5% of the time that the display presents the actual test questions. Such glasses are commercially available consumer products which are used for 3-D television viewing. For an example of such glasses see http://www.dimensionaloptics.com/Panasonic.aspx. The particular frames that contain the actual test questions can be randomized and the random code indicating which frames are to be seen can be sent to the glasses control module in an encrypted form, also protected with a CID system, such that only the glasses worn by the student know which frames to view.

If the hidden camera image capture apparatus used by the consultant is sufficiently sophisticated, each frame could theoretically be captured and thus the consultant could see all of the frames and if it was obvious which frames contained the actual test questions than the consultant could discard all the irrelevant images. It is therefore important that there be no obvious clue as to which images contain the actual test questions and remaining images must look very similar with only slight differences.

FIG. 13 illustrates the glasses worn by the student, shown at 130, allowing the student only to see the test questions. These glasses are designed to fit over prescription glasses and can be part of the headset which contains the microphones, head camera and RF sensors. Glasses 130 may be the device protected by the intrusion detection system described above.

Goggles such as those produced by Oculus Rift™ can be used to provide a measure of secure test taking but they can by defeated if a small camera is positioned either through attachment to the inside of the goggles or through attaching via adhesive, for example, to the face of the viewer. This camera could then watch display on the Oculus Rift™ goggles and broadcast that display to a consultant. If the tower and spherical camera are not present, then the consultant could easily reside within the test taking room to offer assistance to the student. Other methods of capturing the display information are also possible involving splicing additional wires into the Oculus Rift™ hardware. This can be counter-measured through the CID. However, to detect all possible methods of extracting display data from the Oculus Rift™ goggles or equivalent is possible, but can be a daunting task.

The use of display glasses such as Google GlassTM is somewhat more difficult to hack and therefore more secure. The tablet camera, for example, can monitor the face of the student to determine that there are no hidden imagers watching the display. There still remains the possibility of capturing information in the wires to the display but through placing a microprocessor within the display and feeding only encrypted display information through the wires, the chance of this happening is minimized. The disadvantage of the display glasses rests in the fact that the student can still see potential information sources that would be unavailable to the goggles wearer.

Another approach replaces the tablet with a tower which contains the central processor normally resident in a tablet. This tower does not have a display and can be built as a totally sealed unit which cannot be opened without destroying the tower housing. Various methods of detecting housing breach using a CID system as discussed above can be implemented more easily with such a tower than with a laptop or tablet which is designed to be serviced. This can be a relatively secure system and it can interface with a tablet, goggles or display glasses as desired.

It is expected that the process of teaching using the Internet and testing using the concepts herein involves some monitoring of the test-taker including feedback from the test-taker. Also, pattern recognition analysis can be employed more and more to understand the particular students understanding of the course being taught. Eventually, this could result in the elimination of quizzes and tests and the feedback of the progress of the student through the course will lead to an accurate assessment of the degree to which the student has mastered the subject matter. The degree to which the student is motivated to master the subject matter ought to be detectable and thus his success in such mastery also detectable even without the use of the testing system described.

Some important features of this invention differentiate it significantly from prior art attempts to develop secure testing systems. These include:

1. Control over the ports of the computer through a secure operating system to prevent the attachment of devices which can support the transfer of information out of the computer to a nearby or

remote site which can thereby capture the information displayed on the monitor. This control is done through the operating system when the computer is operating in a secure mold which is different from the standard operating system.

2. The use of a spherical camera which allows monitoring of the entire space surrounding the student to detect the presence of helpers or of changing text which can be used to transmit information to the student.

3. The ability to detect the existence of a consultant who would be out of the view of the typical camera which is present in a laptop or tablet. This is done through an array of one or more ultrasonic motion detectors, a variety of cameras and illumination where necessary.

4. The use of strong encryption coupled with the protection of the private key which cannot be extracted from the computer thus requiring that the student use a particular computer for taking tests.

5. The use of a chassis intrusion detection (CID) sensor or system which renders the physical breach of the computer chassis virtually impossible without destroying the private key needed for test decryption.

6. The detection of sound adjacent the ears of the student such that anything that can be detected by the student's hearing can also be detected by the microphones.

7. The placement of RF sensors adjacent the student's ears such that any RF communication to the student and in particular to an earpiece which the student may be wearing can be detected. This defeats a common system used in China for cheating on tests.

8. Visual cues from a consultant which may be displayed out of the view of a standard tablet or laptop camera are detected by the spherical camera system and by the head camera disclosed herein. In particular, the existence of notes, a hidden tablet, or smart phone which the student can view will also be detected by the system of this invention.

9. The location of audio and RF signal sources at known frequencies can be determined to indicate whether those locations are within the room occupied by the student.

10. The detection, for example, of a smart watch or other similar apparatus which can be hidden from view of a tablet or even the spherical camera but can be detected by the head camera.

11. The use of sophisticated neural network based pattern recognition algorithms which allow for continuous improvement of this system as new cheating methods are discovered. This allows for upgrading the software of the system as new improvements are implemented. These neural network systems initially will be used for detecting changing static patterns such as displayed text on a surface such as the ceiling of the room, but the capability exists for adding the detection of suspicious behaviors on the part of the test taking student.

12. The use of a scrambled display and light valve glasses to permit the contents of the display to be only observed by the student and not capable of being captured in a meaningful way by a camera having a view of the display.

Disclosed herein are a series of measures that are designed to prevent the transfer of test related information to anyone other than the test taking student by any means either visually, electronically, or wirelessly. The measures disclosed herein are not exhaustive and the intent of this invention is to cover preferred implementations of such techniques. Similarly, disclosed herein are a series of measures to prevent information from being transmitted to the test taking student on the assumption that the information about the test has leaked to a consultant. Since the consultant now must transmit to the student information which will affect how the student answers the question, this invention has also not exhaustively disclosed all possibilities of information transferal from the consultant but only representative cases. It is not the intent of the inventor to cover all such transferal means including, for example, haptic methods which have not been discussed above. These include, for example, a wire attached to the student and physically held by the consultant who may in fact be located in another room wherein the wire travels through a hole in a wall. In this case, for example, if the consultant knows the test question and has determined that the proper answer is three then the consultant could pull three times on the wire thereby transmitting this information to the student. All sorts of similar haptic techniques exist including electrically actuated vibrators, spark creators etc. To cover all such possibilities of either the leaks of information out of the test taking device or the communication of information to the student would require volumes. Thus, it is the intent of the inventor to cover all such possibilities while disclosing those that are most readily implemented.

