

SYSTEM AND METHOD TO PREVENT THE TAKING OF PHOTOGRAPHS IN SECURE AREAS

5 FIELD OF INVENTION

Embodiments of the present invention provide a system and method to prevent the taking of photographs when an individual visits an area where the taking of photographs is prohibited.

10

BACKGROUND

Mobile electronic devices have become an indispensable tool for individuals all over the world. Today's mobile electronic devices often include multiple features, such as telephone functionality, internet access, a built-in camera, and removable
15 memory.

Unfortunately, over the last few years security has also become a major concern. More and more organizations are designating specific internal areas where the use of cameras of any type is strictly prohibited. Such areas may include, for example,
20 research facilities, government facilities, military facilities, sports complexes or stadiums, etc. Such areas require that both visitors and employees check in at, for example, a guard house located at an entrance to the facility. During the check-in process, any device that includes a capability to take pictures must be surrendered to the guards, who are then required to account for the device, and return it to its
25 rightful owner upon exiting the facility.

This system, while workable, suffers from several problems. First, while the individual is within the secure area, they are unable to use their mobile device. For business travelers, as well as for employees, this restriction can be a major
30 inconvenience. Not only do the individuals have no access to the mobile phone for the purposes of making phone calls, they are also unable to access any data stored on the device, such as phone numbers, files, etc.

Additionally, the system described above entails a significant burden placed on security personnel to receive the devices, provide a suitable receipt to the individual, store the devices in a secure place, and return the devices to the individual when they exit the area. While some locations use miniature lockers for the storage of such devices, this is not an optimal solution. Locker keys must still be issued and retrieved. An issue also arises with respect to accounting for lost keys.

Security systems as described above also indirectly encourage employees to ignore the regulation and smuggle such devices into the secure area. Even if these individuals have no intention of taking pictures, the lack of security awareness demonstrated by such actions is still of great concern to the operators of the facility.

One proposed solution to this problem was discussed in United States Patent No. 6,801,642, issued on October 5, 2004, to Gorday, et al. and entitled "Method and Apparatus for Limiting Storage or Transmission of Visual Information". The '642 patent uses a highly complicated system of transmitters to control the image transfer capability of portable devices. This system suffers from several drawbacks. First, it is very complex and expensive to implement. Second, it provides no capability to obscure an image if the device is not connected to some sort of network, or transmitting some type of electronic signal. For example, the system described in the '642 patent will not work on a simple digital camera that has no communications capability.

It would therefore be a great improvement in the art if a system and/or method could be devised to overcome one or more of the problems cited above.

SUMMARY

One aspect of the present invention provides a system to prevent the taking of photographs in unauthorized areas. The system includes a container for receiving a device capable of taking photographs, the container being made of a material that prevents the device from capturing a clear photographic image and allows a user to access other features of the device while the device is inside the container; and

means for sealing the container such that an attempt to remove the device from the container leaves visible evidence.

5 In some embodiments, the container may be a zip-lock type plastic bag, and the means for sealing may be a tamper-resistant zipper and a security label located proximate the zipper in a closed configuration, the security label providing the visible evidence.

10 In alternate embodiments, the means for sealing may include a thermal sealing device.

In other embodiments, the container may be a plastic bag; and the means for sealing may be a flexible cable slidably attached to the bag, a slider coupled to the cable such that moving the slider along the cable in a first direction closes the bag, and a security seal attached across the cable adjacent the slider, the security seal providing the visible evidence.

20 In some embodiments, the plastic bag may be linear low-density polyethylene (LLDPE), high-density polyethylene (HDPE), and other types of plastic. The device may be a camera, a cellular telephone capable of taking pictures, a personal digital assistant, or a music player.

In some embodiments, the system may further include a small opening in the container to allow the use of accessories for the device.

25 An alternate aspect of the present invention provides a method to prevent the taking of photographs in secure areas, the method including the steps of: receiving a device capable of taking photographs from a user; inserting the device into a container, the container being made from a material that prevents the device from capturing a clear photographic image and allows a user to access to other features of the device while the device is inside the container; sealing the container such that an attempt to remove the device from the container leaves visible evidence; and returning the sealed container to the user.

