US 20160314666A1

(19) **United States**

(12) **Patent Application Publication**

Oh et al.

(10) **Pub. No.: US 2016/0314666 A1**

(43) **Pub. Date: Oct. 27, 2016**

(54) **SECURITY VIDEO DETECTION OF PERSONAL DISTRESS AND GESTURE COMMANDS**

(71) Applicant: **Honeywell International Inc.**, Morristown, NJ (US)

(72) Inventors: **Eric Oh**, Syosset, NY (US); **David S. Zakrewski**, Babylon, NY (US); **Mi Suen Lee**, Hales Corners, WI (US)

(21) Appl. No.: **15/197,214**

(22) Filed: **Jun. 29, 2016**

Related U.S. Application Data

(63) Continuation of application No. 12/950,095, filed on Nov. 19, 2010, now Pat. No. 9,432,639.

Publication Classification

(51) **Int. Cl.**

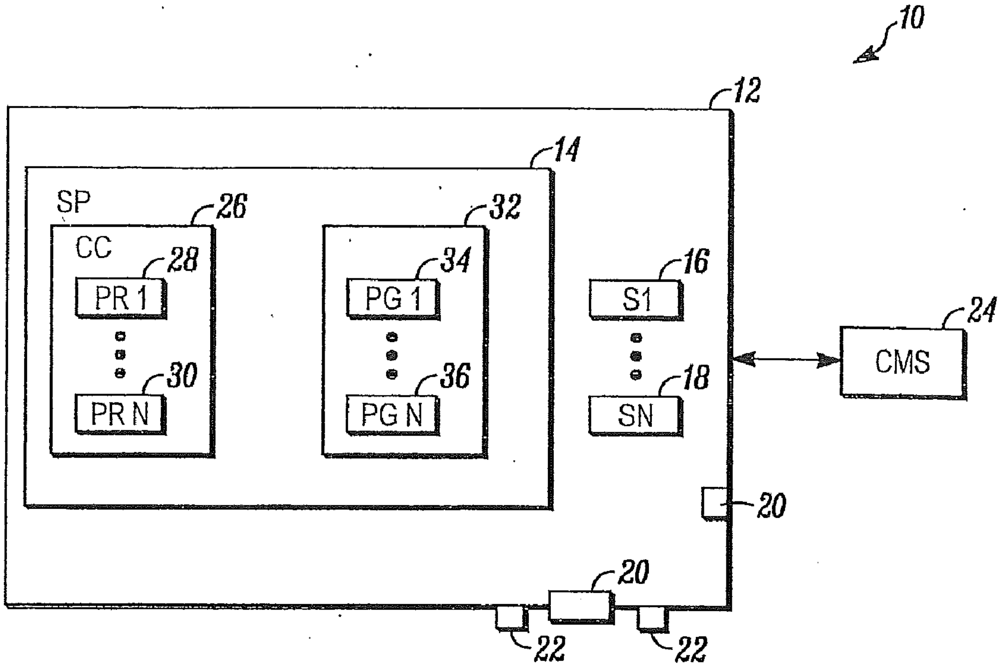
G08B 13/196	(2006.01)
G06K 9/00	(2006.01)

(52) **U.S. Cl.**

CPC ***G08B 13/19608*** (2013.01); ***G06K 9/00771*** (2013.01); ***G06K 9/00885*** (2013.01); ***G06K 9/00389*** (2013.01); ***G08B 13/19613*** (2013.01)

(57) **ABSTRACT**

Systems and methods for detecting personal distress and gesture commands in security video are provided. Some methods can include receiving a sequence of images from a video device monitoring a secured area, analyzing the sequence of images to detect a presence of a human in the sequence of images, when the presence of the human is detected in the sequence of images, analyzing the sequence of images to detect one of a plurality of contexts that requires action in the sequence of images, and when the one of the plurality of contexts that requires the action is detected in the sequence of images, transmitting a signal to execute the action. Each of the plurality of contexts can include an act performed by the human or a condition of the human irrespective of the human being in motion or being stationary.



