(12) UK Patent Application (19) GB (11) 2 363 028 (13) A

(43) Date of A Publication 05.12.2001

(21) Application No 0110084.1

(22) Date of Filing 25.04.2001

(30) Priority Data
(31) 0009855 (32) 25.04.2000 (33) GB

(71) Applicant(s)
Geoffrey Stubbs
63 Dimsdale View East, Porthill, NEWCASTLE, Staffs, ST5 8HN, United Kingdom

Harvey James Stubbs
24 St Marys Road, LITTLE HAYWOOD, Staffs, ST18 0NJ, United Kingdom

(72) Inventor(s)
Geoffrey Stubbs
Harvey James Stubbs

(74) Agent and/or Address for Service
Geoffrey Stubbs
63 Dimsdale View East, Porthill, NEWCASTLE, Staffs, ST5 8HN, United Kingdom

(51) INT CL[7]
H04N 7/18

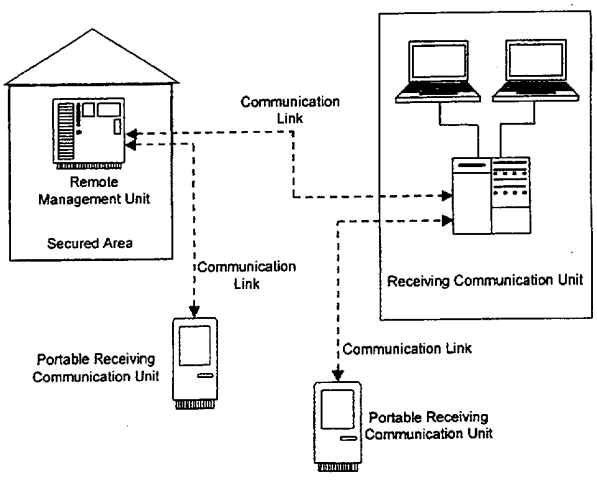
(52) UK CL (Edition S)
H4F FAAE

(56) Documents Cited
GB 2329542 A **GB 2253534 A** **GB 2253121 A**
EP 0979009 A2 **WO 00/45296 A1**

(58) Field of Search
UK CL (Edition S) **H4F FAAE**
ONLINE DATABASES: WPI, EPODOC, JAPIO.

(54) Abstract Title
Surveillance system with remote receiving unit.

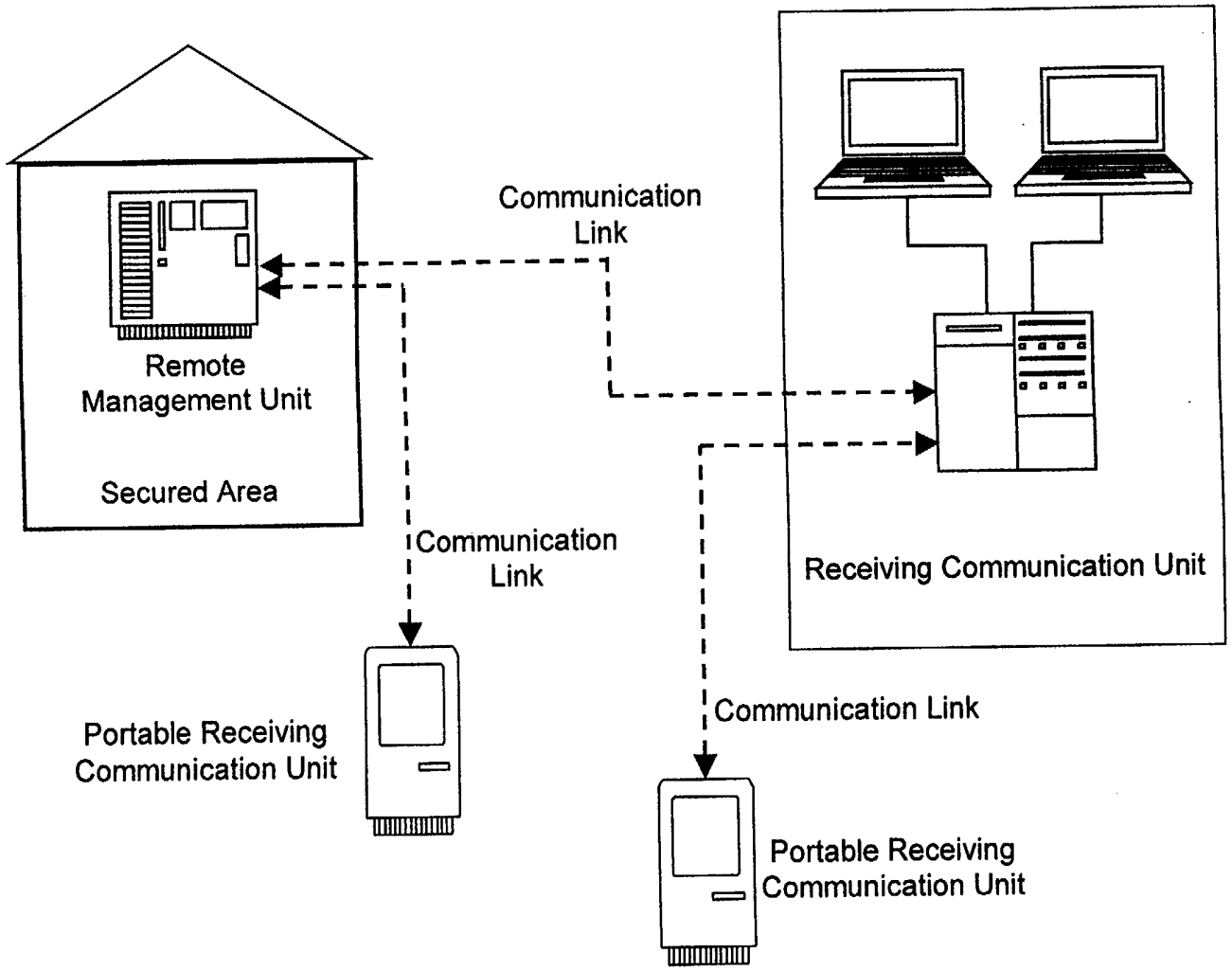
(57) A surveillance system comprises a Remote Management Unit (RMU) or local unit positioned at the location to be monitored, and an associated Receiving Communication Unit (RCU) or receiving unit, distanced from the monitored location. The local unit serves to control, locally and autonomously, monitoring devices such as cameras and other sensors (smoke, temperature and infrared sensors and so on; see Figures 2, 3). Data may be input via keyboards (see Figures 2, 3) and the monitoring data is stored at each local unit (RMU) for transmission to the receiving unit (RCU). Each local unit may be armed or disarmed either locally via the keypads or remotely via the receiving unit. To enhance security, data transmitted to the receiving unit may be watermarked. Also, images captured by the camera may be 'weighted' according to their relative importance using a selection algorithm, allowing for the most important or relevant images to be transmitted first. In addition, the system has the facility of transmit low resolution, highly compressed images first, followed by higher resolution (low compression) images later, on demand.



