

METHOD AND SYSTEM TO IDENTIFY UNAUTHORIZED IMAGE CAPTURE OF SECURE MONITORS IN A WORK ENVIRONMENT

5

TECHNICAL FIELD

The present disclosure relates to security systems for the protection of confidential content. More particularly, the present disclosure relates to a method of system of
10 monitoring and identifying unauthorized image capture (e.g. via photography) of sensitive content displayed on a secure monitor.

BACKGROUND

15 The analog hole is a perceived fundamental and inevitable vulnerability in copy protection schemes of digital data. DRM and data encryption only protect the digital copy. Sensitive content displayed on a secure monitor can be viewed within a viewing cone as dictated by the geometry of the screen of the secure monitor and the viewing angle of the pixels on the surface of the screen. The viewing angle is the angle at
20 which the display of a secure monitor can be viewed with acceptable visual performance. The angular range of the viewing angle is called a viewing cone and the viewing cone includes a multitude of viewing directions.

Within this viewing cone, it is possible for the potential bad actor to take an
25 unauthorized photograph of the content. Privacy screens (or privacy filters), mechanical blinds at the sides of the security monitor, and office and cubicle walls can restrict the viewing cone for a secure monitor. However, the content of a secure monitor will be visible when viewed by a potential bad actor seated or standing directly in front of the secure monitor. The potential bad actor can be a person looking over the
30 shoulder of the computing device's authorized user, for instance, or the authorized user acting in violation of the security rules applicable to the content displayed.

- Well known methods of thwarting unauthorized photography of sensitive content on a secure monitor include the outright ban of mobile phones or the requirement that personnel only possess non-camera mobile phones, such as is common in “Red Zones” in the armed forces and government security agencies. This solution, while effective, is often not practical in a civilian or medium security work environment where mobile phone usage is permitted and wide-spread. In such a work environment, enforcement of a camera ban on mobile phones is not practical, as most mobile phone users consider a camera an essential feature of their mobile phone.
- Employee monitoring software also falls short in preventing unauthorized photography. Employee monitoring software commonly includes file access restrictions, the monitoring of key strokes, and the periodic capture of screen shots of the content on the secure monitor. Computer file access control restrictions do not address the danger of authorized users (or other potential bad actors) taking unauthorized photographs of content when that content is displayed as part of the authorized user’s normal employment duties. Thus employee monitoring software does not prevent unauthorized photography during otherwise sanctioned viewing of computer files by an authorized user.
- Monitoring of suspicious activity using video recognition technology may be known. For instance, in U.S. Patent Application Publication No. 2012/0098918A1, analytics are performed on an audio-visual feed to identify any triggering event, upon which a predetermined action is taken. One application for this recognition technology is a search for an object’s removal or addition from an area. The addition of an object could indicate, in a worst case scenario, the need for an alarm signalling an evacuation alert for the area. The removal of an item could signal the theft of a consumer item from a retail store. An optional notification could be made to a security force. This solution is not linked into an employee’s viewing of content on a secure monitor and does not utilize the cameras and microphones available on the laptop computers of employees.

Prevention of unauthorized photography has been addressed for the presentation of entertainment content at large venues. U.S. Patent Application Publication No. 2006/0098165 discloses the use of infrared light emission to disrupt the quality of an image obtained by unauthorized digital recorders located within the venue. While
5 invisible to the human eye, the infrared light is recorded by the digital recorders. This approach is useful for dissuading the copying of entertainment content, where the quality of the image is of importance to potential unauthorized viewers. However, for potential bad actors that are more concerned with secret information or are equipped with sophisticated photography equipment, this solution does not offer sufficient
10 protection.

Detection of camera usage has been specifically addressed by in the Journal of Science and Technology Volume 2, Issue 5, May 2017, PP 06-11, entitled “Arduino based Anti-Photography System for Photography Prohibited Areas” by Dhulekar, et al. In
15 this publication, the design involves the installation of an infrared transmitter surrounding the camera installed within a laptop computer. In this design there is a continuous transmission of infrared rays in the field of view of the camera. When the infrared rays strikes on an unauthorized camera lens, a white circular speckle is seen in the image captured by the camera of the laptop computer. This white circular speckle
20 is then detected from the video feed of the laptop computer’s camera to created a triggering event. This design requires the customization of all laptop computers in the work environment, an expensive and impractical approach given that most employee computers are obtained from standard commercial vendors.

25 Other solutions for reducing unauthorized photography employ software loaded on mobile phones.

In United States Patent No. 8,346,072, for instance, software installed on a mobile phone prevents a user from taking a picture of a subject if the device has not been
30 steadily focused on the subject in question for a predetermined period of time. This process extends the normal camera-taking procedure and thus requires the camera user to take pictures in a conspicuous manner--the rationale being that a camera user would

be less likely to take unauthorized pictures if such actions could be easily recognized. The camera restriction can be communicated to the device via a wireless communication network. Additionally, the restrictions and boundaries can be communicated to the device as part of an IT security policy. In United States Patent
5 Application Publication No. 2013/0040632, software installed on a mobile phone uploads all photographs taken by the mobile phone to a server. Initially the software does not allow any local copy of the image file on the mobile phone. At the server, the photographs are analysed to determine if they are authorized. If authorized, the photograph is pushed to the mobile phone, if not authorized the mobile phone user is
10 denied a copy of the photograph.

