THE DESIGN, DEVELOPMENT AND IMPLEMENTATION OF AN IMAGING SYSTEM FOR THE AUTOMATIC ALARM INTERPRETATION OF CCTV SEQUENCES USING IKBS TECHNIQUES

Dr Nigel D E Custance and P Golton (Home Office);
T J Ellis, P Rosin and P Moukas (City University)

Scientific Research and Development Branch
Science and Technology Group
Home Office
Horseferry House
Dean Ryle Street
London SW1P 2AW
England

Abstract. The assessment of alarm cause from a perimeter intrusion detection system is manpower intensive. Work by the Home Office has shown considerable benefits can accrue from the use of digital storage, replay and analysis of image sequences from surveillance CCTV. The design of the system is heavily dependent upon the number of cameras on site, the need (or otherwise) for pre-alarm triggering, the probable speed of movement of objects within the scene, and the likelihood of near simultaneous alarms occurring. The techniques used to classify the cause of an alarm are described in a further paper to be presented at the conference.

Introduction

The perimeter of an establishment is the first line of defence or the last form of resistance depending upon whether one is attempting to stop people entering or, in the case of a prison, preventing their escape from a location. Increasing levels of civil and terrorist violence have led to enhanced measures to constrain unwanted elements. The increased emphasis being placed on perimeter barriers and alarm systems by industry and Governments reflects the growing concern that vulnerable point type protection is inadequate on its own.

Perimeters present an exciting challenge to the security market. Solutions need to be found for perimeters with extreme lengths and located in hostile environments. Despite considerable advances in sensor technology, perimeter security relies on the classical combinations of barriers, perimeter intrusion detection systems (PIDS), close circuit television (CCTV) and a response force. Unfortunately the performance of PIDS is poor and CCTV systems are needed to verify the cause of an alarm. Verification requires the use of control room operators to assess the cause of an alarm - the alternative being to dispatch a response force to investigate the zone in question.

The requirement for CCTV verification of alarms by an operator is costly both in terms of equipments and personnel. Increasingly the use of expensive manpower on routine, unchallenging tasks such as monitoring screens in a control room is being challenged by organisations seeking to redeploy staff into more productive areas. Notwithstanding improvements in sensor signal processing and the development of new sensors, the unwanted alarm rates associated with existing commercial systems are far in excess of those that either the supplier or end user should consider acceptable.

The work described in this paper details an approach which it is anticipated will reduce the manpower requirements in the control room. This reduction is to be achieved through the use of hardware with specialist IKBS software to improve greatly the assessment of alarm causes. Considerable advances are expected in both the presentation to an operator of more useful images of the sector in alarm and additional research shows great promise for the automatic identification of alarm cause.

Early work in this area by the Home Office was described at an earlier Carnahan Conference [1].

Objectives of the Work Being Undertaken

The high level objective of the work being undertaken is to reduce the cost to an organisation of its perimeter security by compensating for the shortcomings in the performance of PIDS. In order to put into context the situation which confronts users it is appropriate to review the general performance characteristics of PIDS. From this the implications for control room staff can be inferred.

The performance of PIDS is heavily influenced by the environment in which the systems are located. The dominant factors which influence performance are the type of PIDS (eg a buried sensor, a fence mounted system, or a free standing device); the weather environment in which the system operates; and the characteristics of the site which may vary considerably throughout a 24 hour period. Often the end user has little choice in the family of barrier or PIDS to be used. The choice is normally severely restricted as a result of past investment, eg one has to use existing perimeter fencing, and little hope exists for influencing the weather which a site is subjected to!

causes within a test site for a large number of systems over a considerably number of days. it should be noted that the movement of personnel is closely controlled in order to minimise the number of true alarms. The sensitivity settings of the PIDS are typical of those associated with medium to high risk prisons. This table illustrates the sheer number of unwanted alarms which can be generated on systems spanning a total effective perimeter of several kilometres.

The accrued breakdown of figures illustrated in Table 2, whilst giving an overall picture of the volume of alarms does not illustrate the differing situation within an operational site.