Intelligent Remote Intruder Surveillance System

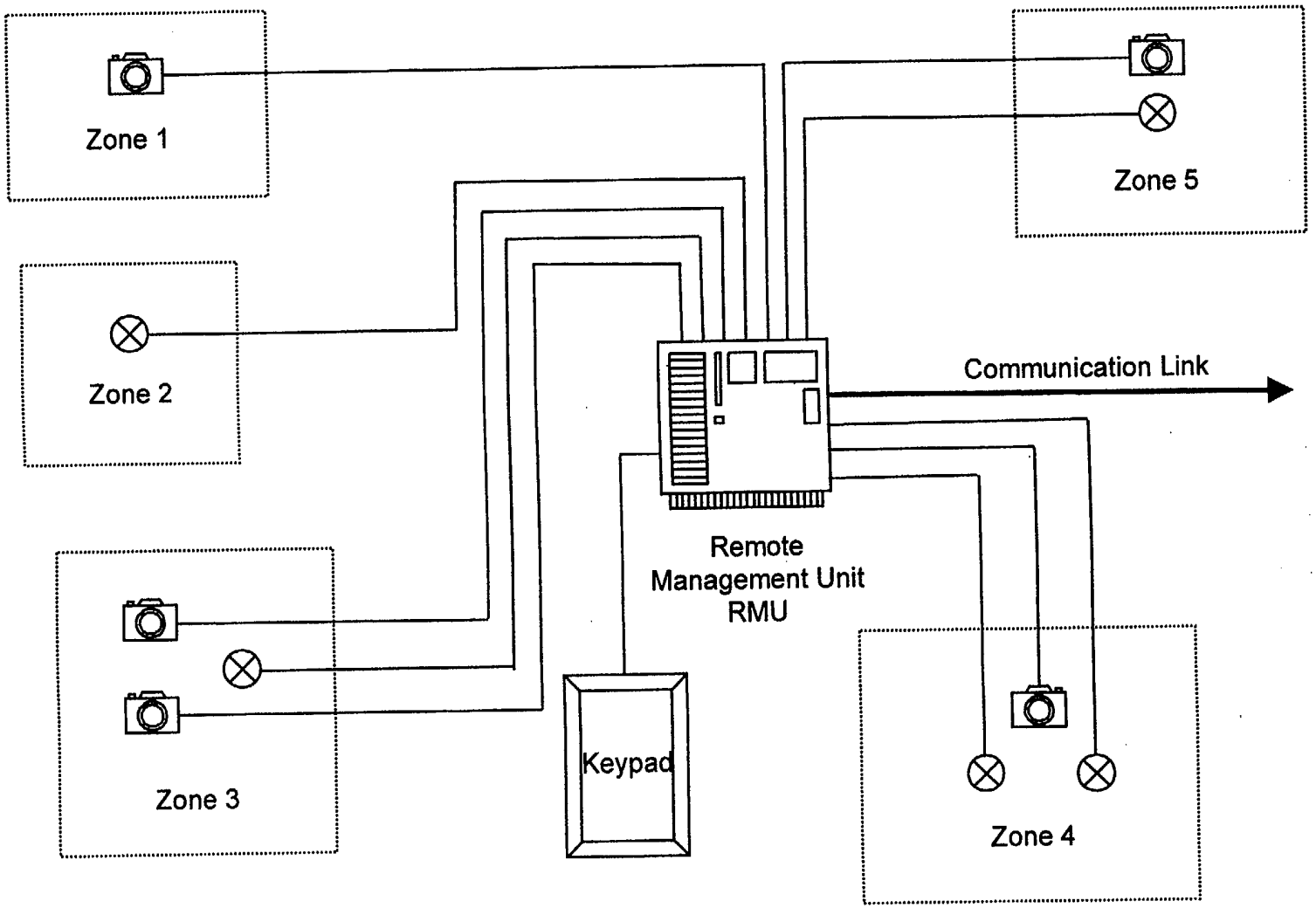
Figure 1

GB 2 363 028 A



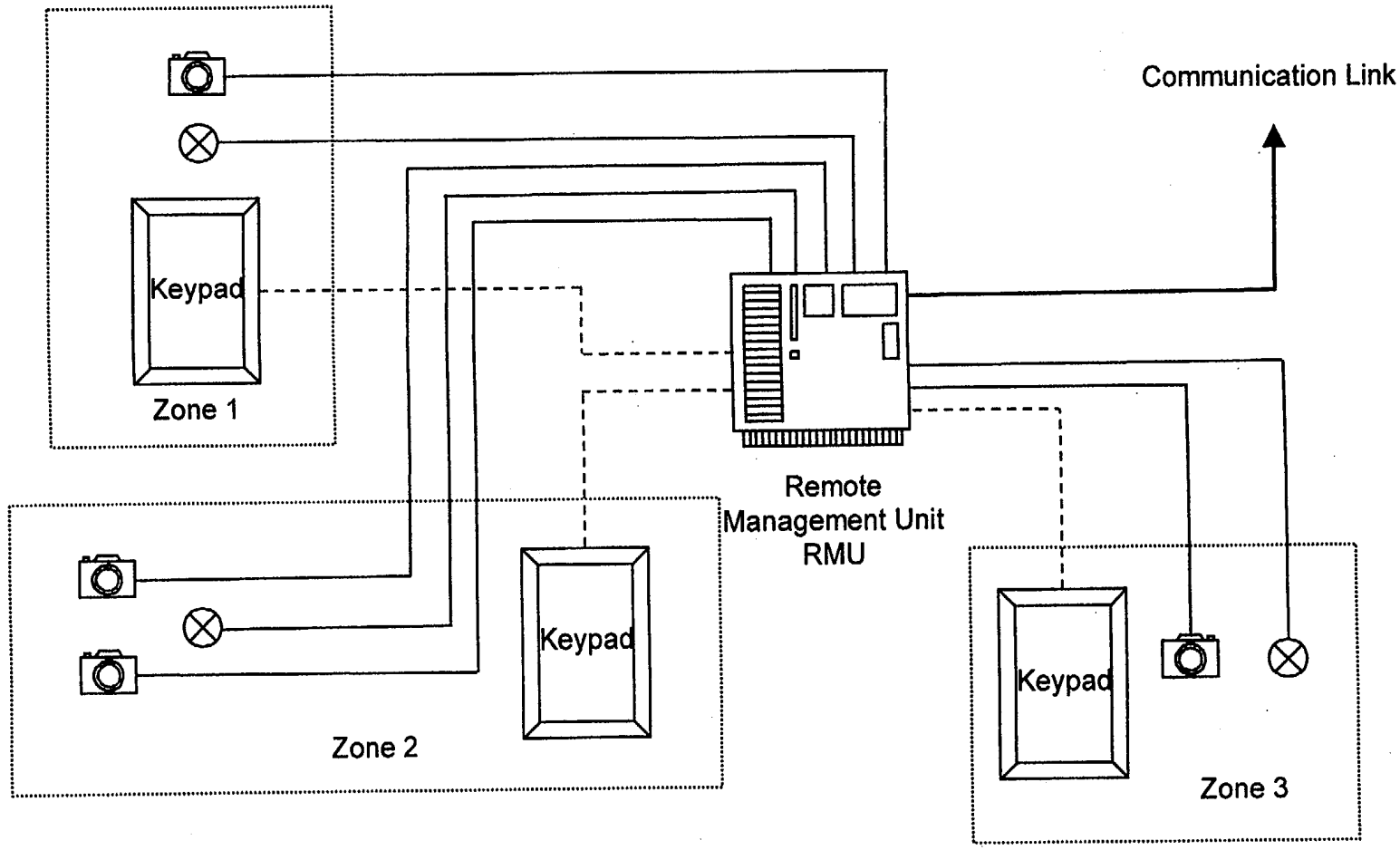
Intelligent Remote Intruder Surveillance System

Figure 1of 3



Intelligent Remote Intruder Surveillance System. Remote Management Unit

Figure 2of 3



Intelligent Remote Intruder Surveillance System.

Logical Remote Management Units

Figure 3of 3

2363028

IRIS

Intelligent Remote Intruder Surveillance

This invention relates to a passive remotely monitored digitised visual security system linked to a central receiving station.