Finally, all patents, patent application publications and non-patent material identified above are incorporated by reference herein. The features disclosed in this material may be used in the invention to the extent possible.

CLAIMS

1. A method for detecting an attempt to physically alter an electronic device, comprising:

enclosing the device in a cover component;

positioning conductive wires in the cover component external to the device;

coupling a security assembly to the wires; then

monitoring impedance of the wires by means of the security assembly; and

when a change in impedance is detected by the security assembly, deleting a required security code needed for use of the device.

2. The method of claim 1, wherein the step of monitoring impedance of the wires comprises monitoring resistance and mutual inductance of a pair of the wires.

3. The method of claim 1, wherein the wires are 0.005 inches wide and spaced apart from one another by 0.005 inches.

4. The method of claim 1, wherein the step of positioning the conductive wires in the cover component external to the device comprises placing the wires in a meandering pattern throughout a film layer.

5. The method of claim 1, further comprising connecting the security assembly to ends of the wires.

6. The method of claim 1, wherein the wires are configured such that a change in geometry causes a change in impedance.

7. The method of claim 1, wherein the step of deleting the required security code needed for use of the device when a change in impedance is detected by the security assembly comprises erasing a RAM memory including the required security code.

8. The method of claim 1, further comprising producing the wires by xerographic techniques.

9. The method of claim 1, wherein the security assembly includes a processor, power source for providing power to the processor and a RAM assembly containing the required security code for use of the device, the security assembly being configured such that any attempt to disassemble the security assembly will break one or more wires connecting the power source to the processor and such that a change in impedance will cause the security code to be erased from the RAM assembly.

10. The method of claim 1, further comprising coupling the security assembly to the device using a port of the device and with the security assembly within the cover component.

11. The method of claim 1, wherein the cover component comprises a front cover and a back cover.

12. An intrusion-protected electronic device, comprising:

a cover component that substantially encloses the device;

conductive wires in said cover component external to the device; and

a security assembly coupled to said wires and that periodically monitors impedance of said wires to determine changes in impedance, and causing deletion of a required security code needed for use of the device based on determined changes in impedance.

13. The device of claim 12, wherein the wires are 0.005 inches wide and spaced apart from one another by 0.005 inches.

14. The device of claim 12, wherein the security assembly is connected to ends of the wires and the wires are configured such that a change in geometry causes a change in impedance.

15. The device of claim 12, wherein said security assembly includes a processor, power source for providing power to said processor and a RAM assembly containing the required security code for use of the device, said security assembly being configured such that any attempt to disassemble said security assembly will break one or more wires connecting the power source to said processor and such that a change in impedance will cause the security code to be erased from said RAM assembly.

16. The device of claim 12, wherein said cover component comprises a front cover and a back cover.

17. The device of claim 12, wherein the device is a headpiece comprising:

a frame having a support portion adapted to be supported on a person's head and a viewable portion adapted to present visual data to the person when said support portion is supported on the person's head;

at least one imaging device arranged on said frame to obtain images of an environment around the person when said support portion is supported on the person's head;

at least one user interface arranged on said frame to receive input from the person when said support portion is supported on the person's head;

a processor arranged on said frame and coupled to said at least one user interface and said viewable portion, said processor being configured to control content of said viewable portion based on input received via said at least one user interface; and

at least one communication-detecting sensor that detects communications,

said processor being configured to monitor detection of communications detected by said at least one communication-detecting sensor and images obtained by said at least one imaging device when said viewable portion is displaying a test to determine whether a person other than the person on which said support portion is supported is present or providing information to the person on which said support portion is supported.

18. The headpiece of claim 17, wherein said at least one user interface comprises a sound-detecting sensor, said processor being configured to monitor detection of sound by said sound-detecting sensor when said viewable portion is displaying a test.

19. The headpiece of claim 18, wherein said sound-detecting sensor is arranged on said frame.

20. The headpiece of claim 17, wherein said at least one communications detecting sensor is arranged on said frame.

21. A method for limiting viewing of content on a display, comprising:

changing images being displayed on the display at a high rate at which viewing the display does not provide a discernible image to a viewer;

equipping a person with a viewing device having lenses that are selectively opaque or transparent; and

controlling the lenses to cause the lenses to be transparent only when determined content is being displayed on the display to enable only a lenses- equipped person to correctly view the predetermined content.

22. The method of claim 21, wherein the predetermined content is a test.

23. The method of claim 21, further comprising randomizing the image frames containing the predetermined content and providing an indication of the randomization only to the viewing device.