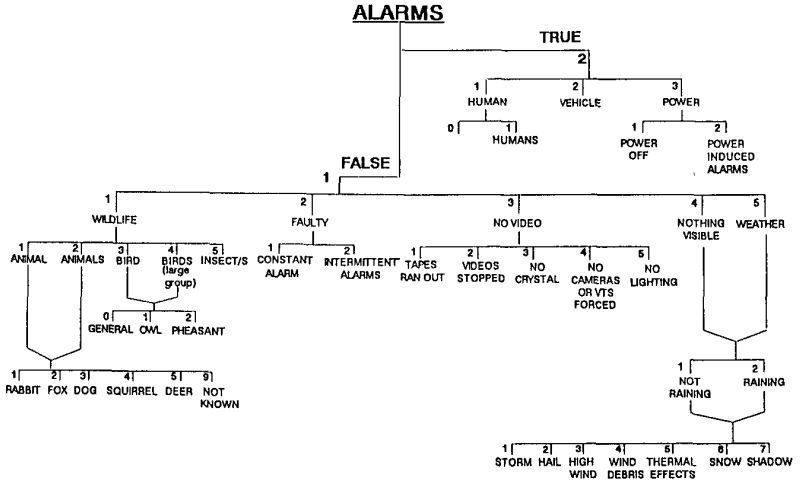

Table 1 Methodology for classifying the cause of an alarm.

SENSOR TYPE	CAUSE (%)			
Fence Mounted	ANIMALS	BIRDS	FAULTY PIDS	WEATHER
1	0	100	0	0
2	0	100	0	0
3	0	100	0	0
4	33	67	0	0
5	25	0	0	75
Other				
1	0	0	0	100
2	13	42	44	2
3	0	0	0	100
4	0	63	0	38
5	0	0	0	100

Table 2 Alarm causes for a typical site.

Table 3 demonstrates clearly the difference between "quiet hours" the normal "working" day. The ratio of unwanted alarms between these periods is approximately 10 : 1. Debates are often held as to how the likelihood of an escape should be combined with these false alarm rates. During the daytime a large number of prisoners will be fairly free to roam within the confines of the prison and it can be argued the likelihood of an escape attempt is high. Similarly at night prisoners should be within secure accommodation areas and the likelihood of one or more being in a position to reach the perimeter is very low. These situations place different demands upon the control room in terms of both the manning levels and the skills needed to discern more subtle attempts at escaping.

The analysis of alarm rates needs to be taken further before the true impact upon control rooms is seen clearly. Table 4 provides, for one specific system, the time between consecutive alarms. This data represents a typical perimeter reacting over many days during which the weather was seen to pass through a number of typical English days. The time between consecutive alarms is an important factor both in terms of the workload placed on the control room and the demands of any alarm verification techniques. Large number of alarms occurring within relatively short periods of time could swamp the control room staff and, place extreme demands upon the use of image storage and retrieval techniques if the verification is to be treated seriously. Some predictive work has been carried out [2] which enables the likely performance of alarm systems to be anticipated and control room manning levels could be adjusted accordingly.

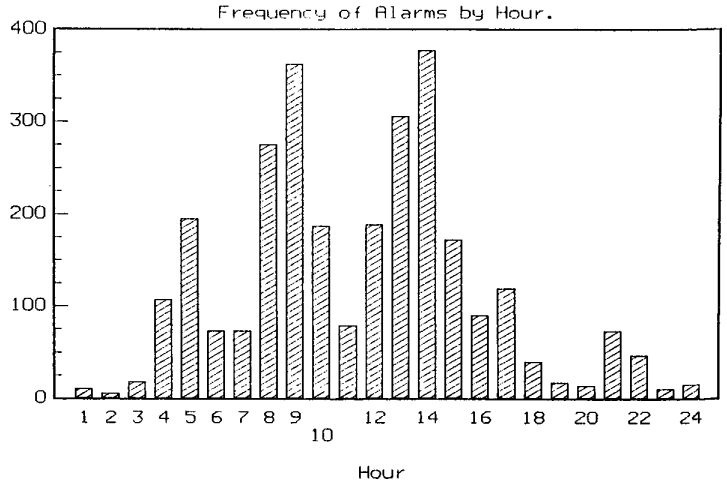

Table 3 Alarm rate variations over a 24 hour period - averaged over many weeks.