Conventional security systems in general comprise of four main elements, input keypad, alarm control, motion detectors and audible alarm. The system is enabled by the input of an alpha - numeric code into the keypad, once enabled is dormant in a passive mode until activated. Movement in range of the motion detectors or the interruption of the sensors activates the system and sounds an audible alarm. The disadvantage of this type of system is their reliance on the public acknowledging the alarm and contacting the appropriate agency (police, security, etc.) The occurrence of spurious or false alarms also impacts on the effectiveness, inviting complacency in the public and hence a failure to respond. Even in the event of a response it is usually too late to apprehend the intruder with identification unlikely.

IRIS is a system designed to: -

a) Eliminate the reliance of involving the general public
b) Photograph the active area of premises and consequently the intruder
c) Transmit the alarm condition and photograph to a central manned control for verification and forwarding to the local police or security service.

The embodiment of this invention is to provide prompt and accurate intelligence of an alarm condition in a secured area either internally within a building or externally in an outdoor scenario and is described by way of example with reference to the accompanying drawings.

- Figure 1: Intelligent Remote Intruder Surveillance System.
- Figure 2: Intelligent Remote Intruder Surveillance System. Remote Management Unit.

- Figure 3: Intelligent Remote Intruder Surveillance System. Logical Remote Management Units.

1. The concept of the Intelligent Remote Intruder Surveillance (IRIS) System is to capture, store and transmit information to a remote location when activated. The IRIS system comprises of two separate units located in different geographic locations. When combined the purpose of the two units is to provide remote surveillance of an area or area to be secured and prompt and accurate intelligence of an alarm condition generated at that area. Information captured with one unit by still digital cameras and sensors being communicated by means of an automatically established bi-directional communications link to the other unit for evaluation and interrogation of the data.

1.1 The two separate units of the IRIS system are the Remote Management Unit (RMU) and the Receiving Control Unit (RCU). The RMU and the RCU are inter-dependent on each other for the system functionality and are linked together via by a communications link.

1.2 The RMU is a dedicate self-contained autonomous unit located at the area or area to be secured and is geographically remote from the RCU. It provides the security of the area or area to be secured by monitoring suitably appropriate (PIR, Electro-Magnetic, Photo-Electric etc.) sensor and surveillance by still digital cameras. See Figure 1.

1.3 Detection by a sensor of a variation to its state initiates a photographic sequence and automatically establishes a secure communications link with the RCU transmitting the photographic sequence and alarm condition to it. The RCU is an operator-controlled unit for the receipt, evaluation and interrogation of the data received from an RMU.

1.4 The communications link can be provided on either a privately owned or public service communication system. Multiple RMUs are managed by a single RCU and the connection between them is created during an alarm condition and destroyed when the alarm condition has terminated.

1.5 The function of the RMU is to: -

- Monitor the area to be secured by various sensors.
- Record and store a sequence of digital images captured by an array of cameras and additional related sensor and status information to a digital storage device in the event of an alarm. The information is stored in chronological order.
- Watermark the stored information in such a way as to prevent tampering of the information or to enable the detection of such tampering.
- Automatically create a secure bi-directional communications link with an RCU during an alarm condition and destroy the link once the alarm condition has ceased.
- Have the ability to take on the existing functions of an installed alarm system or to cooperate with an existing alarm system and provide extra functionality.

1.6 The Remote Management Unit (RMU) is a static, portable or mobile device identified by a unique serial number.

1.7 The RMU is powered according to its configuration, for example:-
The static RMU is powered by a mains voltage electrical supply with an emergency rechargeable battery back-up system to enable operation in the event of a power failure.

The portable RMU is battery powered. The batteries used may be re-chargeable capable of being recharged from a variety of sources.

The mobile RMU is powered from the mobile units (car, train, coach, aircraft, etc) internal electrical supply with an optional rechargeable battery backup system.

1.8 The Receiving Control Unit (RCU) is a separate unit at a geographically distanced location from the Remote Management Unit (RMU). The RCU manages multiple RMU's installed at various remote locations. The RCU is continuously operator manned for the reception, evaluation and subsequent action of incoming information transmitted from the RMU locate at the area or area to be secured.

Numerous operators can evaluate information from multiple RMU's simultaneously connected to one RCU.

1.9 The Receiving Control Unit (RCU) is static, mobile or portable device.

1.10 The RCU is powered according to its configuration, for example:-

The static RCU is powered by a mains voltage electrical supply with an emergency battery back-up system to enable operation in the event of a power failure.

The portable RCU is battery powered. The batteries used may be re-chargeable capable of being recharged from a variety of sources.

The mobile RCU is powered from the mobile units (car, train, coach, aircraft, etc) internal electrical supply with an optional rechargeable battery backup system.

2 Remote Management Unit (RMU)

The core functionality of the Remote Management Unit (RMU) is to: -

- Monitor an area to be secured.
- Allow its state to be changed via attached keypad input or switch.
- Allow its state to be change via the communication link.
- Capture a sequence of still images from multiple digital cameras and record this information to a digital storage device during an alarmed condition.
- Capture information from multiple sensors and record this information to a digital storage device during an alarmed condition.

