METHOD AND SYSTEM FOR CONFIGURABLE SECURITY AND SURVEILLANCE SYSTEMS

FIELD OF THE INVENTION

[01] Certain embodiments of the invention relate to security systems. More specifically, certain embodiments of the invention relate to a method and system for configurable security and surveillance systems.

BACKGROUND OF THE INVENTION

[02] Security and surveillance systems are becoming an important aspect of modern society. In addition to providing security measures that protect assets and individuals in commercial and residential settings, security and surveillance systems may also be adapted to improve the efficiency and versatility of processes, and/or procedures in a variety of businesses. One important aspect of security and surveillance systems is the need for upgrades and/or maintenance operations. This is generally a cumbersome and costly aspect of providing security measures. Moreover, a great number of new security and surveillance applications may be implemented utilizing wireless technology to support mobile operations. This present an even bigger challenge in terms of upgrades and/or maintenance given that cameras and other equipment may be spread out over a wide geographic area, but in some instances, many of the cameras and other hardware that comprises the system may be mobile and constantly changing locations. In order to provide support to mobile security and surveillance systems, hardware may need to be taken out of the system for upgrades and/or maintenance, reducing the protective measures that may be provided by the security and surveillance system.

[03] Security and surveillance operations may require security management systems that are capable of providing either a single security function or, in some instances, a wide range of integrated security functions. Most security management systems, however, are designed to operate as autonomous systems that provide a single security function

such as intrusion detection, access control, or audio and/or video surveillance and recording, for example. These security management systems may not generally support the addition of other security functions and/or the addition of other features to an existing security function without a substantial investment in hardware and/or software. As a result, multiple security management systems are generally utilized when a particular application requires multiple security functions. In this regard, any integration that may be necessary to efficiently and/or effectively operate multiple security management systems is typically left to an installer, an integrator, and/or the customer to carry out.

[04] One of the needs driving security management systems capable of supporting a wide range of integrated security functions and/or features are security operations for large enterprises or entities. These large entities may have many different security requirements extending over multiple locations. A centrally monitored integrated security management system may allow administrators or controllers at a central control center to efficiently oversee the many security activities that are supported at the remote facilities.

[05] The limited ability of most security management systems to add security functions, to add features to existing security functions, and/or to easily integrate with other security management systems generally results in an inefficient use of available resources. For example, multiple security management systems that have not been efficiently integrated may have multiple data entry points and/or duplicate databases. Moreover, limited integration capability may also create inefficient use of personnel by duplicating data entry tasks, requiring manual data exchange between systems, and implementing multiple training requirements for the various systems being utilized. Moreover, even when integration between multiple security management systems has been effectively implemented, continued compatibility may be lost when hardware and/or software on various portions of at least one of the multiple security management systems is upgraded.

[06] A common security function that is generally provided in security management systems is video surveillance. Video surveillance operations may require, in some instances, to be provided with additional features or may require compatibility with other security functions. Most video surveillance operations are provided by stand-alone closed circuit television (CCTV) systems that are commonly found in, for example, office buildings, external structures, schools, railway stations, and even on city streets. An effectively integrated security management systems may require that a CCTV system be compatible with other security functions such as access control methods augmented with biometrics, security tracking systems, and/or access tracking systems, for example. However, most CCTV systems are not easily upgradable nor are they easily integrated with other security functionality. As a result, integrated security management systems comprising video surveillance operations are not readily available. Moreover, the ability of these integrated security management systems to evolve and provide further security functions and/or additional features are generally limited or may be accomplished only with a substantial investment in hardware and/or software.

[07] Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of skill in the art, through comparison of such systems with some aspects of the present invention as set forth in the remainder of the present application with reference to the drawings.

BRIEF SUMMARY OF THE INVENTION

[08] A system and/or method for configurable security and surveillance systems, substantially as shown in and/or described in connection with at least one of the drawings, as set forth more completely in the claims.

[09] Various advantages, aspects and novel features of the present invention, as well as details of an illustrated embodiment thereof, will be more fully understood from the following description and drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[10] FIG. 1A illustrates an exemplary analog security and surveillance system, in connection with an embodiment of the invention.

[11] FIG. 1B illustrates an exemplary Internet protocol (IP)-based security and surveillance system, in connection with an embodiment of the invention.

[12] FIG. 2A illustrates an exemplary configurable security and surveillance system with programmable sensor agents, in accordance with an embodiment of the invention.

[13] FIG. 2B illustrates an exemplary configurable security and surveillance system with programmable sensor agents and a programmable content analysis agent, in accordance with an embodiment of the invention.

[14] FIG. 2C illustrates an exemplary configurable security and surveillance system with programmable sensor agents, programmable content analysis agent, and an access controller, in accordance with an embodiment of the invention.

[15] FIG. 3 illustrates an exemplary network comprising a configurable security and surveillance system and an e-commerce vendor, in accordance with an embodiment of the invention.

[16] FIG. 4A is a block diagram of an exemplary programmable sensor agent, in accordance with an embodiment of the invention.