24. The method of claim 21, wherein the viewing device incorporates a chassis intrusion detection system.

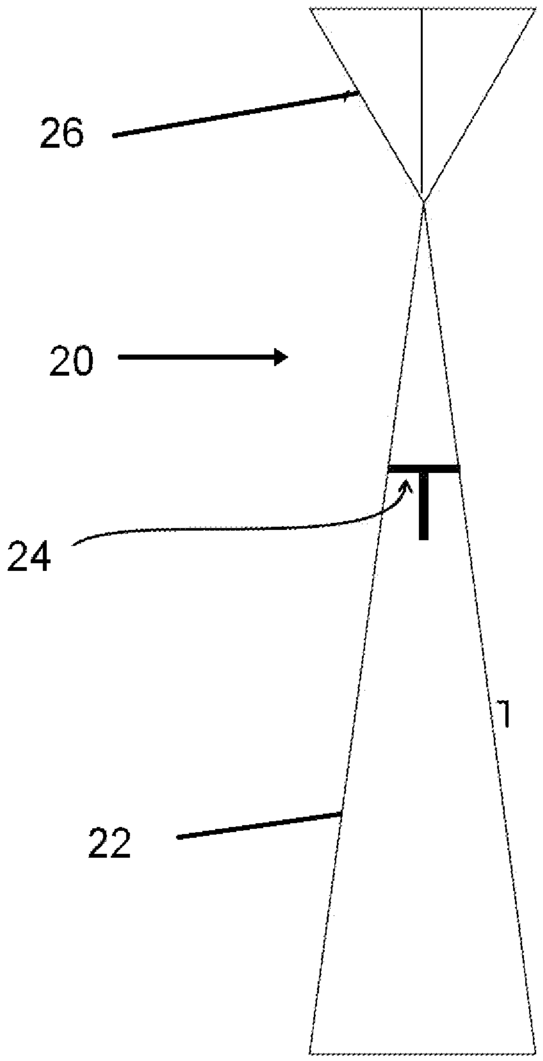
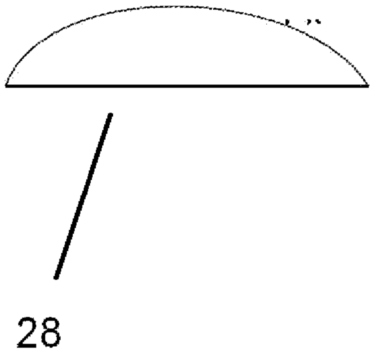


FIG. 1

FIG. 2



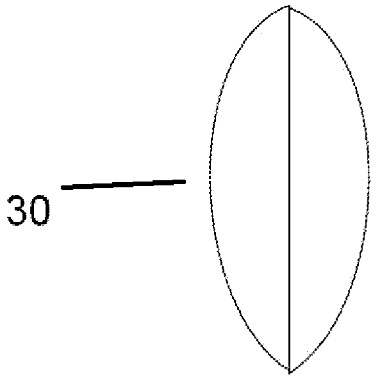
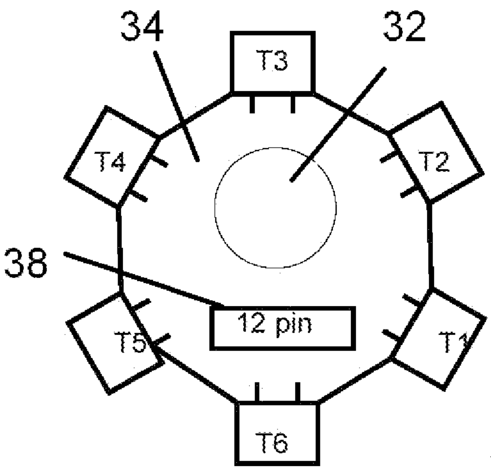