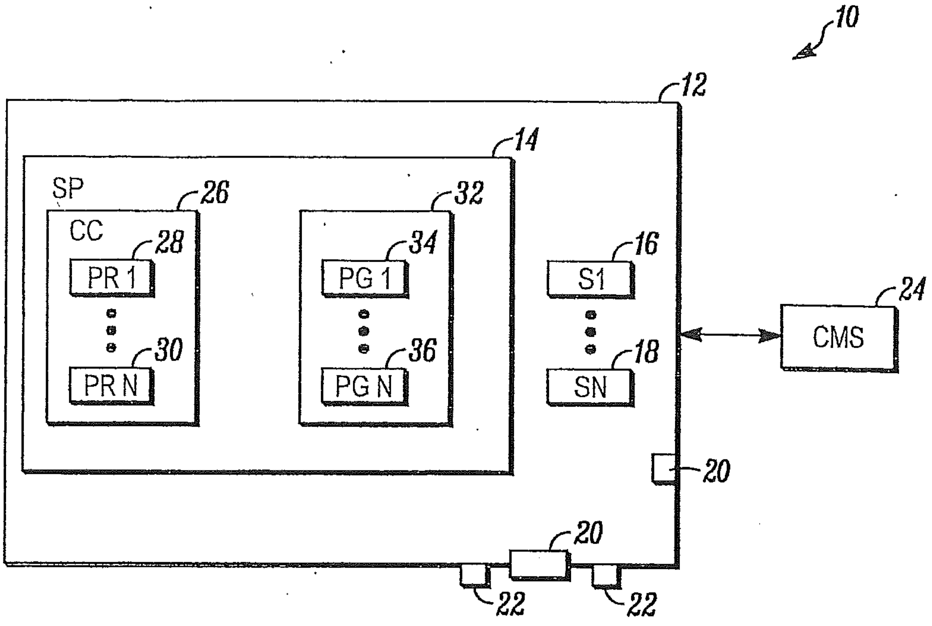

10
12
14
SP
26
CC
28
PR 1
30
PR N
32
34
PG 1
36
PG N
16
S1
18
SN
24
CMS
20
20
22
22

FIG. 1

SECURITY VIDEO DETECTION OF PERSONAL DISTRESS AND GESTURE COMMANDS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of and claims the benefit of the filing date of U.S. application Ser. No. 12/950,095 filed Nov. 19, 2010.

FIELD OF THE INVENTION

[0002] The field of the invention relates to security systems and more particularly to video monitoring in security systems.

BACKGROUND OF THE INVENTIONS

[0003] Security systems are generally known. Such systems typically include some form of physical barrier to intruders, including one or more sensors to detect intruders who are able to surmount the barrier.

[0004] In the case of a home, the physical barrier may be the exterior walls of the home. In this case, the sensors may include door sensors that detect the opening or closing of the doors. Window sensors may also be provided to detect intruders who attempt to enter through a window.

[0005] The sensors within a home are typically electrical switches that are mechanically connected to a door or window. In other cases, motion detectors may be used that are based upon infrared detection of human intruders or the processing of video signals to detect human shapes.

[0006] Security systems typically operate in three modes including disarmed, alarm away and alarm stay. In the disarmed mode, the control panel does not report a burglary alarm when a sensor is activated, while in the alarm away mode the control panel sounds an alarm when a sensor is activated and may report the alarm to a central monitoring station. In the alarm stay (used during night time hours when a homeowner is present), the control panel may only monitor sensors along a periphery of the home.

[0007] While alarm systems are effective, authorized users may still be vulnerable to attack when they enter or exit the secured area. Accordingly, a need exists for better ways of protecting users of security systems.

BRIEF DESCRIPTION OF THE DRAWING

[0008] FIG. **1** is a block diagram of a security system shown generally in accordance with an illustrated embodiment of the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATED EMBODIMENT

[0009] FIG. **1** is a block diagram of a security system **10** shown generally in accordance with an illustrated embodiment of the invention. The security system **10** may include a secured area **12** protected via a security panel **14** and one or more intrusion sensors **16**, **18**. One or more access points (e.g., doors) **20** may be provided for entry into and egress from the secured area **12**.

[0010] Included within the control panel **16** may be control circuitry **26** for controlling the security system **10**. The control circuitry **26** may include one or more computer processors **28**, **30** operating under control of one or more sets of computer program code (programs) **34**, **36** executing on the processors **28**, **30** or saved in a non-transitory computer readable medium **32**.