These two software solutions have limited practical use, as they require installation of intrusive software on all mobile phones located in the work environment. A potential bad actor could alternately remove such software from their mobile phone, use a
15 different mobile phone that is unknown to the employer to take unauthorized photographs, or alternatively use a stand-alone camera for the unauthorized photographs.

As discussed above, the prior art is unable to fully address the need of preventing
20 potential bad actors from taking unauthorized photographs without limiting the types of mobile phones allowed on the premises (e.g., Red Zoning the work environment), modifying the laptop computer hardware (e.g., to add infrared light emission), or installing security software on each mobile phone. Further, the prior art does not disclose or suggest any method of documenting the content viewed on a secure monitor
25 at the time of an attempted unauthorized photograph.

SUMMARY

A first embodiment of the invention is a method of detecting unauthorized image capture of content displayed on at least one secure monitor as configured by a computing device
5 connected to the secure monitor. Each computing device is associated with at least one authorized user and the content displayed on each secure monitor is viewable within a viewing cone of the secure monitor by at least one potential bad actor. The method comprises the steps of: (a) capturing a surveillance feed for each secure monitor, the surveillance feed including a stream of images for at least a portion of the viewing cone of
10 the secure monitor; (b) analyzing the surveillance feed associated with each secure monitor to identify at least one triggering event; (c) upon identifying each triggering event, storing a trigger record for the triggering event; and (d) upon identifying each triggering event, executing at least one remedial action.

15 In the first embodiment, the stream of images for the surveillance feed is captured by at least one of: (i) a first computer camera connected to the computing device connected to the secure monitor capturing a first substream of images; (ii) a second computer camera connected to the computing device connected to the secure monitor capturing a second substream of images; and (iii) at least one CCTV camera mounted in a work environment
20 associated with the secure monitor capturing a third substream of images. Each triggering event includes at least the identification of a camera unit that is: (i) captured within the viewing cone of the secure monitor in at least one of the stream of images; and (ii) positioned to photograph the content displayed on the secure monitor in the possession of the potential bad actor, wherein the content displayed was retrieved from at least one
25 computer file. Each computer file is stored on at least one of: (1) the computing device connected to the secure monitor; and (2) at least one content repository accessible by the computing device connected to the secure monitor. The trigger record for the triggering event includes: (i) a time stamp for the triggering event; (ii) at least one of: (1) a screenshot of the secure monitor that encountered the triggering event at the time of the
30 triggering event; and (2) a summary of the content displayed on the secure monitor at the time of the triggering event; and (iii) at least one image from the surveillance feed associated with the triggering event capturing the camera unit. Each remedial action

comprises at least one of the steps of: (i) locking down the secure monitor that encountered the triggering event with one or more lock down actions; and (ii) sending a security alert to at least one designated person.

- 5 The trigger record for each triggering event can further include, for a first time window extending before and after the triggering event, at least one of: (a) meta data for each computer file displayed on the secure monitor encountering the triggering event within the first time window; (b) login identification for each authorized user logged into the computing device connected to the secure monitor within the first time window; (c) a first
10 captured block of the surveillance feed associated with the secure monitor that encountered the triggering event within the first time window; and (d) a second captured block of additional surveillance feeds associated with other secure monitors co-located in the work environment associated with the secure monitor that encountered the triggering event within the first time window.

15

The step of analyzing the surveillance feed can be performed by AI / ML.

- The surveillance feed for each secure monitor additionally can include additional biometric information comprising at least one of: (a) a stream of audio captured by a computer
20 microphone connected to the computing device connected to the secure monitor; (b) a stream of typing cadence captured by a computer keyboard connected to the computing device connected to the secure monitor; and (c) a stream of pointer control characteristics captured by a computer pointer connected to the computing device connected to the secure monitor. The step of analyzing the surveillance feed to identify each triggering event can
25 include analysis at least one of: (a) a first comparison of the stream of audio with a pre-recorded voice of at least one of the authorized users of the computing device connected to the secure monitor; (b) a second comparison of the stream of typing cadence with a pre-recorded typing cadence of at least one authorized user of the computing device connected to the secure monitor; and (c) a third comparison of the stream of pointer control
30 characteristics with a pre-recorded pointer control characteristic of at least one authorized user of the computing device connected to the secure monitor. The step of analyzing the surveillance feed to identify each triggering event can additionally include a second

behavioral analysis of the potential bad actor from at least one of: (a) the stream of audio; (b) the stream of typing cadence; and (c) the stream of pointer control characteristics. The trigger record for each triggering event can further include, for a second time window extending before and after the triggering event, at least one of: (a) a third captured block of the stream of audio within the second time window; (b) a fourth captured block of the stream of typing cadence within the second time window; and (c) a fifth captured block of the stream of pointer control characteristic within the second time window.

In a second embodiment of the invention, the method of the first embodiment is implemented on a security system, the system comprising a server with a database. The server is connected via a network to the computing device connected to the secure monitor. The system is configured to execute the method of the first embodiment of the invention by at least one of: (a) a first processor within the computing device connected to the secure monitor; and (b) a second processor within the server.