[17] FIG. 4B is a block diagram of an exemplary programmable sensor agent adapted to generate descriptors, in accordance with an embodiment of the invention.

[18] FIG. 4C is a flow diagram illustrating exemplary steps for configuring a programmable sensor agent, in accordance with an embodiment of the invention.

[19] FIG. 5A is a block diagram of an exemplary programmable content analysis agent, in accordance with an embodiment of the invention.

[20] FIG. 5B is a flow diagram illustrating exemplary steps for configuring a programmable content analysis agent, in accordance with an embodiment of the invention.

[21] FIG. 6A illustrates an exemplary network comprising a residential configurable security and surveillance system, in accordance with an embodiment of the invention.

[22] FIG. 6B illustrates an exemplary network comprising a commercial configurable security and surveillance system, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[23] Certain embodiments of the invention may be found in a method and system for a configurable security and surveillance system. In accordance with an embodiment of the invention, a configurable security and surveillance system may comprise at least one programmable sensor agent and/or at least one programmable content analysis agent. A plurality of processing features may be offered by the configurable security and surveillance system by programming configurable hardware devices in the programmable sensor agents and/or the programmable content analysis agents via a system manager. Device programming files may be utilized to program the configurable hardware devices. The device programming files may be encrypted, and decryption keys may be requested to enable the programming of different processing features into the programmable sensor agents and/or the programmable content analysis agents. The device programming files and/or the decryption keys may be received via a network transfer and/or via a machine-readable media from an e-commerce vendor.

[24] FIG. 1A illustrates an exemplary analog security and surveillance system, in connection with an embodiment of the invention. Referring to FIG. 1, there is shown an analog security and surveillance system 100 that comprises at least one analog camera 102, a camera control unit 104, a multiplexer 106, a system manager 110, and a videocassette recorder

(VCR) 108. The analog camera 102 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to capture video information from a particular location. The analog camera 102 may receive control signals from the camera control unit 104 that may be utilized to control various operations, for example, zoom, tilt, and/or pan. The analog camera 102 may generate at least one video signal that corresponds to the video information captured by the analog camera 102. In some instances, the analog camera 102 may provide front end processing of the video information before generating the video signal. The analog camera 102 may transfer at least a portion of the generated video signal to the multiplexer 106. The video signals may be transferred to the multiplexer 106 via coaxial cables, for example.

[25] The system manager 110 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to allow a user to control the operation of an analog camera 102, to control the recording of at least a portion of the video signals generated by an analog camera 102, and to display at least a portion of the video information in the video signals generated by an analog camera 102. In this regard, the system manager 110 may be utilized to control at least a portion of the operation of the camera control unit 104, the multiplexer 106, and/or the VCR 108. The camera control unit 104 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to receive control information from the system manager 110 via the multiplexer 104 and to generate control signals from the received control information. The generated control signals may be transferred to at least one analog camera 102 to control its operation.

[26] The multiplexer 106 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to select a mode of operation. For example, during a recording mode, the multiplexer 106 may receive video information from at least one analog camera 102 and may transfer that video information to the VCR 108. During a playback mode, for example, the multiplexer 108 may retrieve stored video information from the VCR 108

and may transfer the video information to a display portion of the system manager 110. The display portion of the system manager 110 may display the video information from at least one analog camera 102 at the same time. During a control mode, for example, the system manager 110 may transfer control information to the camera control unit 104 via the multiplexer 106. During a display mode, for example, the video information received from at least one analog camera 102 may be displayed directly to the display portion of the system manager 110. In some instances, the multiplexer 106 may be adapted to have more than one mode of operation active at the same time. For example, the recording mode and display mode may be utilized at the same time to record and display video information onto the VCR 108 and the display portion of the system manager 110 respectively.

[27] FIG. 1B illustrates an exemplary Internet protocol (IP)-based security and surveillance system, in connection with an embodiment of the invention. Referring to FIG. 1B, there is shown an IP-based security and surveillance system 120 that comprises at least one analog camera 102 as described in FIG. 1A, an IP network 112, a video server 122, at least one IP-based digital camera 124, a router 126, a transfer control protocol/Internet protocol (TCP/IP) network 128, a system manager 130, and a data storage device 132. The analog camera 102 may be as described in FIG. 1A. The IP network 112 may be a communication network that may be implemented as a local area network (LAN), a wide area network (WAN), a campus area network (CAN), a metropolitan area network (MAN), and/or a home area network (HAN), for example. The IP network 112 may be a wireline and/or a wireless network and components coupled to the IP network 112 may be coupled via a wireline and/or a wireless connection.

[28] The video server 122 may comprise suitable logic, circuitry, code and/or hardware that may be adapted to receive video information from at least one analog camera 102 and to transfer control information to at least one analog camera 102. The video server 122 may be communicatively

coupled to the IP network 112 via a wireline and/or a wireless connection. The video server 122 may also be adapted to compress the video information received from an analog camera 102 and transfer the compressed video information to the system manager 130 and/or the data storage device 132, for example. The video server 122 may correspond to a specified network address in the IP network 112.