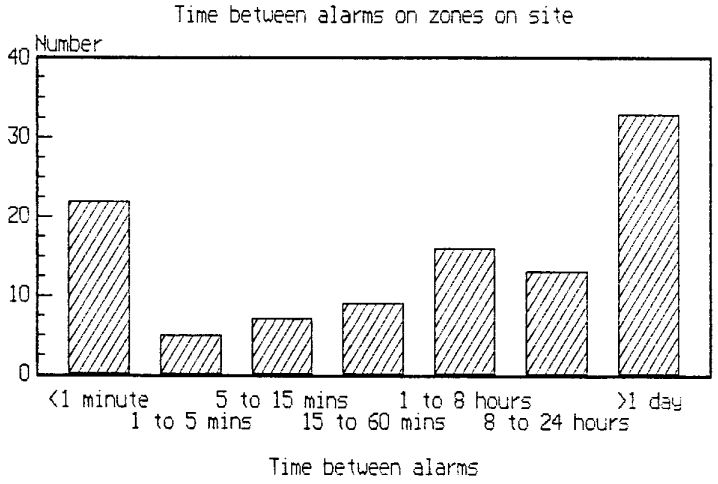

Table 4 Time between alarms for an operational system.

Table 5 completes the picture of performance of alarm systems by showing the percentage of days over an extensive monitoring period for which no false alarms were seen. Once again this illustrates the range over which the verification process is expected to respond. Table 4 illustrated, in the worst case, the very high false alarm rate which may occur on a relatively few number of days. However table 5 showed that for most of the time little demand will exercise the control room personnel.

SENSOR TYPE	
Fence Mounted	
1	100%
2	43%
3	70%
4	97%
5	41%
Other	
1	90%
2	20%
3	50%
4	80%
5	76%

Table 5 Percentage of days for which no alarms occurred - test site data.

SRDB'S Approach to the Problem

The Scientific Research and Development Branch of the Home Office has approached the challenge set by perimeter systems through a number of initiatives. Development of an improved microphonic cable system has been achieved. The use of IKBS techniques for multi-sensor data fusion along lines similar to those described in Carnahan papers by the General Research Corporation [3] has also been pursued. However none of these individual initiatives has been envisaged as providing adequate performance improvements for perimeter systems. The use of alarm verification techniques to assist operators is seen as a complimentary area of research and development. By capitalising on existing CCTV systems within an installation, the cost implications are less than those associated with more fundamental changes such as the use of new sensor technology. The early in-house work with alarm verification techniques has proved the concept. The current objective is to take the laboratory type equipment and tailor it in such a manner that it can be produced by industry in a commercially exploitable form.

Requirements for a Verification System

The requirements for an alarm verification system are that it should be capable of working with the range of PIDS systems currently in existence or envisaged for the market-place. Systems may be stand only (eg microwave), fence mounted (such as microphonic cable systems), or radiating cable systems which may or may not be associated with a physical barrier. The range of systems with which alarm verification needs to function exercises the talents of the system designer. Some PIDS are of a "one shot" variety namely they generate one response from a human as they cross the detection zone. However fence mounted systems are capable of providing a stream of alarms as the barrier is breached. Not only does the alarm system flag an attempted circumvention of the barrier, but the barrier holds the human within the field of view of any verification mechanism for a considerable period of time.

The range of sites for which verification systems are required is considerable. Small unmanned sites in remote locations are just as important as large establishments with relatively high manning levels. These site considerations place emphasis on the value for money which improved verification mechanisms could provide.

Within any proposed system there is a requirement for the operator to be able to confirm the output from the alarm verification mechanism. The importance of effective displays which minimise the workload placed on operators and improve their overall performance are of obvious importance.