[0011] The secured area **12** may also include a number of video monitoring and collection devices (e.g., cameras) **20**, **22**. The video devices **20**, **22** may be used for real time monitoring by security personnel. Alternatively, a video based, motion detection processor **28**, **30** within the security panel **16** may receive video from one of the devices **20**, **22** and process the video to detect intruders by detecting changes between successive frames of video.

[0012] The security system **10** may operate in one or more modes including an alarm away mode, an alarm stay mode and a disarmed mode. In the alarm away mode, a alarm processor **28**, **30** may monitor all of the intrusion sensors **16**, **18** and any video based motion detection processors **28**, **30** for activation by an intruder. In the alarm stay mode, the alarm processor **28**, **30** only monitors sensors **16**, **18** around a perimeter of the secured area **12**. In response to activation of one of the sensors **16**, **18**, the alarm processor **28**, **30** may compose and send an alarm message to a central monitoring station **24**. The central monitoring station may respond by dispatching a private security service or by notifying a local police department.

[0013] The security system **10** may be controlled via a keypad and display **22**. The keypad and display may be separate devices or may be combined in the form of a touch sensitive display **22**. The display **22** may be located outside the secured area **12** as shown in FIG. **1** or may be inside.

[0014] In order to activate a particular operating mode within the security system **10**, an authorized user may enter an identifying code and then activate a mode selection button on the display **22**. For example, the user may enter the number sequence 1, 2, 3, 4 and activate the softkey labeled "ALARM AWAY." In response, the alarm system **10** would enter the alarm away mode.

[0015] Included within the alarm system **10** may be one or more human context detection processors **28**, **30** that are programmed to detect human presence within a sequence of images from video devices **20**, **22** and to analyze video frames associated with that presence to detect specific contexts that require further action. The context detection processors **28**, **30** may be particularly useful when used to process video obtained from camera **20**, **22** located adjacent the entrance **20** to the secured area **12**.

[0016] For example, a context detection processor **28**, **30** may be programmed to detect the context of duress and to send a silent alarm to the central monitoring station **24** upon detection of that duress. The detection of duress in this case can mean the detection of a specific physical action or the detection and comparison of a specific biometric parameter with a threshold value.

[0017] It should be specifically noted that the context detection processor **28**, **30** does not operate by detecting locomotion or movement of humans across an image. Instead, the context detection processor **28**, **30** detects specific acts performed by or a specific condition of that person. That being said, it should also be noted that those specific acts or conditions could just as well be detected while the person is in motion as well as when the person is stationary and not moving.

[0018] As a more specific example, if an authorized user were being threatened by a criminal with a weapon in order to coerce the authorized user to disarm the alarm system **10**

in order to allow the criminal access to the secured area **12**, the context detection processor **28**, **30** may be able to detect that context and to generate a silent alarm. The alarm may be silent in order to not jeopardize the safety of the authorized person.

[0019] In general, the context processor **28**, **30** may analyze contexts using a number of specific steps and/or modes. These specific steps or modes may be executed by a single processor **28**, **30** in sequence or by a number of associated processors **28**, **30** programmed to accomplish that step.

[0020] For example, a first processor **28**, **30** (e.g., a human detection processor) functions to detect human figures within video images. If no human figures are detected within the image, then the first processor simply continues to process frames of video from the video devices **20**, **22**.

[0021] Alternatively, if the human detection processor **28**, **30** were to detect first and second human figures, then that processor (or another associated processor **28**, **30**) may begin to process the outlines of those figures to detect threatening gestures or sounds. A threatening gesture could be an upraised arm.

[0022] A threatening sound may be detected by a microphone associated with the video device **20**, **22**. In this case, a sound processor **28**, **30** may first filter sound to isolate those portions of the sound associated with a particular threat. One such threat could be loud voices. Another threatening sound may be gunfire.

[0023] In general, the gestures or sounds may be associated with a threshold level defined by the context. In the case of voices, the threshold level may be set to that of a loud voice or shouting. In the case of a gesture such as an upraised arm, the threshold may be associated with the speed with which the arm was raised and/or the speed of any downward motion that follows raising the arm.