[29] The IP-based digital camera 124 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to capture video information and transfer video information to the IP network 112. The IP-based digital camera 124 may be adapted to receive control information via the IP network 112. The IP-based digital camera 124 may comprise an image sensor, an image processor, and a compression engine. The image sensor may be, for example, a complementary metal-oxide-semiconductor (CMOS) image sensor or a charge-coupled device (CCD) image sensor and may be adapted to capture video information. The image processor may be, for example, a digital signal processor (DSP) or a dedicated application specific integrated circuit (ASIC) and may be adapted to perform front-end processing of the video information captured by the image sensor. The compression engine may comprise suitable logic, circuitry, and/or code that may be adapted to encode the processed video information before transfer to the IP network 112. The control information received by the IP-based digital camera 124 may be utilized to control, for example, zoom, tilt, and/or pan operations. Each IP-based digital camera 124 may correspond to a specified network address in the IP network 112.

[30] The router 126 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to communicatively couple the IP network 112 with the TCP/IP network 128. The router 126 may transfer at least a portion of the video information captured by at least one analog camera 102 and/or at least one IP-based digital camera 124 and a portion of the control information generated by the system manager 130 to a device, component, and/or element communicatively coupled to the TCP/IP network 128. The router 126 may correspond to a specified network address in the IP network

112. The TCP/IP network 128 shown in FIG. 1B may correspond to, for example, the Internet.

[31] The data storage device 132 may comprise suitable logic, circuitry, and/or code that may be adapted to store at least a portion of the video information captured by at least one analog camera 102 and/or at least one IP-based digital camera 124. In some instances, the data storage device 132 may be part of a network attached storage (NAS) and/or a storage area network (SAN), for example. The data storage device 132 may correspond to a specified network address in the IP network 112.

[32] The system manager 130 may comprise suitable logic, circuitry, and/or code that may be adapted to control the operation of at least one analog camera 102 and/or at least one IP-based digital camera 124. In this regard, the system manager 130 may generate control information that may be transferred to at least one analog camera 102 and/or at least one IP-based digital camera 124 via the IP network 112. The system manager 130 may also display at least a portion of the compressed video information captured by an analog camera 102 and/or an IP-based digital camera 124. Moreover, the system manager 130 may receive information stored in the data storage device 132 and may process and/or display the received information. The system manager 130 may correspond to a specified network address in the IP network 112.

[33] FIG. 2A illustrates an exemplary configurable security and surveillance system with programmable sensor agents, in accordance with an embodiment of the invention. Referring to FIG. 2A, there is shown a configurable security and surveillance system 200 that comprises a first programmable sensor agent 202, a second programmable sensor agent 204, a third programmable sensor agent 206, a system manager 208, a data storage device 210, and a network 212. The network 212 may comprise suitable hardware that may be adapted to communicatively couple a plurality of components, devices, and/or elements. In this regard, the components, devices, and/or elements coupled to the network 212 may correspond to specified network address and/or network locations in the

network 212. The network 212 may be, for example, a TCP/IP network, but need not be so limited. In some instances, portions of the network 212 may be implemented as wireless connections while other portions may be implemented as wireline connections. Moreover, components communicatively coupled to the network 212 may be coupled via wireline or wireless connections, for example.

[34] The first programmable sensor agent 202, the second programmable sensor agent 204, and the third programmable sensor agent 206 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to detect a physical event, generate at least one signal that corresponds to the physical event detected, and transfer the generated signal to the data storage device 210 and/or the system manager 208 via the network 212. Three different types of programmable sensor agents are shown in FIG. 2A as examples to indicate that a plurality of programmable sensor agent types may be utilized to detect different physical events. As a result, the types and the number of programmable sensor agents may depend on the security functions that need to be integrated in the configurable security and surveillance system 200. For example, a programmable sensor agent may correspond to a surveillance camera, a thermal sensor, or a biological/chemical sensor. In the example illustrated in FIG. 2A, each of the programmable sensor agents 202, 204, and 206 may correspond to a specified network address in the network 212.

[35] A programmable sensor agent may be adapted to receive control information from the system manager 208 via the network 212. Moreover, a programmable sensor agent may be adapted to be programmed or configured by the system manager 208. In this regard, the programming or configuration may be performed to add and/or remove features that correspond to a security function or functions performed by a programmable sensor agent. The programming or configuration may be performed dynamically, that is, while the configurable security and surveillance system 200 is in operation. In other instances, the programming or configuration may be performed during installation or

during maintenance periods when at least a portion of the configurable security and surveillance system 200 is not in operation.

[36] The data storage device 210 may comprise suitable logic, circuitry, and/or code that may be adapted to store at least a portion of the signals generated by the programmable sensor agents. In some instances, the data storage device 210 may be part of a network attached storage (NAS) and/or a storage area network (SAN), for example. The data storage device 210 may correspond to a specified network address in the network 212. In some instances, more than one data storage device 210 may be utilized in the configurable security and surveillance system 200.