FIG. 3

FIG. 4



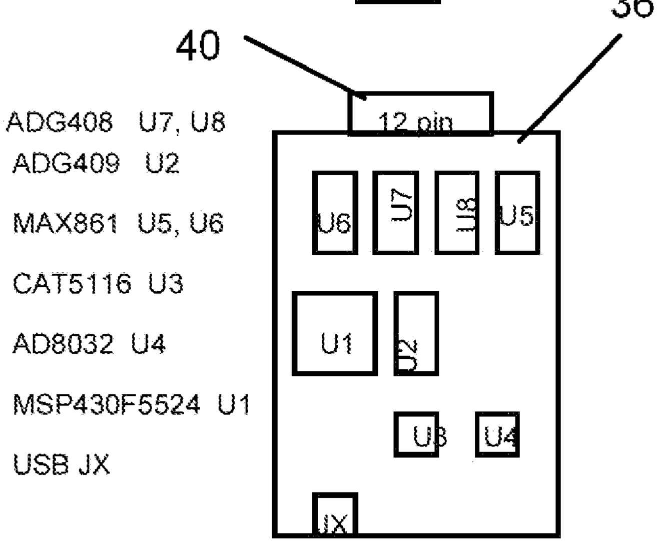


FIG. 5

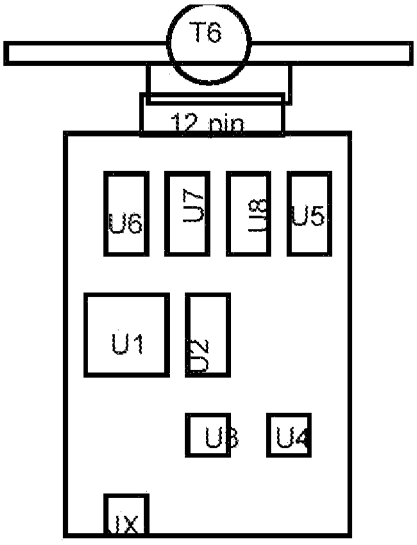


FIG. 6

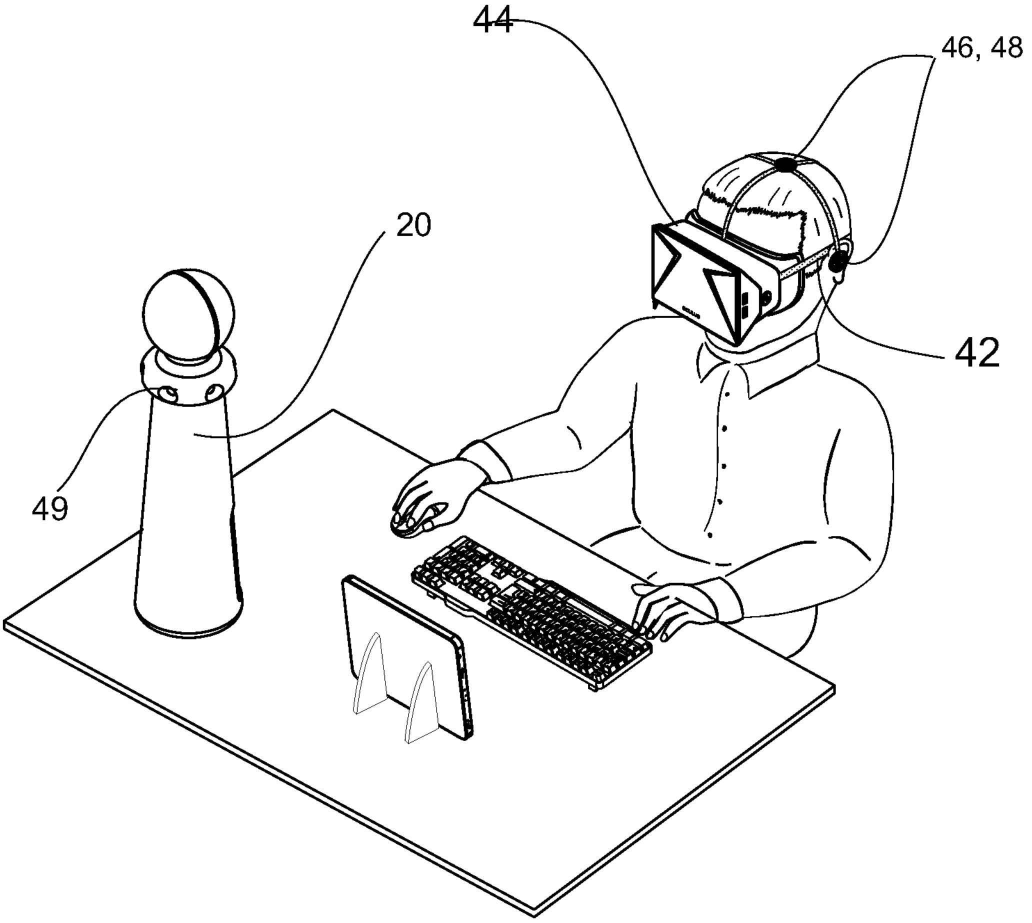


FIG. 7

FIG. 8A