In a third embodiment of the invention, the invention is contained within a computer program comprising instructions which cause the execution of the method of the first embodiment when the instructions are executed by at least one of: (a) a first processor within the computing device connected to the secure monitor; and (b) a second processor within a server connected via a network to the computing device connected to the secure monitor.

In a fourth embodiment of the invention, the invention is contained within a computer-readable storage medium comprising instructions which cause the execution of the first embodiment of the invention when the instructions are executed by at least one of: (a) a first processor within the computing device connected to at least one secure monitor; and (b) a second processor within a server connected via a network to the computing device connected to the secure monitor.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present disclosure are described herein with reference to the drawings in which:

5

FIG. 1 is an illustration of items located in the work environment during the execution of an embodiment of the invention.

10

FIG. 2 is a block diagram of items in the security system connected via a network of an embodiment of the invention.

FIG. 3 is a flowchart of the steps implemented in an embodiment of the invention to identify unauthorized image capture of a content displayed on a secure monitor.

15

FIG. 4 is a chart detailing the stream of information generated by equipment in the system.

FIG. 5 is a list of potential lock down steps for remedial action after a trigger event.

20

DETAILED DESCRIPTION

In the following detailed description, reference is made to the accompanying drawings, which form a part hereof. The illustrative embodiments described in the detailed description, drawings and claims are not meant to be limiting. Other embodiments can be utilized, and other changes can be made, without departing from the spirit or scope of the subject matter presented herein. Unless specified otherwise, the terms “comprising,” “comprise,” “including” and “include” used herein, and grammatical variants thereof, are intended to represent “open” or “inclusive” language such that they include recited elements but also permit inclusion of additional, un-recited elements.

25

30

As used herein, a computing device **04** may be a single stand-alone computer such as a desktop computer or a laptop computer, a thin client, a tablet computer, or a mobile phone. The computing device **04** may run a local operating system and store computer files on a local storage drive. The computing device **04** may access files and application through a gateway **22** to one or more content repositories **26**, the content repository **26** can host files and/or run virtual applications and generate a virtual desktop for the computing device **04**.

As used herein, the secure monitor **08** is a display device for viewing content **09**. The secure monitor **08** may be a dedicated screen incorporated into the computing device **04** (such as the screen display for a laptop computer, a thin client, a tablet computer, or a mobile phone). The secure monitor **08** may be a stand alone display (such as a computer display connected to the computing device **04**, a projected screen, or a conference room monitor).

As used herein, a server **24** may include a single stand-alone computer, a single dedicated server, multiple dedicated servers, and/or a virtual server running on a larger network **23** of servers **24** and/or cloud-based service. As used herein, a database **25** may store data to and access data from a single stand-alone computer, a data server, multiple dedicated data servers, a cloud-based service, and/or a virtual server running on a larger network of servers.

As used herein, the network **23** can be any means of providing communication between the computing device **04** and content **09** stored elsewhere. As used herein, the network **23** can be a personal area network, local area network, a storage area network, a system area network, a wide area network, a virtual private network, and an enterprise private network. As implemented in the invention, the network **23** can include one or more gateways **22** or no gateways **22**. The network **23** communication can be conducted via published standard protocols or proprietary protocols. Communication of data through the network **23** can be: (i) encrypted or unencrypted; (ii) delivered via a wired network, a wireless network, or a combination of wired and wireless. Wireless communication can be accomplished in any practical manner including a Wi-Fi 802.11

network, a BluetoothTM network, or mobile phone network (such as 3G, 4G, LTE, and 5G). The terms “connected”, “connected”, and “connecting” as used herein refer to a communication link between two devices and can be accomplished as discussed in this paragraph.

5

As used herein, the network **23** can connect at least in part along a proprietary network **23** protocol (such as for CCTV and motion detector **03** devices). The CCTV and motion detector **03** devices can also communicate via common Internet-of-Thing (IoT) protocols, such as Narrowband IoT (“NB-IoT”), 3G SIM card based mobile communication network, or a Message Queuing Telemetry Transport. In the case of IoT devices, the IoT devices can be in communication with the gateway **22** and/or network **23** via at least one of a wireless transceiver and a wired link. Also communication between the IoT sensors, the gateway **22**, the server **24**, and the user interfaces can be encrypted and bidirectional. For instance, at least one of the IoT sensors can be configured to receive at least one command from the server **24** through the gateway **22**.

As used herein, the user interface devices connected to the computing device **04** can be connected via dedicated wire or wirelessly to the computing device **04**. The touch pad **07** can be incorporated on the laptop computer or a separate tracking device. The computer microphone **12** can be incorporated into the computing device **04** (as typically engineered within a laptop computer, a tablet computer, and a mobile phone) and a separate device connectable to the computing device **04**.

As used herein, computer image capture device includes video-cam and cameras. Cameras can be any type of camera connected to the computing device **04**. For instance, a dedicated camera can be incorporated atop the display screen of a laptop computer, a tablet computer, and a mobile phone. Modern mobile phones have more than one camera, notably a “selfie” camera directed at the intended device user and a second camera directed opposite the display screen. Another common option for computer cameras are webcams, which are connectable to computing devices **04**.