- To store the information in chronological order for retrieval at a later point in time.
- Watermark the stored information in such a way as to either prevent tampering of the information or to enable the detection of tampering of the information.
- Automatically create a secure bi-directional communications link with RCU during an alarm condition and destroy the link once the alarm condition has ceased.
- Maximise the bandwidth of the communications link.

Control of the Remote Management Unit (RMU) is at all times vested in the owner/occupier of the area or area to be secured. The arming of the RMU is a positive action comprising of two distinctly differing methods. Direct and Indirect arming. Direct arming of the RMU will require the input of an alphanumeric code. The input of the code into the RMU is local by a keypad or remote via a communication link using a transmitting device. See Figure 2.

In emergency situations the RMU can be elevated directly to the alarmed condition irrespective of the current system status. This facility is site specific and optional. The RMU so configured would respond, in addition to the standard alarm conditions, to selected and specific components, i.e. panic buttons, voice activation commands or push buttons for initiating an alarm sequence.

The RMU is continuously powered in either a disarmed, armed or alarmed condition.

In the Disarmed Condition the RMU is:

- Inactive with the transmission of data inhibited.
- Receptive to coded incoming transmissions to arm via the communication link.
- Receptive to keypad arm.
- Receptive to specific emergency commands.

- Able to power on or off cameras depending on the configuration. Those powered on actively recorded images on a closed timed loop.
- Able to power on or off sensors which require power depending on the configuration. For example in the portable battery powered device – the sensors will be powered down in the disarmed state.

In the Armed Condition the RMU:

- Is active with the transmission of data enabled.
- Is receptive to coded incoming transmission to disarm.
- Is receptive to keypad disarm.
- Is able to power on or off cameras depending on the configuration. Those powered on actively recorded images on a closed timed loop.
- Powers on all sensors requiring power.
- Monitors all sensors for a change instate.
- If configured, accept incoming connections from an RCU to allow remote monitoring of the area or area to be secured.

In the Alarmed Condition the RMU:

- Establishes (if required) a secure bi-directional communications link to the RCU.
- If required powers on and off cameras if the zone in which they are located become active/inactive as regards to sensor information for that zone – (zone activation)
- Powers on all other cameras not controlled by zone activation.
- Records captured image and sensor information to the digital storage device.
- Watermarks the information to prevent tampering.
- Is receptive to keypad disarming
- Is receptive to coded incoming transmission to disarming.
- Responds to commands issued from the RCU.

- If required activates ancillary equipment.

The Remote Management Unit (RMU) has three separate though integral functions that are the embodiment of this invention. The functions of the RMU are: -

a) System Management.
b) Storage of Photographic Images and Sensor Status.
c) Communication with and transmission of the recorded images and sensor status to a remote Receiving Control Unit.

2.1 System Management.

2.1.1 The RMU has multiple inputs and outputs for the connection of digital cameras, sensors, communication devices and ancillary equipment .

2.1.2 The RMU may be split into one or more 'Logical RMU units'. Each logical unit behaves like an RMU in its own right but act independently of one another. Each logical RMU shares the one communication link. For example arming one logical RMU does not necessarily arm the other logical RMU's within the same physical unit. In this section RMU is to be read as either a physical RMU unit or a logical sub division of that unit. See Figure 3.

2.1.3 An area to be secured will be assigned a RMU. The RMU enables a secured area to be divided into one or more zones. The RMU provides for a number of sensor and camera inputs each of which is assigned a specific zone. The permutation of cameras with sensors in each zone is variable. For example, single or multiple sensors can be related to an individual camera. Single or multiple sensors can be related to more than one camera. Cameras and sensors can operate independently of each other.

2.1.4 The RMU is aware of the relationship between zones and the installed sensors and cameras within a zone. It can power on and off cameras as and when zones become active/inactive in an effort to preserve power, this is of vital importance within the portable (low power) application.

2.1.5 Still Digital cameras capture images. The number of images captured during any time period is variable and adjustable either from a pre programmed site-specific requirement or by a command from the RCU. The RCU can instruct a variation to the capture rate of images by RMU with RMU in either an armed or disarmed mode. Further to this, the actual capture of images from the cameras can be adapted to suite various different installations.

For example:

- The camera may only record images if there is a sensor active within the same zone.
- The camera will always record images regardless of sensor state – if any - within a particular zone.

2.1.6 A camera may pre-record images for a variable amount of time prior to the elevation of the RMU to the alarmed condition. The pre-recording happens on a closed loop system - a set number of images are captured to begin with, then when the next image is captured, it overwrites the first, and so on. This process continues until the alarmed condition is entered when the pre-recorded images are stored in chronological order to the digital storage device.

2.1.7 Entering a code via the keypad or via the communication link elevates the unit from a disarmed to an armed condition.

2.1.8 Once in the armed condition, entering a code via the keypad or via the communication link returns the unit to the disarmed condition.

2.1.9 The disruption to the sensor status in the armed condition, initiated by a variation in the environmental condition, presence of an intruder or external alternate command registers an alarm state raising the RMU to the higher-level alarmed condition.