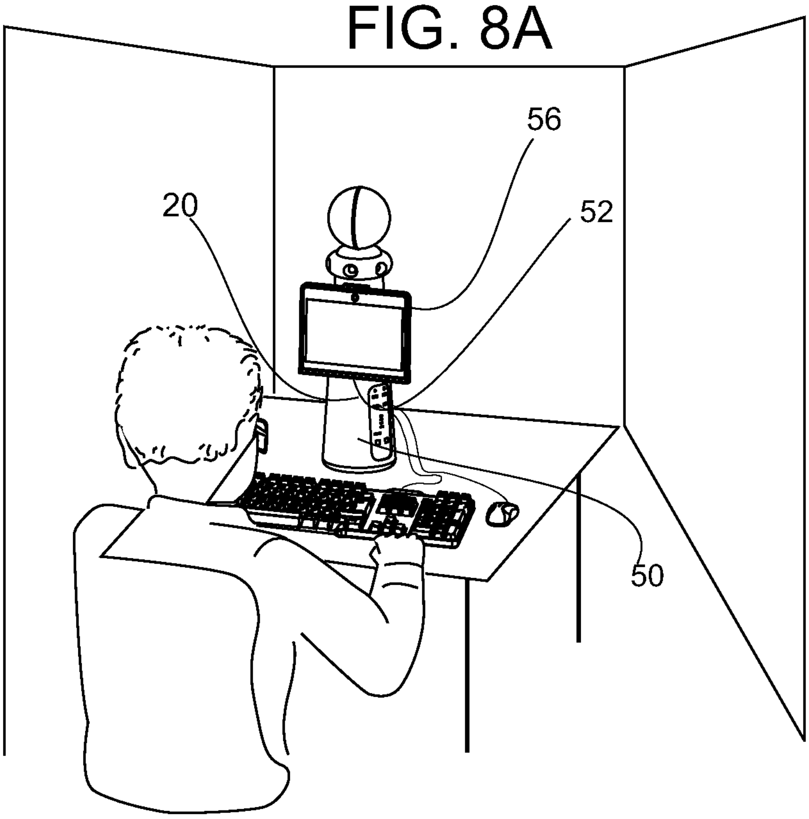


FIG. 8B

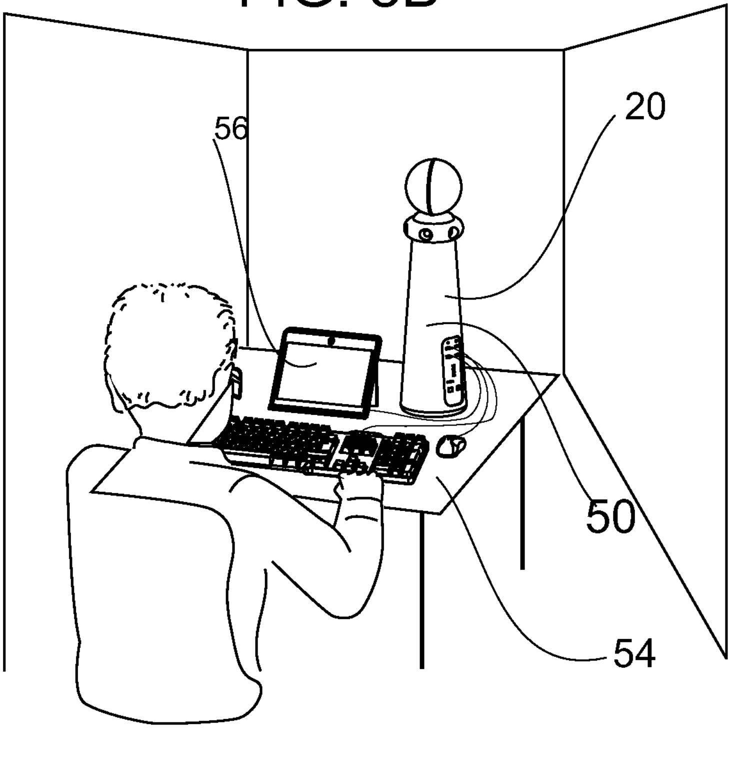


FIG. 9

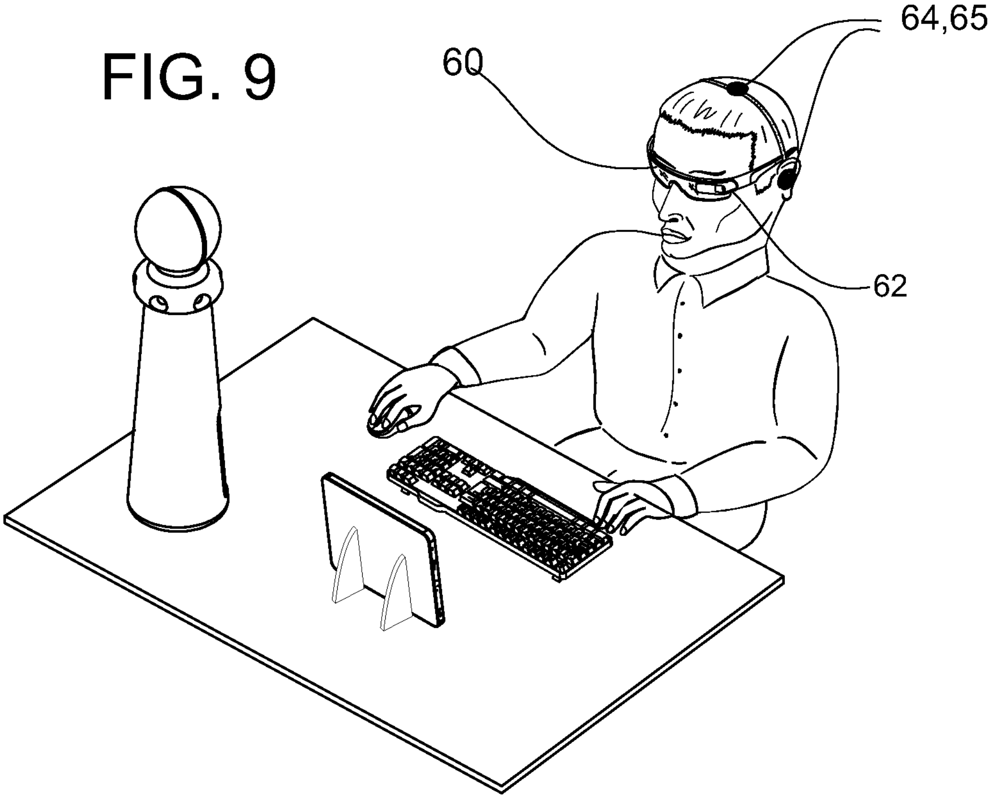
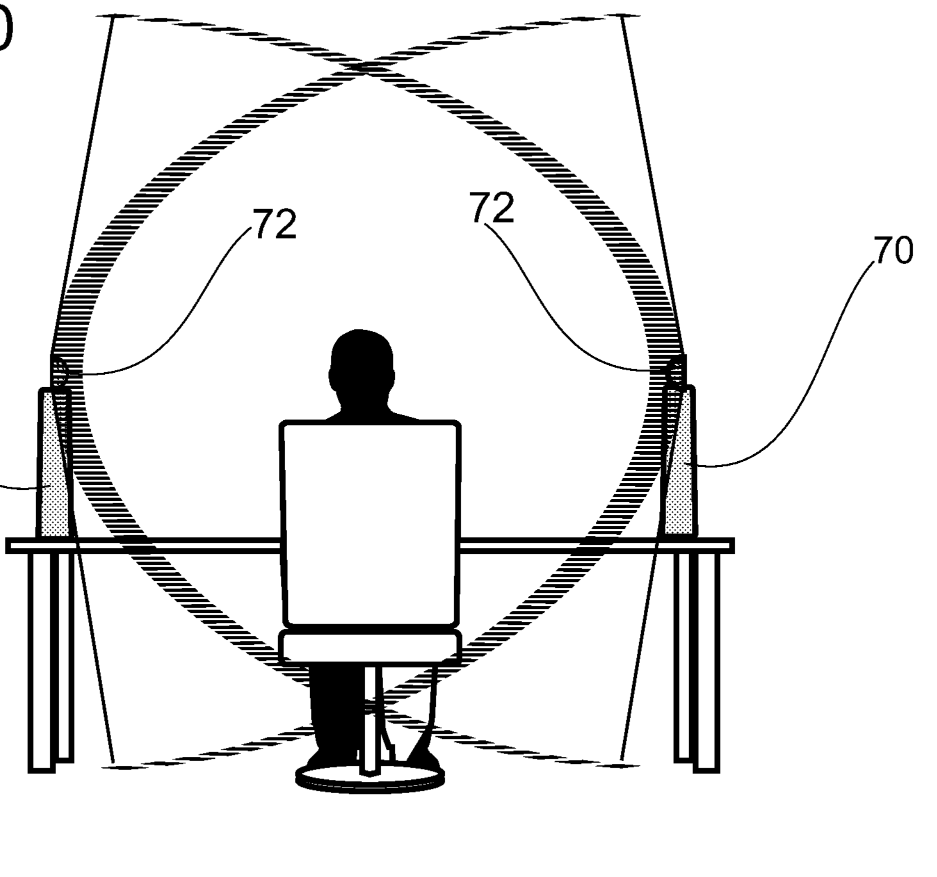