As used herein, viewing angle is the angle at which the display of the secure monitor **08** can be viewed with acceptable visual performance. The angular range of the viewing angle is called a viewing cone and the viewing cone includes a multitude of viewing directions. Within this viewing cone, it is possible for the potential bad actor **13** to take an unauthorized image, such as a photograph **15** of the content **09**. Generally, the content **09** of a secure monitor **08** will be visible when viewed by a potential bad actor **13** seated or standing directly in front of the secure monitor **08**.

As used herein, the camera unit **14** can be any device capable of taking photographs of the content **09** on a secure monitor **08**. The most common camera units **14** in use by typically employees will be mobile phones and stand-alone digital cameras (such as compact, bridge, mirrorless and DSLRs). The camera unit **14**, as used herein, also includes film camera of different dimensions and cover camera designs.

As used herein, a designated person for receiving a security alert can be an onsite or offsite security professional. The designated person could also be a supervisor or other member of the work environment **01** staff designated for receiving the security alerts. More than one person can be a listed in the system **21** as a designated person.

As used herein, the term “associate”, “associated”, “associate”, and “associating” indicate a defined relationship (or cross-reference) between two items and/or persons. For instance, a computing device **04** can be associated with at least one authorized user, indicating that such a user is authorized to log into the computing device **04**. A computing device **04** can have more than one authorized user, such as an employee and an IT administrator. For instance, a computing device **04** can be associated with at least one triggering event, indicating that the triggering event related to potential unauthorized image capture (e.g. via photography) of its connected secure monitor **08**. For instance, a work environment **01**, surveillance feed, CCTV camera **02**, or motion detector **03** can be associated with a secure monitor **08** or its connected computing device **04**. E.g., a work environment **01** could include many work stations, each work station with a secure monitor **08** connected to a computing device **04**. Various

associations can be entered, cross-referenced, and updated by the database **25** in the server **24**.

The at least one potential bad actor **13** can be anyone seeking to obtain an unauthorized
5 copy or image (such as photograph **15**) of content **09**. Each potential bad actor **13** can
be one of the authorized users of the device or one of their co-workers. The potential
bad actor **13** can be staff with authorized access to the work environment **01** but
without authorized access to the content **09**. The potential bad actor **13** can be a
trespasser in the work environment **01**. There can be more than one bad actor, each
10 potential bad actor **13** having various levels of culpability from negligent, to reckless,
to intentional and/or malicious. For instance, the negligence or gullibility of one
potential bad actor **13** could be exploited by a second potential bad actor **13**. For this
reason, the invention contemplates a wide window of surveillance feed capture both
before and after the triggering event, to capture possible activity by more than one
15 potential bad actor **13** and also to provide possible training footage for new security or
other professional staff.

The content **09** viewable on the secure monitor **08** can be generated by computer files
resident on the computing device **04** and/or resident on a content repository **26**. The
20 content repositories **26** can be one or more servers, computers, or data storage devices
accessible by the computing device **04** through a network **23**.

As used herein, the work environment **01** can be an office setting with desk, cubicles,
offices, or other suitable arrangements in a work setting. As the invention can be
25 implemented by devices (such as a laptop computer, a tablet computer) that can be
taken outside an office setting, the work environment **01** can also be professional's
home office, library, conference room, cafe, train, airplane, bus, or other location(s)
where portable work can be performed. Outside the office settings, the CCTV camera
02 and motion detectors **03** may typically not be available and also the computer audio
30 may be too noisy for reliable analyses. However, the first substream of images from
the first camera (as as on a laptop computer, tablet computer, and mobile phone), the
stream of typing cadence from the computer keyboard **05**, and the stream of pointer

control of the computer pointer will be available for analysis if a network **23** is available.

As used herein, the computer pointer can be any device used to dictate position of a cursor on the secure monitor **08**. Example pointer devices for a computing device **04** include a computer mouse **06**, a touch pad **07**, a touch screen, and a pen stylus.

FIG. 1 is an illustration of items located in the work environment **01** during the execution of an embodiment of the invention. As illustrated, the computing device **04** is depicted as a laptop computer. The computing device's **04** shell a secure monitor **08** for viewing content **09**, a keyboard **05**, a touch pad **07**, a first computer camera **10** directed toward a potential user of the computing device **04**, and a computer microphone **12**. Other devices connected to the computing device **04** include a computer mouse **06** and a second computer camera **11** (depicted in **FIG. 1** as a web cam). The secure monitor **08** is located within a work environment **01**. Within the work environment **01** are installed a CCTV camera **02** and a motion detector **03**. In this work environment **01**, within the viewing cone of the secure monitor **08** is a potential bad actor **13** holding a camera unit **14** (here depicted as a mobile phone). The camera unit **14** includes a camera (not shown) within the viewing cone of the secure monitor **08**, the screen of the camera unit **14** displays an unauthorized photograph **15** of the content **09** displayed on the secure monitor **08**. As depicted, the first and second computer cameras **11** are positioned to capture, as a stream of images, the act of the potential bad actor **13** taking an unauthorized photograph **15** of the content **09** on the secure monitor **08**.