2.1.10 Elevated to the alarm condition, the RMU activates the various cameras based on its configuration. Some cameras may be set up to capture images for the full duration of the alarm condition, others may capture images only when there is an active sensor in the same zone as the camera.

2.1.11 During the alarm condition, the RMU captures images from the active cameras as determined by its configuration. The images, system and sensor information are recorded and stored within the RCU digital storage device. The images are stored in high resolution. The capture of information continues until either the RMU runs out of storage capacity or until the operator at the RCU instructs the RMU to stop the capture of information.

2.1.12 Elevated to the alarmed condition the RMU if required will automatically establish a secure communications link for the transmission of images and sensor status information with the RCU. The establishment of a secure communications link opens the control function of the RMU to the RCU.

2.1.13 The Remote Unit (RMU) uses the relationship between sensors and cameras as well as other algorithms to maximise the utilisation of the communications link by intelligently transmitting information to the RCU which it deems to be of interest first. The selection of information to be transmitted is accomplished by utilising an Intelligent Selection Algorithm as described in section 3.

2.1.14 The Intelligent Selection Algorithm may be overridden by the operator RCU instructing the RMU to transmit information and images from a different camera.

3 The Intelligent Selection Algorithm.

The algorithm uses the relationship between sensors and cameras as well as other algorithms to determine the information of most importance to send to the RCU first. The selection of which image and information to transmit is made by examining the contents of the storage device. This holds the chronological history of images, sensor and status information. By interpreting the information and weighting the stored images as appropriate, the most important image held in the storage device can be determined. For example an image captured from a camera in a zone with no sensors active has a lower weight than an image captured from a camera in a zone with an active sensor.

This weighting occurs across all images which have not been transmitted to the RCU held within the storage device.

Subsequently to this the weighting may be changed by other factors – for example:

1. The percentage change of the current image from the last image captured for that camera. A change of a set amount increases the weighting of the image. A reduction lowers the weight.
2. An increase or decrease in image complexity from the previous to the current image for that camera. An increase of complexity increases the weighting and a reduction of complexity decreases the weighting

The highest weighted image – i.e. the one of most probable interest – is selected for transmission to the RCU. To preserve bandwidth further, the image is compressed even more by reducing the quality of the image (low resolution) prior to the transmission. Using this intelligent transmission of images, the RCU will only receive active and relevant information.

If all the images have been transmitted in low resolution format, the algorithm repeats the exercise, this time selecting high resolution versions of the images.

One particular image can only be transmitted twice – once in low resolution format and again in high resolution format. Note that if an image has already been transmitted in high resolution format, the algorithm will not select the low resolution version for transmission.

4 Storage of Photographic Images, Sensor and System Status information.

The digital storage device used to store the recorded information has a finite capacity. A property of the invention is to maximise the available space by intelligently capturing only the information of interest to the device.

4.1 The captured images and all the information relating to them, including sensor and system status is recorded and stored in chronological order in the RMU's digital storage device. Information relating to whether images and information have been transmitted to the RMU is also stored within the storage device.

4.2 All images captured by the camera array are stored in a compressed high resolution format.

4.3 Depending on the configuration of the RMU, an image captured from an active camera can be discarded if the unit deems the image to be worthless. For example if the image was captured from a camera in a zone registering no sensor activity the image may be discarded.

4.4 Selected cameras are active, irrespective of the RMU status, continuously capturing images at a predetermined frequency on a limited closed loop timed sequence. After the predetermined time elapse the earliest captured image is deleted with only the most recent images being retained. This process continues until the alarmed

condition is entered when the pre-recorded images are stored in chronological order to the digital storage device.

5 **Communication With and Transmission of the Recorded Images and Sensor Status to the Receiving Control Unit (RCU).**

The communication link used between the RMU and the RCU has a finite bandwidth, it being imposable to transmit more than a specific amount of information per second. A property of the invention is to maximise the available bandwidth by intelligently transmitting only the information of interest between the devices.

5.1 As previously described the transmission of information can only take place with the RMU in the alarmed condition.

5.2 The establishment of a secured bi-directional link between the RMU and RCU is vitally important to preserve the integrity of the system as a whole. As the RMU units may not be under the direct control or ownership of the RCU, a challenge and response system is used to authenticate that an RMU unit connecting to the RCU is really what it claims to be.

Having passed the challenge and response phase, all communication between the RMU and the RCU is subsequently encrypted.

5.3 To maximize the bandwidth of the communications system all information is compressed prior to transmission.

5.4 To maximise the utilisation of the communication link, information is transmitted in a priority order as determined by the Intelligent Selection Algorithm.

5.5 The images captured by the cameras during an alarmed condition are transmitted to the RCU in low resolution format first but are of sufficient clarity to determine the cause of the alarm condition. On command of the RCU operator high resolution images can be selected and retrieved from the RCU's storage device in any order of priority and transmitted to the RCU.

5.6 After all images have been transmitted in low resolution format, the sequence begins again but this time transmits the high resolution versions of the images.

5.7 The RMU will not allow the same image to be transmitted twice neither will it allow an image to be transmitted in low resolution if it has already been transmitted in high resolution format.