FIG. 10



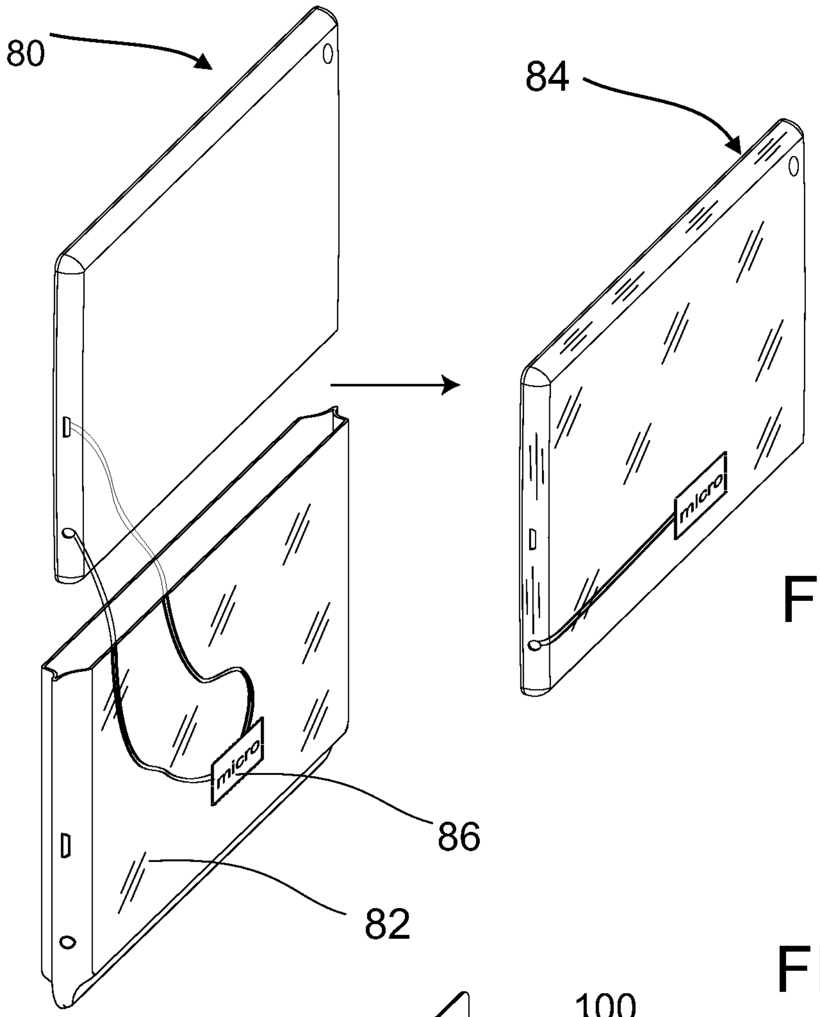
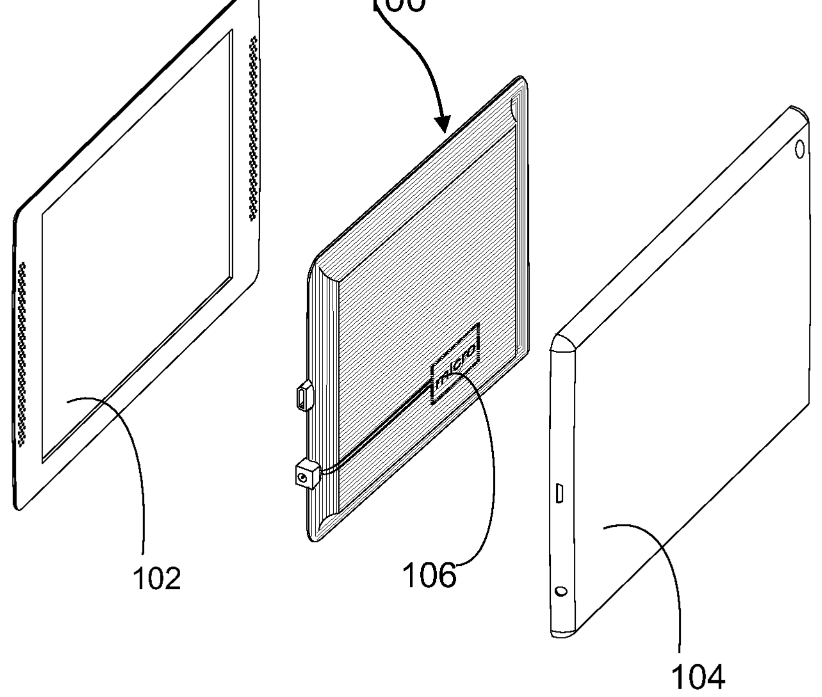