[37] The system manager 208 may comprise suitable logic, circuitry, and/or code that may be adapted to control the operation of at least one of the programmable sensor agents in the configurable security and surveillance system 200. In this regard, the system manager 208 may generate control information that may be transferred to the programmable sensor agents via the network 212. The system manager 208 may also be adapted to display at least a portion of the information in the signals generated by the programmable sensor agents. Moreover, the system manager 208 may receive information stored in the data storage device 210 and may process and/or display the information received from the data storage device 210. The system manager 210 may correspond to a specified network address in the network 212.

[38] The system manager 208 may also be adapted to program or configure security features into the programmable sensor agents in the configurable security and surveillance system 200. In this regard, the system manager may receive device programming files that may be utilized to program or configure a portion of the programmable sensor agents in order to provide new, additional, and/or upgraded security features. The device programming files may be transferred to the corresponding programmable sensor agents via the network 212. In some instances, the device programming files received by the system manager 208 may be encrypted or protected. When the device programming files are encrypted,

the system manager 208 may receive at least one decryption key or password that may be utilized to decrypt the encrypted device programming files or to gain access to the device programming files. In this regard, encryption and protection may be substantially similar restrictions on the device programming files that they may be referred to interchangeably. When the device programming files have been decrypted, the system manager 208 may transfer the device programming files to the corresponding programmable sensor agents via the network 212.

[39] The system manager 208 may also be adapted to execute code or software that may be adapted to perform control, management, and/or maintenance operations that may be utilized in the operation and/or the configuration of the configurable security and surveillance system 200.

[40] FIG. 2B illustrates an exemplary configurable security and surveillance system with programmable sensor agents and a programmable content analysis agent, in accordance with an embodiment of the invention. Referring to FIG. 2B, there is shown a configurable security and surveillance system 220 that differs from the configurable security and surveillance system 200 in FIG. 2A in that a programmable content analysis agent 214 is shown communicatively coupled to the network 212.

[41] The programmable content analysis agent 214 may comprise suitable logic, circuitry, and/or code that may be adapted to perform sensor analysis operations and/or security analysis operations. For example, sensor analysis operations may comprise, but need not be limited to, processing sensor information, classifying sensor information, and/or generating control information that may be transferred to other programmable sensor agents in the configurable security and surveillance system 220. Security analysis operations may comprise, but need not be limited to, identifying security anomalies, managing emergency situations, providing access control, and/or triggering alarms, for example. The results of sensor analysis operations may be utilized to generate and/or add information to a comprehensive knowledge base that may be utilized by, for

example, the security analysis operations. In this regard, the programmable content analysis agent 214 may store at least a portion of the results generated by the sensor analysis operations. Storage of the results generated by the sensor analysis operations may be local on the programmable content analysis agent 214 and/or on the data storage device 210. The programmable content analysis agent 214 may correspond to a specified network address in the network 212. In some instances, more than one programmable content analysis agent 214 may be utilized by the configurable security and surveillance system 220.

[42] The programmable content analysis agent 214 may also be adapted to receive control information from the system manager 208 via the network 212. Moreover, the programmable content analysis agent 214 may be adapted to be programmed or configured by the system manager 208. In this regard, the programming or configuration may be performed to add, remove, and/or upgrade features that correspond to the sensor analysis operations and/or security analysis operations performed by the programmable content analysis agent 214. The programming or configuration may be performed dynamically, that is, while the configurable security and surveillance system 220 is in operation. In other instances, the programming or configuration may be performed during installation or during maintenance periods when at least a portion of the configurable security and surveillance system 220 is not in operation.

[43] FIG. 2C illustrates an exemplary configurable security and surveillance system with programmable sensor agents, programmable content analysis agent, and an access controller, in accordance with an embodiment of the invention. Referring to FIG. 2C, there is shown a configurable security and surveillance system 230 that differs from the configurable security and surveillance system 220 in FIG. 2B in that an access controller 216 is shown communicatively coupled to the network 212.

[44] The access controller 216 may comprise suitable logic, circuitry, and/or code that may be adapted to provide access to specified locations

based on a verified security clearance. For example, upon keycard and/or biometric information verification, a user may enter a specified location or site in a building or campus covered by the configurable security and surveillance system 230. Access to that area by the user may be further detected by, for example, video surveillance functions provided by at least one programmable sensor agent located in the specified location or site. The programmable sensor agents may transfer information regarding the user to the programmable content analysis agent 214. The programmable content analysis agent 214 may process the user information and may add the results to other information that may have been generated on that user and that may be currently stored information in the programmable content analysis agent 214 and/or in the data storage device 210. A user may be represented by a label in the configurable security and surveillance system 230 and the user label may correspond to a data structure comprising information related that user.

[45] In another example, security and/or emergency personnel may be searching or attempting to locate a specified user. In this regard, the security and/or emergency personnel may query the configurable security and surveillance system 230 by label to locate the specified user. Data available on the data structure that corresponds to the user label may be utilized to accurately determine of the user's location. When additional data is required, the configurable security and surveillance system 230 may send control information to at least a portion of the programmable sensor agents and/or the access controller 216 to obtain additional data that may be utilized to locate the specified user.