[0024] In addition, the gestures and sounds may be logically ANDed with or supplanted by other contexts or context parameters. One context parameter is the detection of a weapon. In this regard, a processor (e.g., a weapons processor) **28**, **30** may identify the distal end of a human figure's arm and process the distal end for any unusual image details that could be construed as a weapon. In this regard, the detection of a gun is relatively straightforward. On the other hand, the detection of a rock held in the hand of a criminal would be less conclusive. In this case, a threat factor or value may be assigned to this image detail that is added to other threat factors or values (e.g., loud voices, speed of arm movement, etc.). A threshold value may be used in conjunction with the summation of threat factors or values.

[0025] Another context parameter may be biometric. In one example, the video devices **20**, **22** may collect heat signatures of portions of the human figures (e.g., the face). The heat signature of the face may be compared with a threshold value to again determine if the threat factor exceeds an associated threshold value.

[0026] Another processor **28**, **30** (e.g., a face recognition processor) may be programmed to compare a face portion of detected human figures with templates of authorized users to recognize an authorized user from within a group of two or more human figures. In this case, the heat signature of a recognized authorized user may be taken as a sign of duress where the heat signature exceeds a threshold value for that user.

[0027] Another processor **28**, **30** (e.g., a gesture processor) may be programmed to identify predefined actions by authorized users that have already been (or concurrently) identified by the face recognition processor **28**, **30**. In this case, an authorized user may preprogram or define certain overt gestures as a sign of duress. For example, the act of an authorized user placing the palm of his/her hand over their face with fingers spread and holding their hand there for some predefined period while that person approaches the entrance **20** may be a predetermined gesture of duress.

[0028] Alternatively, repetitive acts may be a predefined indicator of duress. For example, the authorized user placing his/her forefinger to his/her nose twice in a predefined period may be one of the predefined indicators of duress.

[0029] As a still further alternative, predefined actions by an authorized user may be used to execute certain processes by the alarm system **10** as a convenience to the authorized user or to defuse a situation where the authorized user feels threatened. For example, if the authorized user is approached by a stranger while attempting to enter the secured area **12**, the authorized user may perform the predefined action in order to cause the security system **10** to perform the process associated with that predefined act. The process performed in response to the predefined act may be for the system **10** to provide an audio announcement through a speaker located adjacent the entrance **20** that the security system **10** is armed. Alternatively, the process may involve the security system **10** announcing that a video recording is being made of all actions at that location. In this case, the announcement may operate as a deterrent to the approaching stranger intent on performing some criminal act.

[0030] As a still further alternative, a processor **28**, **30** (e.g., a fight detection processor) may be programmed to detect a fight between two detected humans. In this case, the momentary merging of the detected human figures and speed of motion of the appendages of the detected human figures may cause the fight detection processor to detect a fight and then compose and send an alarm message to the central monitoring station announcing the fight. This may be a lower level alarm message since it is outside the secured area **12** unless one of the figures can be identified as an authorized user. If one of the participants is an authorized user, then a higher level alarm is sent since this may be a criminal assault on the authorized user or an attempt to gain access to the secured area **12**.

[0031] A specific embodiment of a method and apparatus for detecting intruders has been described for the purpose of illustrating the manner in which the invention is made and used. It should be understood that the implementation of other variations and modifications of the invention and its various aspects will be apparent to one skilled in the art, and that the invention is not limited by the specific embodiments described. Therefore, it is contemplated to cover the present invention and any and all modifications, variations, or equivalents that fall within the true spirit and scope of the basic underlying principles disclosed and claimed herein.

1-20. (canceled)

21. A method comprising:

receiving a sequence of images from a video device monitoring a secured area;

analyzing the sequence of images to detect a presence of a human in the sequence of images;

when the presence of the human is detected in the sequence of images, analyzing the sequence of images to detect one of a plurality of contexts that requires action in the sequence of images; and when the one of the plurality of contexts that requires the action is detected in the sequence of images, transmitting a signal to execute the action,

wherein each of the plurality of contexts includes an act performed by the human or a condition of the human irrespective of the human being in motion or being stationary.

22. The method of claim **21** wherein the one of the plurality of contexts includes duress, and wherein transmitting the signal to execute the action includes transmitting a silent alarm to a central monitoring station or providing an audio announcement through a speaker adjacent the video device.