Meeting the Requirement

The philosophy for alarm verification techniques was outlined in an earlier Carnahan Conference [1]. This work has been followed by researchers at City University. The City University work has enabled the basic rationale behind the use of intelligent knowledge based system (IKBS) techniques to be proved. This has been achieved through the use of bespoke software running on hardware configurations using commercial imaging systems. This work is described in an allied paper at the current conference (see Ellis et al).

The proof of concept work undertaken by City University has demonstrated how simple image processing techniques can improve dramatically the performance of operators in the on-line assessment of alarm cause. Further work has demonstrated the impact which IKBS techniques can have in performing automated alarm cause analysis. In order to turn the proof of concept into an operational system certain objectives associated with user requirements have had to be identified in order that the appropriate hardware environment can be configured.

Objectives Sought for the Operational System

The operation system is required to provide a dramatic improvement to the verification of PIDS alarms. The term "dramatic" equates to a throughput increase of between ten and one hundredfold of the ability of an operator to identify the cause of alarm.

The system is required to work with real time CCTV imagery (at least on input) and to enable verification to be completed within, at worst, a few tens of seconds.

The resolution of the system must, for operational sites, clearly be capable of resolving/discerning human targets presenting low cross sectional areas under a wide range of environmental conditions.

The system needs to work in conjunction with existing CCTV coverage. Thus the range over which the CCTV system looks, the time taken for an intruder to pass through the field of view of the system, and perspective effects are those found on existing operational sites.

Cost targets for operational systems should be considered against the price of the more advanced video motion detection systems. It is unlikely that end users will easily be persuaded to pay more than three or four times the cost of commercially available VMD systems unless the performance is of the order of 100 x better.

Design Considerations

The objectives outlined above map directly onto design considerations for the system.

The proof of concept work identified the need for image storage to be associated with the CCTV system. Thus, there will be direct cost implications depending upon the number of operational cameras on site.

The sensor type and any associated barrier will determine the rate at which images from cameras need to be captured. In the case of fence mounted systems a human will be within the field of view of a camera for many seconds. This contrasts with an individual running through a microwave beam when his presence may be of the order of 1 second. Image sequences capable of showing the motion of the human through the field of view of the TV system requires a number of images to be captured for each CCTV.

The performance of alarm systems, their association with physical barriers etc also influence decisions on "pre-alarm image capture". In many instances it has been found that the cause of an alarm is more readily identified if image sequences prior to, at, and after the alarm trigger are gathered. Pre-alarm image capture requires considerable numbers of image stores and becomes very costly with large numbers of cameras. The value of pre-alarm information needs very careful cost benefit analysis.

The increasing use of multiplexed rather than hard-wired systems for relaying alarms from the field to the control room can create delays of the order of seconds between the physical event and the control room being given an alert. Such delays can result in an intruder having passed outside the field of view of a CCTV camera before an operator in the control room is aware that a PIDS has gone into alarm. In such instances the use of pre-alarm image capture appears to be the only option, however expensive this solution may be.

Hardware Configuration to Meet the Requirements

The design of the hardware needs to consider the range of constraints discussed earlier in the paper. The issues which need to be addressed are discussed below.

The resolution of the image store could be either 256 x 256 or 512 x 512. Unless very high quality CCTV cameras, transmission lines and monitors are used, then 256 x 256 will suffice.

Economical use of frame stores by the careful selection of frame rate and number of images to be associated with each alarm is essential. Currently sequences of 8 images at a rate of 3 per second are being used at the test site. Other sites will require different values.

The field rate (50 fields per second UK, 60 fields per second USA) tends to constrain the maximum number of cameras associated with a storage device. Thus for cameras whose pictures are gathered at 3 frames per second, a maximum of 10 cameras could be stored on one device with a field rate of 60 fields (30 frames) per second.

Synchronisation of cameras is essential to enable fast picture-to-picture switching to be accomplished.