In some embodiments of the method, the flexible container may be a zip-lock type plastic bag, the means for sealing the container may further include a tamper-resistant zipper, and the step of sealing the container may include closing the zipper and applying a security label proximate the zipper, the security label providing the visual evidence.

In an alternate embodiment, the step of sealing the container may include thermally sealing the container. Additionally, the step of sealing the container may further include leaving a small gap in the container to accommodate an accessory for the device.

In some embodiments, the method may further include the steps of allowing the user to enter the secure area with the sealed container; receiving the sealed container from the user; visually inspecting the sealed container for signs of tampering; if no signs of tampering are detected, unsealing the container; and returning the device to the user.

In other embodiments, the container may be a plastic bag; and the sealing step includes providing a flexible cable slidably attached to the bag, a slider coupled to the cable such that moving the slider along the cable in a first direction closes the bag, and a security seal attached across the cable adjacent the slider, the security seal providing the visible evidence.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Figure 1 illustrates a plan view of one embodiment of a system to prevent the taking of photographs according to the present invention;

Figure 2 illustrates a plan view of the system of Figure 1 including a device capable of taking photographs;

Figure 3 illustrates a close-up plan view of a photograph taken using the system of Figures 1 and 2;

- 5 Figures 4a and 4b illustrate a plan view of an alternate embodiment of a system to prevent the taking of photographs according to the present invention; and

Figure 5 illustrates a flow chart of one embodiment of a method to prevent the taking of photographs in secure areas using the systems of Figures 1-4.

10

DETAILED DESCRIPTION

- 15 Figure 1 illustrates one embodiment of a system 100 that allows a person to enter areas where the taking of pictures is restricted or prohibited, without having to surrender communications devices capable of taking pictures. Figure 2 illustrates a plan view of the system 100 including a device capable of taking photographs.

- 20 With reference to Figures 1 and 2, the system 100 includes a container 102 having an opening 103 that is large enough to receive a device 106 that is capable of taking photographs. In this embodiment, the system 100 includes means 104 for sealing the opening 103, as well as means 108 for ensuring that, once sealed, any attempt to open the container 102 and remove the device 106 can be detected. In some
25 embodiments, the container 102 may be a flexible plastic container. A portion 110 of the container 102 is shown in Figure 3. This will be discussed in more detail below.

- 30 In this embodiment, the sealing means 104 can be a "zipper" type device that allows the container 102 to be closed. In some embodiments, the zipper can provide a strong seal that resists tampering, such that the seal does not pull apart. Any attempt to pull the sealed portion apart without using the zipper results in visually apparent damage to the container 102. Once the device 106 is secured in the container 102, the zipper 104 can be used to seal the container 102. In this embodiment, the means 108 to ensure that unauthorized attempts to open the

container 102 can be detected, may be an adhesive backed sticker placed proximate the zipper once the container 102 has been sealed with the device 106 inside. In some embodiments, once this adhesive backed sticker 108 is attached to the container 102 adjacent to the zipper 104, any attempt to remove the sticker 108, or pull apart the seal, may provide a clear visual reference to security personnel that the container 102 has been tampered with. Additional security measures, such as a visual and/or functional inspection of the device 106 to determine if any photographs were taken, may then be conducted. In some embodiments, a small gap 103a in the opening 103 (Figure 2) may be provided to allow a user to access the device 106 using, for example, a hands-free headset or the like, while the device 106 is secured in the container 102.

An alternate embodiment of a system 200 of the present invention is shown in Figures 4a and 4b. In this embodiment, the system 200 includes a flexible container 202 having an opening 203 that is large enough to receive the device 106 that is capable of taking photographs. In this embodiment, the means for sealing the opening 203 can include a cable 204, a slider 206, and a security seal 208.