23. The method of claim **22** further comprising detecting a physical action or a threatening gesture by the human in the sequence of images, wherein the physical action or the threatening gesture indicates the duress.

24. The method of claim **23** wherein the threatening gesture indicates the duress when the threatening gesture exceeds a predetermined threshold value.

25. The method of claim **22** further comprising:

detecting a biometric parameter of the human in the sequence of images; and

comparing the biometric parameter to a predetermined threshold value,

wherein the biometric parameter indicates the duress when the biometric parameter exceeds the predetermined threshold value.

26. The method of claim **22** wherein the human includes an authorized user of a security system monitoring the secured area.

27. The method of claim **26** further comprising detecting an unauthorized user or a weapon threatening or fighting with the authorized user in the sequence of images, wherein the unauthorized user or the weapon threatening or fighting with the authorized user indicates the duress.

28. The method of claim **22** further comprising detecting a threatening sound captured by a microphone associated with the video device, wherein the threatening sound indicates the duress.

29. The method of claim **28** wherein the threatening sound indicates the duress when the threatening sound exceeds a predetermined threshold value.

30. The method of claim **22** further comprising:

detecting multiple ones of the plurality of contexts that require action in the sequence of images;

assigning a threat value to each of the detected multiple ones of the plurality of contexts;

identifying a total threat value by adding each of the threat values assigned to the detected multiple ones of the plurality of contexts; and

comparing the total threat value to a predetermined threshold value, wherein the total threat value indicates the duress when the total threat value exceeds the predetermined threshold value.

31. A system comprising:

a programmable processor; and

executable control software stored on a non-transitory computer readable medium,

wherein the programmable processor and the executable control software receive a sequence of images from a video device monitoring a secured area,

wherein the programmable processor and the executable control software analyze the sequence of images to detect a presence of a human in the sequence of images,

wherein, when the programmable processor and the executable control software detect the presence of the human in the sequence of images, the programmable processor and the executable control software analyze the sequence of images to detect one of a plurality of contexts that requires action in the sequence of images,

wherein, when the programmable processor and the executable control software detect the one of the plurality of contexts that requires the action in the sequence of images, the programmable processor and the executable control software transmit a signal to execute the action, and

wherein each of the plurality of contexts includes an act performed by the human or a condition of the human irrespective of the human being in motion or being stationary.

32. The system of claim **31** wherein the one of the plurality of contexts includes duress, and wherein the programmable processor and the executable control software transmitting the signal to execute the action includes the programmable processor and the executable control software transmitting a silent alarm to a central monitoring station or providing an audio announcement through a speaker adjacent the video device.

33. The system of claim **32** wherein the programmable processor and the executable control software detect a physical action or a threatening gesture by the human in the sequence of images, and wherein the physical action or the threatening gesture indicates the duress.

34. The system of claim **33** wherein the threatening gesture indicates the duress when the threatening gesture exceeds a predetermined threshold value.

35. The system of claim **32** wherein the programmable processor and the executable control software detect a biometric parameter of the human in the sequence of images and compare the biometric parameter to a predetermined threshold value, and wherein the biometric parameter indicates the duress when the biometric parameter exceeds the predetermined threshold value.

36. The system of claim **32** wherein the human includes an authorized user of a security system monitoring the secured area.

37. The system of claim **36** wherein the programmable processor and the executable control software detect an unauthorized user or a weapon threatening or fighting with the authorized user in the sequence of images, and wherein the unauthorized user or the weapon threatening or fighting with the authorized user indicates the duress.

38. The system of claim **32** wherein the programmable processor and the executable control software detect a threatening sound captured by a microphone associated with the video device, and wherein the threatening sound indicates the duress.

39. The system of claim **38** wherein the threatening sound indicates the duress when the threatening sound exceeds a predetermined threshold value.

40. The system of claim **32** wherein the programmable processor and the executable control software detect multiple ones of the plurality of contexts that require action in the sequence of images, assign a threat value to each of the detected multiple ones of the plurality of contexts, identify a total threat value by adding each of the threat values assigned to the detected multiple ones of the plurality of contexts, and compare the total threat value to a predetermined threshold value, and wherein the total threat value indicates the duress when the total threat value exceeds the predetermined threshold value.

* * * * *