The design study has shown the need for a design which offers considerable flexibility in the amount of image storage which can be used. The basic operations of switching, capture and retrieval are common to whatever design is selected. Image storage is likely to be the single most costly element of the whole system and every advantage needs to be taken of the enhancement and automatic alarm verification techniques currently under development, in order that such costs are minimised.

Sophisticated labelling of image sequences is essential to enable their speedy retrieval when required.

The likelihood of simultaneous alarms on a system (eg table 4) needs to be recognised and accommodated by any design.

The requirements for storage of image sequences for subsequent manual verification need to be recognised.

A complex site will have a range of PIDS, IDS and camera systems all needing a tailored alarm verification mechanism. Flexibility in design is essential to meet varying end user requirements.

The choice of PIDS and barrier will dramatically influence the need, or otherwise, for pre-alarm image capture. Any hardware configuration should be capable of accommodating such user requirements.

The hardware design needs to be sufficiently flexible so that as many of the above constraints can be met. The basic field/frame rate tends to dictate the maximum number of cameras which can be accommodated once the capture rate and number of images in a sequence have been decided upon. Conceptually therefore modules of image store running at 50Hz (60Hz USA) are seen as a basic building block. Fast inter-field switchers feed synchronised images into this image store. The switcher/addressing logic needs to be fairly intelligent in order that, once an alarm is generated, the sequences from the camera(s) are preserved for verification.

The complexity of the addressing logic, combined with the likelihood of an operator wishing to perform long verification at the same time as new image sequences from other cameras are stored, tends to suggest that disc storage devices are inappropriate.

A schematic showing the outline design concept is given in figure 1.

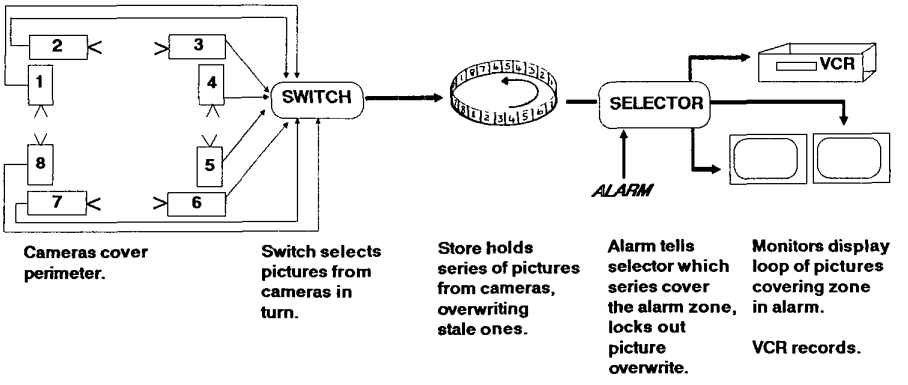

Figure 1 Schematic of outline design

Project Status

The project has reached the stage at which industry is to be encouraged to develop systems to meet the needs of end users. The Home Office has been using image sequences captured and retrieved by/from digital disc for a number of years. This experience has enabled the range of parameters such as the rate of image capture and length of sequence to be identified when the cause of an alarm is needed.

The enhancement of image sequences has been undertaken by City University and is, along with the research into the application of IKBS techniques for alarm verification, presented in an allied paper at this conference. The work undertaken by City University has given the Home Office confidence that such techniques should now move from the research and development environment into trials at operational sites.

The requirements of a range of users with diverse applications has been analysed and industry will be approached shortly. The objective of future work will be to encourage industry to develop systems incorporating the advances discussed in this and the allied paper in order that end users can enhance their use of manpower within a control room.

Acknowledgements

The help, support and guidance of the Prison Department is acknowledged. The expertise of those at City University and SRDB is reflected by the success of the work described in this paper.

References

[1] Custance, N D E, Proceedings of the 1987 International Carnahan Conference on Security Technology: Crime Countermeasures.

[2] Custance, N D E, Proceedings of the 1988 International Carnahan Conference on Security Technology: Crime Countermeasures, p 89-97.

[3] Bartek, R J, Proceedings of the 1988 International Carnahan Conference on Security Technology: Crime Countermeasures p 99-103.