[46] The access controller 216 may provide an additional security function to the other security functions, for example, video surveillance, performed by the configurable security and surveillance systems 230. This additional security function may be controlled, at least in part, by the system manager 208. Moreover, the programmable content analysis agent 214 may be utilized to integrate at least a portion of the access control functions and other security functions.

[47] FIG. 3 illustrates an exemplary network comprising a configurable security and surveillance system and an e-commerce vendor, in accordance with an embodiment of the invention. Referring to FIG. 3, there is shown the configurable security and surveillance system 230 as described in FIG. 2C, a security and surveillance features vendor (SSFV) 300, a first machine-readable media 302, a second machine-readable media 304, a first router 306, a second router 308, and the TCP/IP network 128 as described in FIG. 1B.

[48] The first router 306 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to communicatively couple the network 212 in the configurable security and surveillance system 230 to the TCP/IP network 128. The second router 308 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to communicatively couple the SSFV 300 to the TCP/IP network 128.

[49] The first machine-readable media 302 and the second machine-readable media 304 are examples of media that may be utilized to provide the configurable security and surveillance system 230 with device programming files, decryption keys, and/or operating software or code that may be utilized by the system manager 208, the programmable content analysis agent 214, the data storage device 210, and/or the access controller 216. While the first machine-readable media 302 as shown corresponds to at least one diskette and the second machine-readable media 304 as shown corresponds to at least one optical disk, other machine-readable media may also be utilized in this regard.

[50] The SSFV 300 may be an e-commerce vendor that provides a plurality of features that may be programmed into a programmable agent in the configurable security and surveillance system 230. A programmable agent may refer to a programmable sensor agent such as those represented by the programmable sensor agents 202, 204, and 206 and/or a programmable content analysis agent 214. The SSFV 300 may be adapted to receive requests for device programming files and/or decryption keys that may be utilized to configure or program at least one of the

programmable agents. Decryption keys may be requested from the SSFV 300 when at least a portion of the device programming files is encrypted. The SSFV 300 may transfer any requested programming files and/or decryption keys to the system manager 208 via the TCP/IP network 128 and the network 212. In some instances, the SSFV 300 may transfer any requested programming files and/or decryption keys to the system manager 208 via at least one machine-readable media.

[51] FIG. 4A is a block diagram of an exemplary programmable sensor agent, in accordance with an embodiment of the invention. Referring to FIG. 4A, there is shown a programmable sensor agent 400 that comprises a sensor 402, a first digital reconfigurable processor (DRP) 404, a second DRP 406, and a memory block 408. The sensor 402 may comprise suitable logic, circuitry, code, and/or hardware that may be adapted to detect physical events. For example, for security functions that require video surveillance, the sensor 402 may be a solid-state image sensor that may be implemented utilizing CMOS or CCD technology. The sensor 402 may be adapted to generate at least one signal that corresponds to the detected physical events. The sensor 402 may be also adapted to receive control information and/or to transfer generated signals that correspond to the detected physical events to the first DRP 404.

[52] The first DRP 404 and the second DRP 406 may comprise suitable logic, circuitry, and/or code that may be adapted to provide digital processing. The first DRP 404 and the second DRP 406 may be referred to a configurable devices that may adapted to be configured or programmed in order to provide at least one feature for at least one security function. The first DRP 404 or the second DRP 406 may be a digital signal processor (DSP), a central processing unit (CPU), a field programmable gate array (FPGA), or a complex programmable logic device (CPLD), for example.

[53] The programmable sensor agent 400 may receive at least one device programming file to program or configure at least a portion of the first DRP 404 and/or at least a portion of the second DRP 406. The device programming files may be code, embedded code, firmware, and/or

compiled hardware description language (HDL) code in accordance with the type of configurable device. For example, when utilizing a DSP and/or a CPU as configurable devices, at least a portion of the embedded code that is executed on the configurable device may be configured to provide new, additional, and/or upgraded features. In another example, when utilizing an FPGA and/or a CPLD as configurable devices, at least a portion of the logic in the configurable device may be configured or programmed to provide new, additional, and/or upgraded features. In some instances, an FPGA and/or a CPLD configurable device may be utilized as a processing engine that may be able to support an embedded operating system (OS), such as Linux, for example. In such instances, the logic and/or the embedded code that is executed on the FPGA and/or the CPLD configurable device may be configured or programmed to provide new, additional, and/or upgraded features.

[54] The memory block 408 may comprise suitable logic, circuitry, and/or code that may be adapted to store information generated from the first DRP 404 and/or the second DRP 406. The memory block 408 may also be adapted to transfer stored information to the first DRP 404 and/or the second DRP 406. The memory block 408 may comprise at least one memory device. In some instances, the device programming files may be stored in the memory block 408 and may be transferred to the first DRP 404 and/or the second DRP 406 from the memory block 408.