In the embodiment shown in Figures 4A and 4B, the cable 204 may be slidably attached to top portion of the container 202, with the slider 206 coupled to the cable 204 such that moving the slider 206 towards the container 202 bunches up the top portion of the container 202 to close the container 202 and block the opening 203. The security seal 208 may then be attached across or around the cable 204 such that, any attempt to remove the seal 208 by moving the cable 204 to open the container 202, provides a clear visual reference to security personnel that the container 202 has been tampered with. It is understood that the cable 202 may be any type of line, string, metallic cable, etc. capable of sealing the container 202 such that attempts to tamper with the container 202 may be detected.

Other devices and methods for sealing the container 102 may also be used. By way of example and not limitation, the container 102 may be sealed using a thermal sealer (not shown) that melts both sides of the opening 103 together. In this embodiment, a tag, such as a numbered security seal, may be placed on the container 102 to prevent a user from swapping containers. In order to remove the

device 106, the container 102 can be destroyed, e.g. by ripping. This makes it easy for security personnel to determine if the container 102 has been tampered with in any way.

5 In one embodiment, the flexible container 102 can be a plastic bag made from, by way of example and not limitation, linear low-density polyethylene (LLDPE), high-density polyethylene (HDPE), and other types of plastic suitable for use in plastic bags. In order to prevent the taking of pictures, the plastic may incorporate features that obscure, cloud, or otherwise block the picture-taking capability of the device 106,
10 while still allowing a user to access other functions of the device 106 through the container 102. Figure 3 illustrates a close up view of a portion of the container 102 of Figure 1, designated generally as reference numeral 110, illustrating such features. Portion 110 can include a plurality of fine opaque patterns 112 that scatter the light entering a lens of the device 106. Alternately, the container 102 may be
15 made from an optically opaque material that scatters the light entering a lens of the device 106, while still allowing the user to access other features of the device 106. Similarly, the container 106 may be made from a transparent material incorporating the fine opaque patterns 112. It is understood that combinations of materials and patterns can also be used to prevent the device 106 from taking usable
20 photographs.

In operation of the systems 100, 200, the container 102, 202 may be issued to the carrier of the device 106 when he declares ownership of a camera phone at a guard station at an entrance to a secure facility. Figure 5 illustrates one method, designated
25 generally with reference numeral 300, to prevent the taking of photographs in secure areas using the systems 100, 200. The first step is that a guard or other individual protecting the secure area receives a device 106 capable of taking photographs from a user who desires entrance into the area, as shown with reference numeral 302. Security personnel will then insert the device 106 into a container 102, 202 made from a
30 material that both prevents the device 106 from capturing a clear photographic image and allows a user to access to other features of the device 106, as shown with reference numeral 304. Examples of such other features can include, but are not limited to, telephone features, internet features, any other type of communications features, or other features of the device that do not involve the

capability to take photographs. Security personnel then seal the container 102, 202, using any of the sealing means discussed above, as shown with reference numeral 306, and return the sealed container 102, 202 to the user, as shown with reference numeral 308.

5

For example, as discussed above, security personnel may seal the container 102 using, for example, the zipper 104 and adhesive security label 108 shown in Figure 2. The container 102 then functions to prevent the user of the device 106 from taking a clear picture. However, the container 102 does not prevent the user from using other features
10 associated with the device 106. The container 102 also prevents the user from directly accessing/removing any memory modules stored in the device 106, such as various types of memory storage cards known to those of skill in the art.

If the secure facility also has rules concerning the introduction of other small items, such as, but not limited to, additional memory storage cards, these items can also be placed
15 in the container 102, 202 prior to sealing. This feature may eliminate the need to provide storage lockers, etc. to those working at the site. Additionally, if the secure facility requires that a visitor or employee use some type of access or identification card, these cards can also be placed within the container 102, 202 to further streamline the
20 access process.

In optional steps, the user is then allowed to enter the secured area carrying the sealed container 102, 202, as shown with reference numeral 310. When leaving the premises, the carrier/user returns the container 102, 202 to security personnel, together with any
25 security pass, as shown with reference numeral 312. The security guard can then visually inspect the container 102, 202 for signs of tampering, as shown with reference numeral 314. If no signs of tampering are discovered, the security guard can then unseal the container 102, 202, as shown with reference numeral 316, and return the device to the user, as shown with reference numeral 318.