6 The Receiving Control Unit

The Receiving Control Unit (RCU) provides the following core functionality for a number of RMU's:

- Authentication of the RMU unit and Secured bi-directional communication link.
- Storage and retrieval of RMU information.
- Storage and archive of transmitted images, sensor and status information from the Remote RMU.
- Operator control of the RMU unit.
- Provide the ability to forward the transmitted images, status and system information onto a third party.
- Provide the ability for an Operator to contact an RMU Unit to access it remotely.
- Retrieval of archived information.

The RCU itself may take a number of different formats, for example:

- It may be a continually manned static operations centre.
- It may be a portable device capable of receiving incoming communication connections.

Remote RMU unit data.

The RCU is responsible for storing details of all of the RMU units installed at various remote locations. Information and data relative to the RMU is stored against its unique serial number. Examples of the types of information stored are site location, owner, configuration of the RMU and contact list for the RMU etc.

Once the RMU unit has authenticated itself to the RCU, it further identifies itself with its unique serial number and the reason for the connection. Using this information the RCU can determine the location of the RMU and which person(s) are to be contacted in the event of an alarm condition being raised at that location.

Storage of Transmitted Images.

Having connected to the RCU the RMU automatically begins to intelligently transmit the information, which it believes, are of most interest to the RCU Operators. Images may be transmitted in a random sequence due to the mechanism of selection and it is the function of the RCU to re-order them into a coherent chronological order. The images received initially will be of low-resolution quality – but contain sufficient detail to enable the Operator to visually understand the events which are occurring in the secured area.

In conjunction with the transmission of images, the RMU also transmits sensor and status information to further enhance the data presented to the RCU Operator(s).

All actions that the Operators take are logged as part of the information stored for the alarmed condition.

Given sufficient time all of the information held on the remote RMU will be copied (in a random order) to the RCU. The information held at the RCU would then contain low-resolution images of all of the high-resolution images stored on the remote RMU.

The order of transmission of information from the RMU to the RCU is determined by the Intelligent Selection Algorithm.

Once the transmission of low-resolution images has been completed the system then repeats the whole process again but this time transmitting the high-resolution images.

The RMU will not allow duplication of effort if, for example an image has already been transmitted in high resolution the RMU will not transmit a low resolution version of the same image.

Operator Control of Alarmed RMU.

The RMU is capable of receiving commands from the operator controlled RCU dealing with the alarmed condition. For example if a high resolution image is required from a particular camera, the operator can instruct the remote RMU to transmit it as soon as possible – regardless of the fact that the Intelligent Selection Algorithm may have identified other images for transmission.

The operator can command the remote RMU from the RCU to:

- Pan and Tilt the cameras.
- End the connection and Re-arm system.
- End the connection and Disarm system.
- Control other devices.
- Stop capturing images.
- Control ancillary equipment.

Archiving of Transmitted Images.

At the commencement of an alarmed condition all incoming data to the RCU is recorded to establish a record of events irrespective of resolution.

At the end of an alarmed condition the images, status and sensor information is archived. This archive allows the review of an alarmed condition at a later date. The archive itself is encrypted so as to prevent tampering of the archive at a later date.

Forwarding Images, Status and System Information onto a Third Party.

The RCU has the ability to forward the images onto a third party. This can be accomplished in two ways:

1. The third party is given direct access to the RCU in that they can act as an Operator and control the RMU directly.
2. The third party is granted access to only the received images and cannot request images from or control in any way the RMU.

Remote Access of the RMU.

Providing the RMU unit supports the function, it is possible for the RCU to contact the RMU itself to allow remote monitoring of the area or area to be secured

Claims

1. A dedicated autonomous Intelligent Remote Intruder Surveillance system comprising monitoring, capturing, storing of images and information of an area or areas to be secured and transmitting the images and information, via a communications system, to a distant receiving unit.
2. An Intelligent Remote Intruder Surveillance system as claimed in claim 1 where the unit located at the area or areas to be secured is a dedicated self contained and autonomous unit, here after called the Remote Management Unit (RMU) to provide monitoring and surveillance of an area or areas to be secured
3. An Intelligent Remote Intruder Surveillance system as claimed in claim 1 where the distant receiving unit, here after called the Remote Communication Unit (RCU) is at a remote geographic location to the RMU.
4. A communications link connecting the RMU as claimed in claim 2 to the RCU as claimed in claim 3 in a secure manner comprising of but not limited to PSTN/ISDN/mobile telephone networks.
5. A RMU as claimed in claim 1 or claim 2 which will have attached a number of still digital cameras, a number of sensors and optionally one or more key pads, one or more displays to show the state of the RMU and connections for external ancillary devices.
6. A RMU as claimed in claim 5 where sensors means various environmental sensors, including but not limited to PIR detectors, Electro-magnetic devices, push buttons, smoke and temperature sensors and audible commands.
7. A RMU as claimed in claim 5 where photographic images are captured in sequence by the still digital cameras.
8. A RMU as claimed in claim 5 or claim 7 stores the captured digital images, sensor and status information in chronological order to a storage device.
9. A RMU as claimed in claim 2 that is battery backed to enable operation in the event of power failure.