[55] As shown in FIG. 4A, the programmable sensor agent 400 may be adapted for video surveillance functions. For example, the sensor 402 may capture video information and may provide front-end processing of the captured sensor information. When the sensor 402 is a color image sensor, for example, the front-end operations performed by the sensor 402 may comprise automatic gain control (AGC), color balancing, and/or white balancing. The first DRP 404 may receive the front-end processed video information from the sensor 402, and may perform additional image processing features such as image interpolation, image correction, dynamic range enhancement, and/or noise filtering, for example. The first DRP 404

may also be adapted to generate a processed sensor output from the sensor information.

[56] The second DRP 406 may receive at least a portion of the processed sensor information and may be adapted to provide image analysis and/or failure management for the programmable sensor agent 400. For example, in case of a system failure, the second DRP 404 may activate a backup power source to the programmable sensor agent 400. Moreover, the second DRP 406 may also be adapted to provide maintenance features that may be operated at specified times. For example, the second DRP 406 may be configured or programmed to detect dirt on a lens on the image sensor by analyzing at least a portion of the processed video information generated by the first DRP 404. When the lens is dirty, for example, a signal or message may be sent to the system manager 208 so that further action may be taken.

[57] FIG. 4B is a block diagram of an exemplary programmable sensor agent adapted to generate descriptors, in accordance with an embodiment of the invention. Referring to FIG. 4B, there is shown a programmable sensor agent 414 that differs from the programmable sensor agent 400 in FIG. 4A in that a third DRP 410 is communicatively coupled to the first DRP 404. The third DRP 410 may be a configurable device substantially as described for the first DRP 404 and the second DRP 406. The third DRP 410 may be utilized to generate data content descriptors from the processed sensor output generated by the first DRP 404.

[58] As shown, the third DRP 410 may be adapted for video surveillance functions by further processing the processed sensor output generated by the first DRP 404. In this regard, the third DRP 410 may be adapted to generate video content descriptors. The video content descriptors may be, for example, motion and/or color descriptors. Motion descriptors may result as a byproduct of other video or image processing operations such a video compression, for example. A plurality of descriptors may be generated in accordance with the level of integration desired among security functions.

[59] FIG. 4C is a flow diagram illustrating exemplary steps for configuring a programmable sensor agent, in accordance with an embodiment of the invention. Referring to FIG. 4C, after start step 422, in step 424, features may be selected that may be programmed into at least one configurable device in at least one programmable sensor agent in a configurable security and surveillance system. In step 426, an e-commerce feature vendor may provide device programming files for the selected features. The device programming files may be transfer to the configurable security and surveillance system via a network connection and/or via machine-readable media. In step 428, decryption keys may be requested and obtained from the e-commerce feature vendor for device programming files that are encrypted. The decryption keys may be provided to the configurable security and surveillance system via a network connection and/or via machine-readable media.

[60] In step 430, the encrypted device programming files may be decrypted by utilizing the decryption keys received in step 428. In step 432, the device programming files may be transferred to the programmable sensor agents to program the configurable devices. In step 434, the programming of the configurable devices in the programmable sensor agents may be verified. In step 436, a user and/or installer of the configurable security and surveillance system may determine whether new, additional, and/or upgraded features may be necessary in at least one programmable sensor agent. When a user may find new, additional, and/or upgraded features necessary, the flow chart 420 may proceed to step 424 where new, additional, and/or upgraded features may be selected. When a user may not require new, additional, and/or upgraded features, the flow chart 420 may proceed to end step 438.

[61] FIG. 5A is a block diagram of an exemplary programmable content analysis agent, in accordance with an embodiment of the invention. Referring to FIG. 5A, there is shown a programmable content analysis agent 500 that comprises a first DRP 502, a second DRP 504, a third DRP

506, a fourth DRP 508, and a memory block 510. In some instances, more or fewer digital reconfigurable processors may be utilized.

[62] The first DRP 502, the second DRP 504, the third DRP 506, and the fourth DRP 508 may comprise suitable logic, circuitry, and/or code that may be adapted to provide digital processing and may be referred to a configurable devices that may adapted to be configured or programmed in order to provide at least one feature for at least one security function. The first DRP 502, the second DRP 504, the third DRP 506, and the fourth DRP 508 may be a digital signal processor (DSP), a central processing unit (CPU), a field programmable gate array (FPGA), or a complex programmable logic device (CPLD), for example.

[63] The programmable content analysis agent 500 may receive at least one device programming file to program or configure at least a portion of the first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508. The configurable devices may be programmed or configured via a programming file bus, for example. The device programming files may be code, embedded code, firmware, and/or compiled hardware description language (HDL) code in accordance with the type of configurable device. For example, when utilizing a DSP and/or a CPU as configurable devices, at least a portion of the embedded code that is executed on the configurable device may be configured to provide new, additional, and/or upgraded features. In another example, when utilizing an FPGA and/or a CPLD as configurable devices, at least a portion of the logic in the configurable device may be configured or programmed to provide new, additional, and/or upgraded features. In some instances, an FPGA and/or a CPLD configurable device may be utilized as a processing engine that may be able to support an embedded operating system (OS), such as Linux, for example. In such instances, the logic and/or the embedded code that is executed on the FPGA and/or the CPLD configurable device may be configured or programmed to provide new, additional, and/or upgraded features.