FIG. 2 is a block diagram of items in the security system **21** connected via a network **23** of an embodiment of the invention. The work environment **01** includes a computing device **04**, a CCTV camera **02**, and a motion detector **03** connected via a gateway **22** to a network **23**. The network **23** is connected to a plurality of content repositories **26** and a server **24**. The server **24** includes a database **25**. The computing device **04** includes a keyboard **05**, a computer mouse **06**, a touch pad **07**, a first computer camera **10**, a

second computer camera **11**, and a computer microphone **12**, all of which are connected to the gateway **22** via a network interface card (“NIC”) **27**.

FIG. 3 is a flowchart **3-00** of the general steps implemented in an embodiment of the invention. The steps **3-01** to **3-07** in **FIG. 3** include:

- 3-01** install surveillance software on the computing devices **04** for the work environment **01** to capture a stream of images for at least a portion of the viewing cone of the secure monitor **08** from each computing device **04** for analysis as part of a surveillance feed
- 3-02** connect CCTV cameras **02** and motion detectors **03** to the gateway **22** and route their substreams to the server **24** for analysis as an additional part of the surveillance feed
- 3-03** analyse the stream of images to identify a camera unit **14** that is within the viewing cone of the secure monitor **08** and positioned to photograph the content **09** displayed on the secure monitor **08**
- 3-04** store a trigger record with a time stamp, a screenshot of the secure monitor **08**, and an image of the potential bad actor **13**
- 3-05** lock down the computing device **04** for the associated secure monitor **08** that encountered the triggering event
- 3-06** send a security alert to a security professional
- 3-07** attempt to identify and locate the potential bad actor **13** based on information from the surveillance feed

FIG. 4 is a chart **4-00** detailing the stream of information generated by equipment in the system **21** that can be included in the surveillance feed. As detailed in this chart, a

first computer camera **10** generates a first substream of images of a potential bad actor **13**, a second computer camera **11** generates a second substream of images of the potential bad actor **13**, a CCTV camera **02** generates a third substream of images of the potential bad actor **13**, a computer microphone **12** generates an audio stream of the potential bad actor **13**, a computer keyboard **05** generates a stream of typing cadence of the user of the computing device **04** (which could also be the potential bad actor **13**), and the computer pointer generates a stream of pointer control characteristics of the user of the computing device **04** (which could also be the potential bad actor **13**). Note that all this information is potentially assembled and analyzed to determine any triggering events and potentially to document a trigger record for the triggering event.

FIG. 5 is a list **5-00** of potential lock down steps for remedial action after a trigger event. The order of the lock down steps is exemplary, all or some of these steps could be performed in a different order or in parallel. The potential lock down steps are listed as **5-01** to **5-07** in **FIG. 5** and include:

- 5-01** deactivate the secure monitor **08**
- 5-02** close one or more windows displaying the content **09** on the secure monitor **08**
- 5-03** lock each computer file displayed on the secure monitor **08**
- 5-05** delete each computer file displayed on the secure monitor **08** from the computing device **04**
- 5-05** restrict access to the computing device **04** for the authorized user logged into the computing device **04** connected to the secure monitor **08** during the triggering event
- 5-06** restrict access to each content repository **26** accessible by the computing device **04** associated with the triggering event

5-07 wipe at least a portion of a local storage drive of the computing device
04 associated with the triggering event

A first embodiment of the invention is a method of detecting unauthorized image capture (e.g. via photography) of content **09** displayed on at least one secure monitor **08**. The content **09** displayed on each secure monitor **08** is configured by a computing device **04** connected to the secure monitor **08**, each computing device **04** is associated with at least one authorized user, and the content **09** displayed on each secure monitor **08** is viewable within a viewing cone of the secure monitor **08** by at least one potential bad actor **13**. The method comprises the steps of: (a) capturing a surveillance feed for each secure monitor **08**, the surveillance feed including a stream of images for at least a portion of the viewing cone of the secure monitor **08**; (b) analyzing the surveillance feed associated with each secure monitor **08** to identify at least one triggering event; (c) upon identifying each triggering event, storing a trigger record for the triggering event; and (d) upon identifying each triggering event, executing at least one remedial action. The stream of images for the surveillance feed is captured by at least one of: (i) a first computer camera **10** connected to the computing device **04** connected to the secure monitor **08** capturing a first substream of images; (ii) a second computer camera **11** connected to the computing device **04** connected to the secure monitor **08** capturing a second substream of images; and (iii) at least one CCTV camera **02** mounted in a work environment **01** associated with the secure monitor **08** capturing a third substream of images. Each triggering event includes at least the identification of a camera unit **14** that is: (i) captured within the viewing cone of the secure monitor **08** in at least one of the stream of images; and (ii) positioned to photograph the content **09** displayed on the secure monitor **08** in the possession of the potential bad actor **13**, wherein the content **09** displayed was retrieved from at least one computer file. Each computer file is stored on at least one of: (1) the computing device **04** connected to the secure monitor **08**; and (2) at least one content repository **26** accessible by the computing device **04** connected to the secure monitor **08**. The trigger record for the triggering event includes: (i) a time stamp for the triggering event; (ii) at least one of: (1) a screenshot of the secure monitor **08** that encountered the triggering event at the time of the triggering event; and (2) a summary of the content **09** displayed on the secure monitor **08** at the time of the triggering event; and (iii) at least one image from the surveillance feed associated with the triggering event capturing the camera unit **14**. Each remedial action comprises at least one of the steps of: (i) locking down the secure monitor **08** that encountered the

triggering event with one or more lock down actions; and (ii) sending a security alert to at least one designated person.