10. A RMU as claimed in claim 2 that is purely battery powered having the option of being rechargeable from a variety of sources.
11. A RMU as claimed in claim 2 that divides an area to be placed under surveillance into individual zones with an arbitrary number of cameras and sensors allocated to each of these zones.
12. A RMU as claimed in claim 2 wherein it may be continually armed or its state may be controlled by use of the keypads to armed or disarm the unit.
13. A RMU as claimed in claim 2 wherein it may be armed or disarmed remotely by use of a communications link.
14. A RMU as claimed in claim 2 wherein the RMU may be divided into two or more 'logical RMUs', each logical RMU responsible for one or more areas, in which no zone is covered by more than one logical RMU.
15. A RMU as claimed in claim 14 wherein each 'logical RMU' has its own independent still digital cameras, a number of sensors and optionally one or more keypads capable of arming and disarming each 'logical RMU'.
16. A RMU as claimed in claim 2 with the ability to switch off and on the attached sensors and still digital cameras to preserve power.
17. A RMU as claimed in claim 2 when in an alarmed condition has the ability to switch on the still digital camera(s) – if any - in the zone(s) that register activity by the change of state of the associated sensor within that zone.
18. A RMU as claimed in claim 2 wherein during an alarmed condition, stores captured images, sensor and status information in chronological order to a storage device.
19. A RMU as claimed in claim 2 that watermarks the stored images, sensor and status information in such a way as to guarantee authenticity and to prevent tampering of the information held on the storage device.
20. A RMU as claimed in claim 2 wherein the stored images, sensor and status information may be communicated via a link as claimed in claim 4 to a static, mobile or portable Receiving Control Unit (RCU) as claimed in claim 3 capable of receiving the information via a communication link.

21. A RCU as claimed in claim 3 that determines and verifies the authenticity of a RMU as claimed in claim 2.

22. A RCU as claimed in claim 3 wherein the RCU verifies and authenticates the information received by the examination of the watermarking data as claimed in claim 19 contained within the information sent from the RMU as claimed in claim 2.

23. A RMU as claimed in claim 2 wherein the captured images held within the storage device are allocated weights in such a way as to identify the images of most interest utilising image comparison between current and previous images, sensor and status information, and other algorithms.

24. A RMU as claimed in claim 2 transmits stored images and associated information to the RCU in an order determined by an Intelligent Selection Algorithm (ISA) as claimed in claim 23 utilising the weighting information to select the images of most probably interest for transmission first.

25. A RMU as claimed in claim 2 wherein low quality, low resolution images are first transmitted to the RCU as claimed in claim 3 for the maximisation and utilisation of the communication bandwidth using the Intelligent Selection Algorithm (ISA) as claimed in claim 23.

26. A RCU as claimed in claim 3 wherein the RCU can retrieve images from the RMU as claimed in claim 2 without them having been sent via the Intelligent Selection Algorithm as claimed in claim 23.

27. A RCU as claimed in claim 3 wherein the RCU reassembles the images transmitted using the Intelligent Selection Algorithm as claimed in claim 23 from the RMU as claimed in claim 2 into chronological order for examination by an operator.

28. A RCU as claimed in claim 3 wherein the RCU can retrieve stored information directly from the RMU as claimed in claim 2 in the event of communication link as claimed in claim 4 failure between the RMU and the RCU.

29. A RCU as claimed in claim 3 wherein the RCU can contact via a communications link as claimed in claim 4 an RMU as claimed in claim 2 and

access stored images, sensor and status information as claimed in claim 8 at a later date after an alarm condition.

30. A RCU as claimed in claim 3 wherein the RCU can contact to an RMU as claimed in claim 2 via a communication link as claimed in claim 4 and access images, sensor and status information directly from the attached still digital cameras and sensors as claimed in claim 5 at any time.

31. A RMU as claimed in claim 2 wherein the RMU has the ability to take on the existing functions of an installed alarm system or to cooperate with an existing alarm system and provide extra functionality.

21

Application No: GB 0110084.1 **Examiner:** Matthew Males
Claims searched: 1 - 31 **Date of search:** 27 September 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4F (FAAE)

Int Cl (Ed.7):

Other: Online databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2329542 A	(SONY) - whole document but see abstract	1, 14, 15
X	GB 2253534 A	(ADVANCED TECHNOLOGY INDUSTRIES) - whole document but see abstract, Figure 1, page 2, fourth paragraph and page 4, third paragraph	1 - 11, 13, 16 - 18, 20, 26, 29, 30
X	GB 2253121 A	(NORTHERN TELECOM) - whole document but see abstract and page 2, second paragraph; also page 4, fourth paragraph - page 5, third paragraph	1 - 8, 11 - 13, 16 - 18, 20, 21, 26, 29, 30
X	EP 0979009 A2	(MATSUSHITA) - see abstract; appears to show priority transmission of low-resolution images.	1, 23, 25
X	WO 00/45296 A1	(AXIS AB) - whole document but see abstract, Figure 3 and summary on pages 4 and 5; page 6, lines 22 - 33; page 12, line 28 - page 15, line 27	1 - 3, 5 - 8, 11 - 13, 16, 18, 20, 23, 24, 26, 29, 30

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.