[64] The memory block 510 may comprise suitable logic, circuitry, and/or code that may be adapted to store information generated from the first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508. The memory block 510 may also be adapted to transfer stored information to the first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508. The memory block 510 may comprise at least one memory device. In some instances, the device programming files may be stored in the memory block 510 and may be transferred to the first DRP 502, the second DRP 504, the third DRP 506, and the fourth DRP 508 from the memory block 408. Communication between the configurable devices and the memory block 510 may be performed via a memory bus, for example.

[65] As shown in FIG. 5A, the programmable sensor agent 500 may be adapted to perform sensor analysis operations and/or security analysis operations. The sensor analysis operations may correspond to video surveillance functions, for example. In this regard, a portion of the first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508 may be utilized for video surveillance features and a remaining portion may be utilized for security analysis operations. For example, video surveillance features may comprise motion detection, generation of shape descriptors, object tracking, and/or object surveillance. Security analysis operations may comprise security event classification, generating control information to be transferred to programmable sensor agents, and/or system failure detection, for example.

[66] In this regard, the first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508 may be utilized to further process information or content generated by the programmable sensor agents. The first DRP 502, the second DRP 504, the third DRP 506, and/or the fourth DRP 508 may communicate with the programmable sensor agents in a configurable security and surveillance system via a data bus, for example.

[67] FIG. 5B is a flow diagram illustrating exemplary steps for configuring a programmable content analysis agent, in accordance with an embodiment

of the invention. Referring to FIG. 5B, after start step 522, in step 524, features may be selected that may be programmed into at least one configurable device in at least one programmable content analysis agent in a configurable security and surveillance system. In step 526, an e-commerce feature vendor may provide device programming files for the selected features. The device programming files may be transfer to the configurable security and surveillance system via a network connection and/or via machine-readable media. In step 528, decryption keys may be requested and obtained from the e-commerce feature vendor for device programming files that are encrypted. The decryption keys may be provided to the configurable security and surveillance system via a network connection and/or via machine-readable media.

[68] In step 530, the encrypted device programming files may be decrypted by utilizing the decryption keys received in step 528. In step 532, the device programming files may be transferred to the programmable content analysis agents to program the configurable devices. In step 534, the programming of the configurable devices in the programmable content analysis agents may be verified. In step 536, a user and/or installer of the configurable security and surveillance system may determine whether new, additional, and/or upgraded features may be necessary in at least one programmable content analysis agent. When a user may find new, additional, and/or upgraded features necessary, the flow chart 520 may proceed to step 524 where new, additional, and/or upgraded features may be selected. When a user may not require new, additional, and/or upgraded features, the flow chart 520 may proceed to end step 538.

[69] FIG. 6A illustrates an exemplary network comprising a residential configurable security and surveillance system, in accordance with an embodiment of the invention. Referring to FIG. 6A, there is shown a network 600 that comprises a residential configurable security and surveillance system 602 substantially as described in FIGS. 2A-2C, a mobile phone 604, a wireless center 626, a personal digital assistant (PDA) 606, a school 608, a satellite link 610, an emergency agency 612, a police

center 614, a home 616, at least one core router 618, at least one gate router 620, a commercial entity 624, a security and surveillance features vendor (SSFV) 300 as described in FIG. 3, and a TCP/IP network 128 as described in FIG. 1B. The residential configurable security and surveillance system 602 may be adapted to provide security functions for a home and/or small commercial entities.

[70] In operation, the SSFV 300 may provide device programming files and/or decryption keys to configure the configurable security and surveillance system 602 via the TCP/IP network 128 and the network of at least one gate router 620 and at least one core router 618. The features provided by the device programming files may support access to the configurable security and surveillance system 602 via the mobile phone 604 and/or the PDA 606 to a user. The user may utilize the mobile phone 604 and/or the PDA 606 as an interface to control at least a portion of the operations and/o display at least a portion of the contents generated by the configurable security and surveillance system 602. In this regard, the user may utilize the network of at least one gate router 620 and at least one core router 618 to communicatively couple the wireless center 626 and the configurable security and surveillance system 602.

[71] The configurable security and surveillance system 602 may be adapted to generate appropriate emergency signals and/or alarms to, for example, the school 608, the satellite link 610, the emergency agency 612, the police center 614, the commercial entity 624, and/or at least one home 616 in accordance with the features configured into the residential configurable security and surveillance system 602. For example, security breaches may be reported to any of these locations in accordance to the features supported by the residential configurable security and surveillance system 602. The types of security breaches and/or the locations to which the appropriate emergency signals are sent may depend on the security features received from the SSFV 300.