To identify the camera, the computing device **04** or the server **24** can store a library of example images or models of sample camera units **14**, then perform a pattern recognition step to identify any camera unit **14** that is captured within the viewing cone of the secure monitor **08** in at least one of the stream of images. The step of evaluating whether the camera unit **14** is positioned to photograph the content **09** displayed on the secure monitor **08** is made to reduce the number of false alarms. E.g., to distinguish between regular mobile phone usage for texting, web surfing, and telephone calls from the act of taking photographs. For the pattern recognition, the advent of AI / ML software can be utilized. Given the high computational demands of AI / ML, the pattern recognition step is likely performed on a server **24** rather than a computing device **04**.

The trigger record for each triggering event can further include, for a first time window extending before and after the triggering event, at least one of: (a) meta data for each computer file displayed on the secure monitor **08** encountering the triggering event within the first time window; (b) login identification for each authorized user logged into the computing device **04** connected to the secure monitor **08** within the first time window; (c) a first captured block of the surveillance feed associated with the secure monitor **08** that encountered the triggering event within the first time window; and (d) a second captured block of additional surveillance feeds associated with other secure monitor **08** co-located in the work environment **01** associated with the secure monitor **08** that encountered the triggering event within the first time window.

The step of analyzing the surveillance feed to identify each triggering event can include a first behavioral analysis of the potential bad actor **13** from the stream of images.

The step of analyzing the surveillance feed to identify each triggering event can include comparison of the stream of images with a pre-recorded image of at least one authorized user of the computing device **04**.

The step of analyzing the surveillance feed can be performed by AI / ML.

- The surveillance feed additionally can include at least one of: (a) motion detection information from at least one motion detector **03** in the work environment **01** associated with the secure monitor **08**; and (b) location information accessed at least one mobile device associated with one or more of the authorized users of the computing device **04** connected to the secure monitor **08**. The mobile device can be a mobile phone, a tablet computer, or other personal device that tracks location of its user.
- 10 The surveillance feed for each secure monitor **08** additionally can include additional biometric information comprising at least one of: (a) a stream of audio captured by a computer microphone **12** connected to the computing device **04** connected to the secure monitor **08**; (b) a stream of typing cadence captured by a computer keyboard **05** connected to the computing device **04** connected to the secure monitor **08**; and (c) a stream of pointer control characteristics captured by a computer pointer connected to the computing device **04** connected to the secure monitor **08**. The step of analyzing the surveillance feed to identify each triggering event can include analysis at least one of: (a) a first comparison of the stream of audio with a pre-recorded voice of at least one of the authorized users of the computing device **04** connected to the secure monitor **08**; (b) a second comparison of the stream of typing cadence with a pre-recorded typing cadence of at least one authorized user of the computing device **04** connected to the secure monitor **08**; and (c) a third comparison of the stream of pointer control characteristics with a pre-recorded pointer control characteristic of at least one authorized user of the computing device **04** connected to the secure monitor **08**. The step of analyzing the surveillance feed to identify each triggering event can additionally include a second behavioral analysis of the potential bad actor **13** from at least one of: (a) the stream of audio; (b) the stream of typing cadence; and (c) the stream of pointer control characteristics. The trigger record for each triggering event can further include, for a second time window extending before and after the triggering event, at least one of: (a) a third captured block of the stream of audio within the second time window; (b) a fourth captured block of the stream of typing cadence within the second time window; and (c) a fifth captured block of the stream of pointer control characteristic within the second time window.

A pre-recorded voice of at least one of the authorized users of the computing device **04** connected to the secure monitor **08** can act like a fingerprint in identifying authorized users, even if entry to the computing device **04** was with the proper login and password. A pre-
5 recorded typing cadence or a pre-recorded pointer control characteristic of at least one authorized user of the computing device **04** connected to the secure monitor **08** also acts like a fingerprint in identifying the authorized users. E.g., the difference between an authorized user and an imposter can be identified by by comparing the voice patterns, typing cadence, and/or pointer control characteristics with pre-recorded samples.

10

The one or more lock down actions, for the computing device **04** connected to the secure monitor **08** during the triggering event, can comprise at least one of: (a) deactivating the secure monitor **08**; (b) closing one or more windows displaying the content **09** on the secure monitor **08**; (c) locking each computer file displayed on the secure monitor **08**; (d)
15 deleting each computer file displayed on the secure monitor **08** from the computing device **04**; (e) restricting access to the computing device **04** for the authorized user logged into the computing device **04** connected to the secure monitor **08** during the triggering event; (f) restricting access to each content repository **26** accessible by the computing device **04** associated with the triggering event; and (g) wiping at least a portion of a local storage
20 drive of the computing device **04** associated with the triggering event.

The security alert for each triggering event can comprise at least one of: (a) an email; (b) a text message; (c) a phone call; (d) an audio alarm; and (e) a transmission of at least a portion of the surveillance feed associated with the secure monitor **08** that
25 encountered the triggering event.