30

Embodiments of the systems and method of the present invention provide several advantages over the prior art. First, there is no longer a need for security personnel to account for devices capable of taking photographs, either by inventory or by providing a secure storage space for the device while the user is inside the secure facility. The

storage facilities can then be used for other purposes instead of being overwhelmed with numerous photographic devices. Additionally, the user still has access to the device, allowing them, for example, to still make and receive incoming phone calls on their camera phone, without compromising the security of the installation. Efforts and time saved in the process of issuing keys for the mobile phone storage cabinet can be devoted to other security activities such as the checking of bags.

The system and method also encourage employees and visitors to declare the devices, as they still can continue to use them on the premises without breaking the rules. The system and method further preclude a user from using the memory slots on the device. Finally, the system and method provide additional common storage for control items such as the memory devices and a security pass with little inconvenience to the owner.

It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. A system to prevent the taking of photographs in unauthorized areas, the system comprising:

5 a container for receiving a device capable of taking photographs, the container comprising a material that prevents the device from capturing a clear photographic image and allows a user to access other features of said device while said device is inside said container; and

10 means for sealing said container such that an attempt to remove said device from said container leaves visible evidence.

2. The system of claim 1, wherein said container comprises a zip-lock type plastic bag.

15 3. The system of claims 1 or 2, wherein said means for sealing comprises a tamper-resistant zipper and a security label located proximate said zipper in a closed configuration, said security label providing said visible evidence.

20 4. The system of claims 1 or 2, wherein said means for sealing comprises a thermal sealing device.

5. The system of claim 1, wherein:

said container comprises a plastic bag; and

25 said means for sealing comprises a flexible cable slidably attached to said bag, a slider coupled to said cable such that moving the slider along the cable in a first direction closes the bag, and a security seal attached across said cable adjacent said slider, said security seal providing said visible evidence.

30

6. The system of any one of claims 2 to 5, wherein said plastic bag comprises Linear low-density polyethylene (LLDPE) or High-density polyethylene (HDPE).

7. The system of any one of the previous claims, wherein said device is a camera, a cellular telephone capable of taking pictures, a personal digital assistant, or a music player.
- 5 8. The system of any one of the previous claims, further comprising a small opening in said container to allow the use of accessories for the device.
9. A method to prevent the taking of photographs in secure areas, the method comprising the steps of:
 - 10 receiving a device capable of taking photographs from a user;
inserting said device into a container, the container comprising a material that prevents the device from capturing a clear photographic image and allows a user to access to other features of said device while said device is inside said container;
 - 15 sealing said container such that an attempt to remove said device from said container leaves visible evidence; and
returning said sealed container to said user.
- 10 10. The method of claim 9, wherein said flexible container comprises a zip-lock type plastic bag.
11. The method of claim 10, wherein said container further comprises a tamper-resistant zipper, and the step of sealing said container comprises closing said zipper and applying a security label proximate said zipper,
 - 25 said security label providing said visual evidence.
12. The method of claims 9 or 10, wherein the step of sealing said container comprises thermally sealing said container.
- 30 13. The method of any one of claims 9-12, wherein the step of sealing said container further comprises leaving a small gap in said container to accommodate an accessory for said device.

14. The method of any one of claims 9-13, further comprising allowing said user to enter said secure area with said sealed container.

15. The method of any one of claims 9-14, further comprising:

5 receiving said sealed container from said user;
 visually inspecting said sealed container for signs of tampering;
 if no signs of tampering are detected, unsealing said container; and
 returning said device to said user.

10 16. The method of any one of claims 9-15, wherein:

 said container comprises a plastic bag; and
 said sealing step comprises providing a flexible cable slidably
 attached to said bag, a slider coupled to said cable such that moving
 the slider along the cable in a first direction closes the bag, and a
 15 security seal attached across said cable adjacent said slider, said
 security seal providing said visible evidence.