FIG. 11A

FIG. 11C



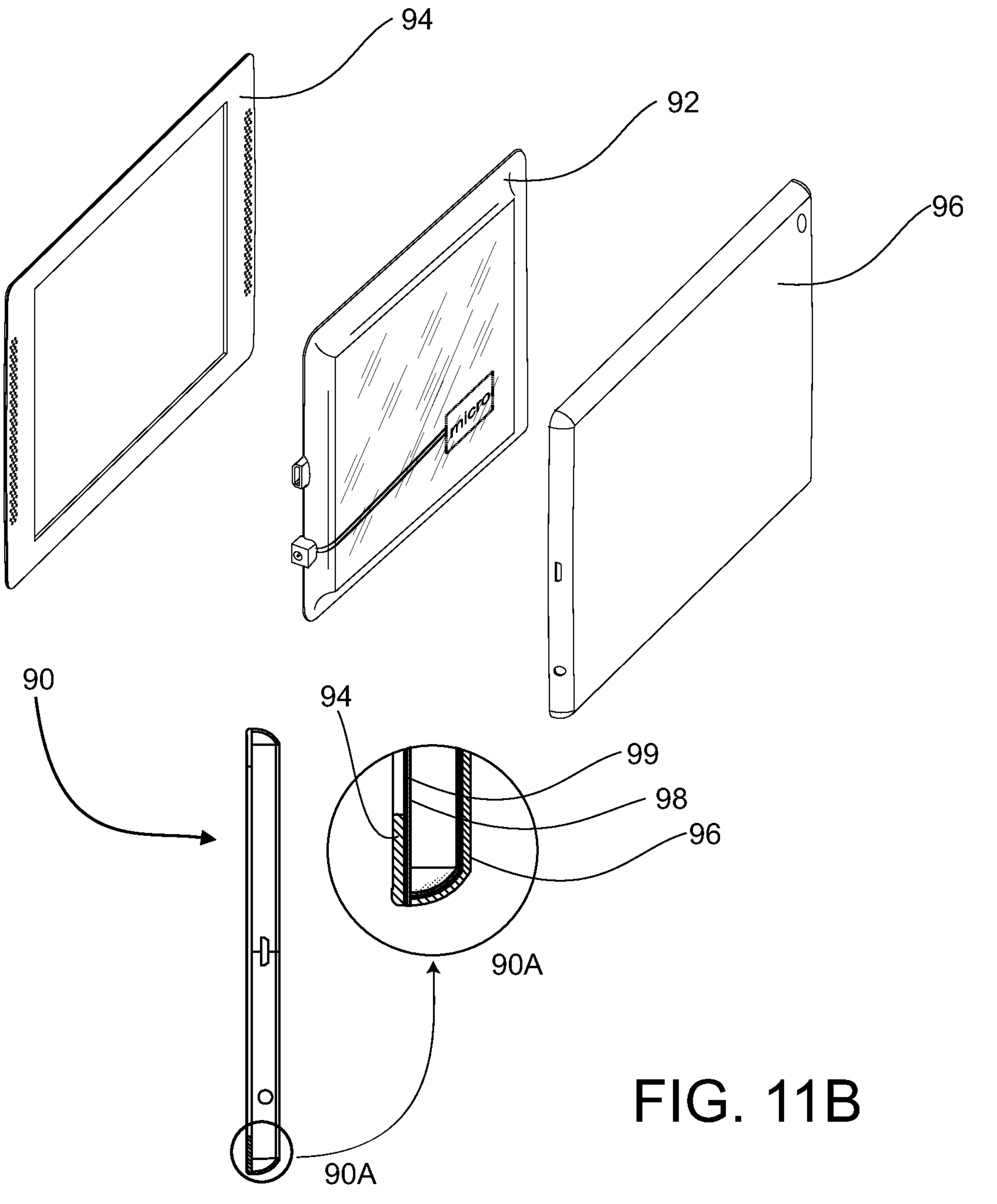


FIG. 11B

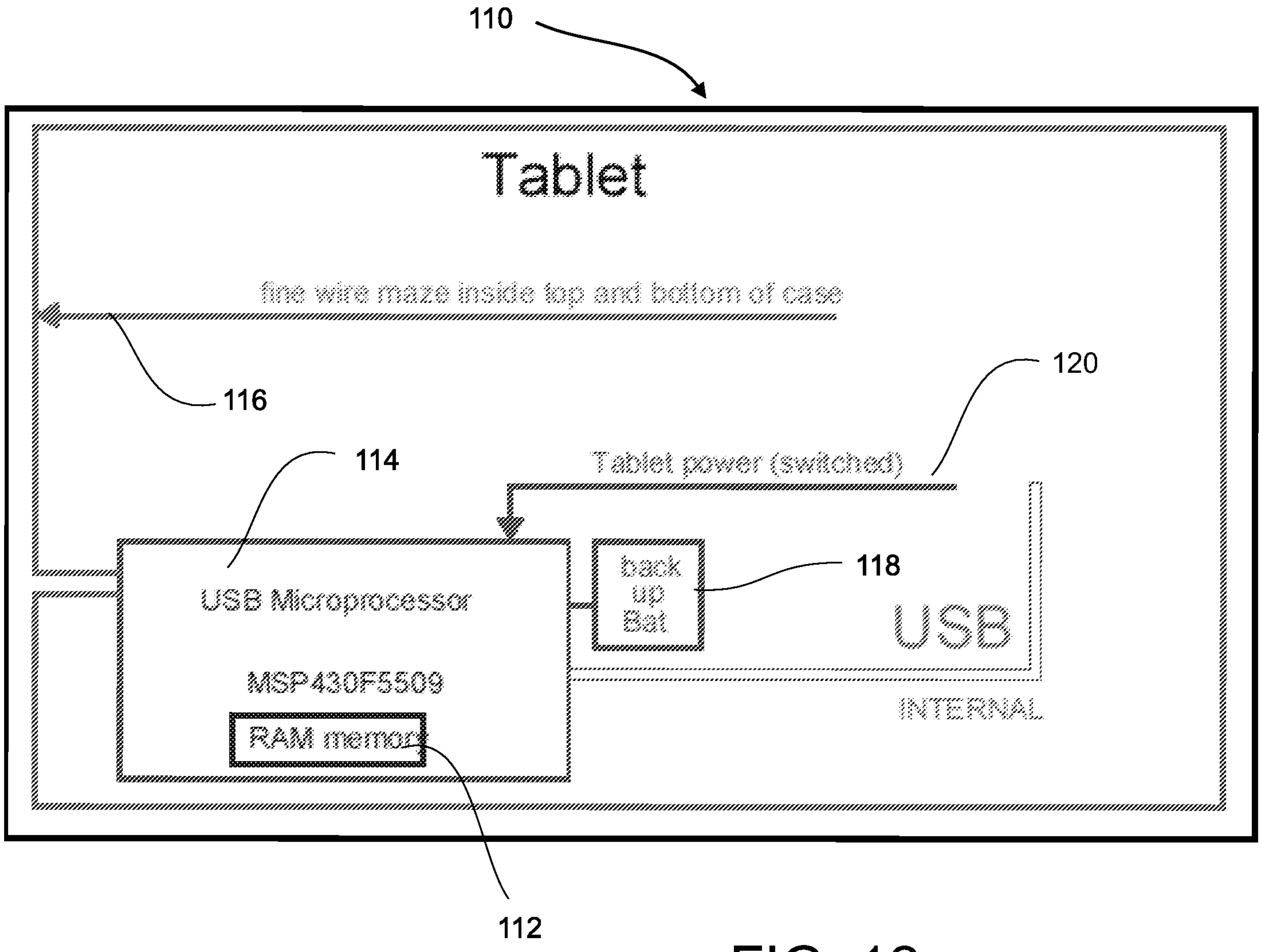

110
Tablet
fine wire maze inside top and bottom of case
116
120
114
Tablet power (switched)
118
back up Bat
USB Microprocessor
USB
MSP430F5509
INTERNAL
RAM memory
112