Each trigger record can be stored on at least one of: (a) the computing device **04** connected to the secure monitor **08** undergoing the triggering event; and (b) a database **25** of a server **24** connected via a network **23** to the computing device **04** connected to
30 the secure monitor **08** undergoing the triggering event.

The step of analyzing the surveillance feed can be performed upon on at least one of: (a) the computing device **04** connected to the secure monitor **08**; and (b) a server **24** connected via a network **23** to the computing device **04** connected to the secure monitor **08**.

5

In a second embodiment of the invention, the method of the first embodiment is implemented on a security system **21**, the system **21** comprising a server **24** with a database **25**. The server **24** is connected via a network **23** to the computing device **04** connected to the secure monitor **08**. The system **21** is configured to execute the method
10 of the first embodiment by at least one of: (a) a first processor within the computing device **04** connected to the secure monitor **08**; and (b) a second processor within the server **24**. For instance, the computing device **04** could be loaded with software that captures and pushes the surveillance feed to the server **24** and the server **24** performs the computationally intensive analysis of the surveillance feed.

15

In a third embodiment of the invention, the invention is contained within a computer program comprising instructions which cause the execution of the method of the first embodiment when the instructions are executed by at least one of: (a) a first processor within the computing device **04** connected to the secure monitor **08**; and (b) a second
20 processor within a server **24** connected via a network **23** to the computing device **04** connected to the secure monitor **08**. For instance, the computing device **04** could be loaded with software that captures the surveillance feed and also performs the analysis of the surveillance feed. Alternatively, the computing device **04** could be loaded with software that captures and pushes the surveillance feed to the server **24** and the server
25 **24** performs the computationally intensive analysis of the surveillance feed.

In a fourth embodiment of the invention, the invention is contained within a computer-readable storage medium comprising instructions which cause the execution of the first embodiment of the invention when the instructions are executed by at least one of: (a)
30 a first processor within the computing device **04** connected to at least one secure monitor **08**; and (b) a second processor within a server **24** connected via a network **23** to the computing device **04** connected to the secure monitor **08**. For instance, the

computing device **04** could be loaded with software that captures the surveillance feed and also performs the analysis of the surveillance feed. Alternatively, the computing device **04** could be loaded with software that captures and pushes the surveillance feed to the server **24** and the server **24** performs the computationally intensive analysis of the surveillance feed.

While various aspects and embodiments have been disclosed herein, it will be apparent that various other modifications and adaptations of the invention will be apparent to the person skilled in the art after reading the foregoing disclosure without departing from the spirit and scope of the invention and it is intended that all such modifications and adaptations come within the scope of the appended claims. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit of the invention being indicated by the appended claims.

CLAIMS

1. A method of detecting unauthorized image capture of content displayed on at least
5 one secure monitor,
wherein the content displayed on each secure monitor is configured by a computing
device connected to the secure monitor, the computing device is associated with at least
one authorized user, and the content displayed on each secure monitor is viewable within a
viewing cone of the secure monitor by at least one potential bad actor,
10 the method comprising the steps of:
(a) capturing a surveillance feed for each secure monitor, the surveillance feed
including a stream of images for at least a portion of the viewing cone of the secure
monitor, wherein the stream of images for the surveillance feed is captured by at least one
of:
15 (i) a first computer image capture device connected to the computing device
connected to the secure monitor capturing a first substream of images;
(ii) a second computer image capture device connected to the computing device
connected to the secure monitor capturing a second substream of images; and
(iii) at least one CCTV image capture device mounted in a work environment
20 associated with the secure monitor capturing a third substream of images;
(b) analyzing the surveillance feed associated with each secure monitor to identify at
least one triggering event, wherein each of the at least one triggering event includes at least
the identification of a camera unit that is:
(i) captured within the viewing cone of the secure monitor in at least one of the
25 stream of images; and
(ii) positioned to obtain an image of the content displayed on the secure monitor
in the possession of the potential bad actor, wherein the content displayed was
retrieved from at least one computer file, wherein each computer file is stored on at
least one of: (1) the computing device connected to the secure monitor; and (2) at
30 least one content repository accessible by the computing device connected to the
secure monitor;

- (c) upon identifying each triggering event, storing a trigger record for the triggering event, the trigger record for the triggering event including:
 - (i) a time stamp for the triggering event;
 - (ii) at least one of: (1) a screenshot of the secure monitor that encountered the triggering event at the time of the triggering event; and (2) a summary of the content displayed on the secure monitor at the time of the triggering event; and
 - (iii) at least one image from the surveillance feed associated with the triggering event capturing the camera unit; and
 - (d) upon identifying each triggering event, executing at least one remedial action, wherein each remedial action comprises at least one of the steps of:
 - (i) locking down the secure monitor that encountered the triggering event with one or more lock down actions; and
 - (ii) sending a security alert to at least one designated person.
2. The method of any of the preceding claims, wherein the trigger record for each triggering event further includes, for a first time window extending before and after the triggering event, at least one of:
- (a) meta data for each computer file displayed on the secure monitor encountering the triggering event within the first time window;
 - (b) login identification for each authorized user logged into the computing device connected to the secure monitor within the first time window;
 - (c) a first captured block of the surveillance feed associated with the secure monitor that encountered the triggering event within the first time window; and
 - (d) a second captured block of additional surveillance feeds associated with other secure monitors co-located in the work environment associated with the secure monitor that encountered the triggering event within the first time window.
3. The method of any of the preceding claims, wherein the step of analyzing the surveillance feed to identify each triggering event includes a first behavioral analysis of the potential bad actor from the stream of images.