[72] FIG. 6B illustrates an exemplary network comprising a commercial configurable security and surveillance system, in accordance with an

embodiment of the invention. Referring to FIG. 6B, there is shown a network 630 that differs from the network 600 in FIG. 6A in that a commercial configurable security and surveillance system 622 is utilized. The commercial configurable security and surveillance system 602 may be adapted to provide security functions for a large commercial entities and/or governmental entities. In this regard, the commercial configurable security and surveillance system 622 may be adapted to support a large number and wide range of programmable sensor agents and programmable content analysis agents. Moreover, new, additional, and/or upgraded features may be provided periodically and/or routinely by the SSFV 300 as a result of a commercial agreement.

[73] The approach described herein may result in more effectively and/or efficiently integrated security and surveillance systems. The use of configurable devices in the programmable sensor agents and the programmable content analysis agents provides significant flexibility in the system architecture and may also increase the length of operation of a security and surveillance system before significant investments are required. In this regard, a user may determine the security functions and features necessary to their security operations while maintaining the ability to add and/or modify their security operations without having to replace significant portions of their existing hardware and/or software.

[74] Accordingly, the present invention may be realized in hardware, software, or a combination of hardware and software. The present invention may be realized in a centralized fashion in at least one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system or other apparatus adapted for carrying out the methods described herein is suited. A typical combination of hardware and software may be a general-purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein.

[75] The present invention may also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which when loaded in a computer system is able to carry out these methods. Computer program in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following: a) conversion to another language, code or notation; b) reproduction in a different material form.

[76] While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims.

CLAIMS

1. A method for configuring installed security systems, the method comprising:

receiving from a remote server via one or more networks, by at least one configurable device operable to capture video information and perform a plurality of security functions in an installed security system, at least one device programming file, wherein said plurality of security functions are associated with a plurality of video analytic and/or video processing applications; and

programming said at least one configurable device to add a new security function associated with a new video analytic application, to said at least one configurable device, said programming based on said received at least one device programming file.

2. The method according to claim 1, wherein said programming is performed while said installed security system is in operation.

3. The method according to claim 1, comprising decrypting at least one encrypted device programming file based on at least one decryption key to generate said at least one device programming file.

4. The method according to claim 3, comprising receiving said at least one decryption key via a network transfer.

5. The method according to claim 1, comprising programming said at least one configurable device to update at least one of said plurality of security functions performed by said at least one configurable device, said programming based on said received at least one device programming file.

6. The method according to claim 1, comprising verifying said

programming of said at least one configurable device.

7. The method according to claim 1, comprising storing programming information regarding said programmed at least one configurable device in a portion of said installed security system.

8. A machine-readable storage having stored thereon, a computer program having at least one code for configuring installed security systems, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving from a remote server via one or more networks, by at least one configurable device operable to capture video information and perform a plurality of security functions in an installed security system, at least one device programming file, wherein said plurality of security functions are associated with a plurality of video analytic and/or video processing applications; and

programming said at least one configurable device to add a new security function associated with a new video analytic application, to said at least one configurable device, said programming based on said received at least one device programming file.

9. The machine-readable storage according to claim 8, wherein said programming is performed while said installed security system is in operation.

10. The machine-readable storage according to claim 8, comprising code for decrypting at least one encrypted device programming file based on at least one decryption key to generate said at least one device programming file.

11. The machine-readable storage according to claim 10, comprising code for receiving said at least one decryption key via a network transfer.

12. The machine-readable storage according to claim 8, comprising code

for programming said at least one configurable device to update at least one of said plurality of security functions performed by said at least one configurable device, said programming based on said received at least one device programming file.

13. The machine-readable storage according to claim 8, comprising code for verifying said programming of said at least one configurable device.

14. The machine-readable storage according to claim 8, comprising storing programming information regarding said programmed at least one configurable device in a portion of said installed security system.

15. A system for configuring sensoring systems, the system comprising:

at least one configurable device in an installed security system that receives from a remote server via one or more networks, at least one device programming file, said at least one configurable device operable to capture video information and perform a plurality of security functions, wherein said plurality of security functions are associated with a plurality of video analytic and/or video processing applications; and

a system manager that programs said at least one configurable device to add a new security function associated with a new video analytic application, to said at least one configurable device, said programming based on said received at least one device programming file.

16. The system according to claim 15, wherein said programming is performed while said installed security system is in operation.

17. The system according to claim 15, wherein said system manager decrypts at least one encrypted device programming file based on at least one decryption key to generate said at least one device programming file.

18. The system according to claim 17, wherein said system manager receives said at least one decryption key via a network transfer.

19. The system according to claim 15, wherein said system manager receives said at least one device programming file via a network transfer.

20. The system according to claim 15, wherein said system manager verifies said programming of said at least one configurable device.

21. The system according to claim 15, wherein a storage device stores programming information regarding said programmed at least one configurable device in a portion of said installed security system.

22. The system according to claim 15, wherein a programmable sensor agent comprises at least one of said at least one configurable device.

23. The system according to claim 15, wherein a programmable content analysis agent comprises at least one of said at least one configurable device.