FIG. 12

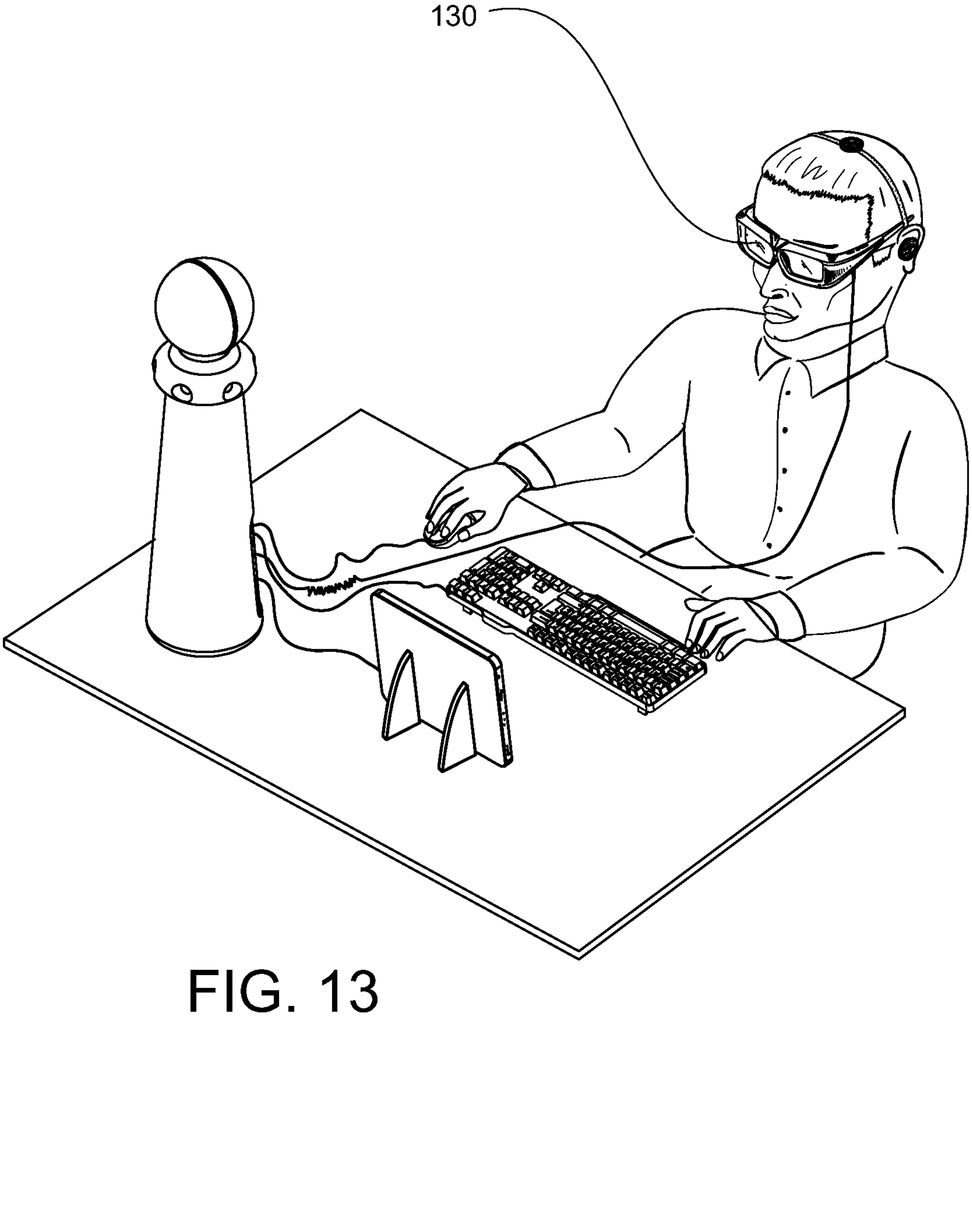


FIG. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/022390

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G08B 13/14 (2015.01)
CPC - G08B 13/14 (2015.04)
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)
IPC(8) - G08B 13/12, 13/14, 23/00 (2015.01)
USPC - 340/568.1, 568.2, 568.8, 571, 572.8; 361/760

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G08B 13/12, 13/14, 13/128, 13/2434 (2015.04) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Orbit, Google Patents, ProQuest
Search terms used: security assembly, cover, wires, computer, test taking, laptop, detecting, cheating, tamper, processor, interface, RAM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0327856 A1 (LOWY) 30 December 2010 (30.12.2010) entire document	1-3, 5, 11-13, 16
Y		4, 6-10, 14-15, 17-20
Y	US 2010/0097215 A1 (LOCHER) 22 April 2010 (22.04.2010) entire document	4
Y	US 2002/0130673 A1 (PELRINE et al) 19 September 2002 (19.09.2002) entire document	6, 14
Y	EP 0 128 672 A1 (GALE) 19 December 1984 (19.12.1984) entire document	7, 9, 15
Y	US 5,291,243 A (HECKMAN et al) 01 March 1994 (01.03.1994) entire document	8
Y	US 2011/0187523 A1 (EDELSTEIN et al) 04 August 2011 (04.08.2011) entire document	10
Y	US 2012/0212414 A1 (OSTERHOUT et al) 23 August 2012 (23.08.2012) entire document	17-20
A	US 2010/0180350 A1 (GLAUBERT) 15 July 2010 (15.07.2010) entire document	1-20
A	US 2004/0177658 A1 (MITCHELL) 16 September 2004 (16.09.2004) entire document	1-20
A	US 2004/0101178 A1 (FEDOROVSKAYA et al) 27 May 2004 (27.05.2004) entire document	1-20

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

* 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 another 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 17 July 2015	Date of mailing of the international search report 29 JUL 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/022390

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See last page

1. □ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-20

Remark on Protest

□ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

□ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

□ No protest accompanied the payment of additional search fees.

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-20, drawn to detecting an attempt to alter an electronic device.
Group II, claims 21-24, drawn to a method for limiting viewing of content on a display.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: monitoring impedance of the wires by means of the security assembly; and when a change in impedance is detected by the security assembly, deleting a required security code needed for use of the device as claimed therein is not present in the invention of Group II. The special technical feature of the Group II invention: changing images being displayed on the display at a high rate at which viewing the display does not provide a discernible image to a viewer; equipping a person with a viewing device having lenses that are selectively opaque or transparent as claimed therein is not present in the invention of Group I.

Since none of the special technical features of the Group I or II inventions are found in more than one of the inventions, unity of invention is lacking.