- 4 The method of any of the preceding claims, wherein the step of analyzing the surveillance feed to identify each triggering event includes comparison of the stream of images with a pre-recorded image of at least one authorized user of the computing device.
- 5 5. The method of any of the preceding claims, wherein the step of analyzing the surveillance feed is performed by AI / ML.
6. The method of any of the preceding claims, wherein the surveillance feed additionally includes at least one of:
- 10 (a) motion detection information from at least one motion detector in the work environment associated with the secure monitor; and
- (b) location information accessed at least one mobile device associated with one or more of the authorized users of the computing device connected to the secure monitor.
- 15 7. The method of any of the preceding claims, wherein the surveillance feed for each secure monitor additionally includes additional biometric information comprising at least one of:
- (a) a stream of audio captured by a computer microphone connected to the computing device connected to the secure monitor;
- 20 (b) a stream of typing cadence captured by a computer keyboard connected to the computing device connected to the secure monitor; and
- (c) a stream of pointer control characteristics captured by a computer pointer connected to the computing device connected to the secure monitor.

8. The method of claim 7, wherein the step of analyzing the surveillance feed to identify each triggering event includes analysis at least one of:
- (a) a first comparison of the stream of audio with a pre-recorded voice of at least one of the authorized users of the computing device connected to the secure monitor;
 - 5 (b) a second comparison of the stream of typing cadence with a pre-recorded typing cadence of at least one authorized user of the computing device connected to the secure monitor; and
 - (c) a third comparison of the stream of pointer control characteristics with a pre-recorded pointer control characteristic of at least one authorized user of the computing
 - 10 device connected to the secure monitor.
9. The method of claim 7, wherein the step of analyzing the surveillance feed to identify each triggering event additionally includes a second behavioral analysis of the potential bad actor from at least one of:
- 15 (a) the stream of audio;
 - (b) the stream of typing cadence; and
 - (c) the stream of pointer control characteristics.
10. The method of claim 7, wherein the trigger record for each triggering event further
- 20 includes, for a second time window extending before and after the triggering event, at least one of:
- (a) a third captured block of the stream of audio within the second time window;
 - (b) a fourth captured block of the stream of typing cadence within the second time window; and
 - 25 (c) a fifth captured block of the stream of pointer control characteristic within the second time window.

11. The method of any of the preceding claims, wherein the one or more lock down actions, for the computing device connected to the secure monitor during the triggering event, comprise at least one of:
- (a) deactivating the secure monitor;
 - 5 (b) closing one or more windows displaying the content on the secure monitor;
 - (c) locking each computer file displayed on the secure monitor;
 - (d) deleting each computer file displayed on the secure monitor from the computing device;
 - (e) restricting access to the computing device for the authorized user logged into
 - 10 the computing device connected to the secure monitor during the triggering event;
 - (f) restricting access to each content repository accessible by the computing device associated with the triggering event; and
 - (g) wiping at least a portion of a local storage drive of the computing device associated with the triggering event.
- 15
12. The method of any of the preceding claims, wherein the security alert for each triggering event comprises at least one of:
- (a) an email;
 - (b) a text message;
 - 20 (c) a phone call;
 - (d) an audio alarm; and
 - (e) a transmission of at least a portion of the surveillance feed associated with the secure monitor that encountered the triggering event.
- 25
13. The method of any of the preceding claims, wherein each trigger record is stored on at least one of:
- (a) the computing device connected to the secure monitor undergoing the triggering event; and
 - (b) a database of a server connected via a network to the computing device
 - 30 connected to the secure monitor undergoing the triggering event.

14. The method of any one of claims **1-12**, wherein the step of analyzing the surveillance feed is performed upon on at least one of:
- (a) the computing device connected to the secure monitor; and
 - (b) a server connected via a network to the computing device connected to the
- 5 secure monitor.
15. A security system comprising a server with a database,
wherein the server is connected via a network to the computing device
connected to the secure monitor, and
- 10 the system is configured to execute the method of any one of claims **1-12** by at
least one of:
- (a) a first processor within the computing device connected to the secure monitor;
and
 - (b) a second processor within the server.
- 15
16. A computer program comprising instructions which cause the execution of the
method of any one of claims **1-12** when the instructions are executed by at least one of:
- (a) a first processor within the computing device connected to the secure monitor;
and
- 20 (b) a second processor within a server connected via a network to the computing
device connected to the secure monitor.
17. A computer-readable storage medium comprising instructions which cause the
execution of the method of any one of claims **1-12** when the instructions are executed
- 25 by at least one of:
- (a) a first processor within the computing device connected to at least one secure
monitor; and
 - (b) a second processor within a server connected via a network to the computing
device connected to the secure monitor.
- 30