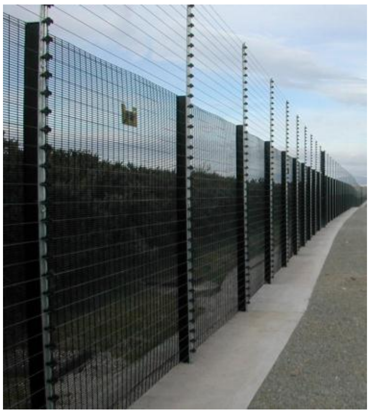
CPNI
Centre for the Protection of National Infrastructure

SURVEILLANCE THERMAL IMAGERS

GUIDANCE DOCUMENT

Issue 1: January 2014



Acknowledgements

The content of this document has been drawn from research publications and publicly available material published by manufacturers. CPNI acknowledges the help provided by the Isle of Grain Security Staff, NPL and Userperspective.

Any comments or suggestions regarding this document should be directed to: cse@cpni.gsi.gov.uk

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Executive summary

Traditional protection technologies, primarily visible band closed circuit television (CCTV), although very widely used, have limitations and there is an increasing interest in newer systems such as thermal imagers (TI). Until relatively recently these were only used in the military domain, but cheaper systems mean that they have become a viable alternative, with potential benefits over CCTV to civilian security systems. The use of Thermal Imaging systems is growing in popularity in the security industry and although the sales pitch for TI is compelling the imagery is rarely as good as the manufacturer implies.

Thermal Imager systems do not provide a 'familiar' image as seen by the human vision system or visible band CCTV systems and can be difficult to interpret. Distinction between 'friend' and 'foe' is difficult to make and although analytics can work on a smaller image size (presented on a screen) when a human views the footage the minimum image size is still determined by the human vision system. The minimum size of image is still comparable to that of a visible band camera. When CCTV or Thermal Imaging is being used by human operators the minimum target size, as a percentage of screen height, which will enable an attack to be recognised and detected should be maintained at 10%.

Thermal security cameras operate under low or zero lighting conditions. When conditions are ideal, thermal cameras allow an operator to 'see' what the eye cannot, even in complete darkness. However, the systems rely on temperature differences: no difference, no image. Outdoor conditions are rarely ideal.

Thermal imagers provide a 'different' view of the world. Interpretation of the imagery is not straightforward and as a result the human operator becomes an even more critical element of the threat management chain. The 'human in the loop' of a surveillance system brings limitations which must be understood. The human vision system is not perfect and has limitations on how much information it can attend to.

The issues for human perception and understanding that arise from TI technologies mean that both operator and guard force need to learn a different skill set when using TI technology rather than CCTV. There is an awareness of key issues such as the need to adapt ways to share an understanding of the environment as viewed from TI as opposed to CCTV communication in order to maintain a common situational and spatial awareness. It is important to apply the science and understanding of human factors to derive data and evidence from real-world environments to identify specifically what that skill set needs to be and how to train it.

Based on the background information in this document relating to TI systems, their potential use as part of a site's perimeter security system and the comparison with conventional CCTV systems, the following recommendations are made:

- **Operators should receive training on the use of TI systems and understand their limitations.**
- **Site-specific methods to ensure reliable identification of friend or foe should be developed.**
- **Quantitative understanding of the real operational characteristics of TI installation from a Human Factors (HF) perspective should be obtained**.

Contents

Introduction

This document provides background information on the technology and characteristics of human vision in relation to thermal imagery and discusses the issues that managers and operators of such systems need to be aware of.

Traditional protection technologies, primarily visible band closed circuit television (CCTV), although very widely used, have limitations and there is an increasing interest in newer systems such as thermal imagers (TI*). Until relatively recently these were only used in the military domain, but cheaper systems mean that they have become a viable alternative, with potential benefits over CCTV to civilian security systems.

Perimeters are often extensive. Maintaining lights as well as cameras can add significantly to the expense of securing the perimeter. TI systems offer advantages both in day-night operation and in terms of reduced costs.

* *The abbreviation TI and the term 'thermal imager' are used throughout the document to refer to thermal-based surveillance systems operating in the 3-5micron and 8-12micron band. Various commercial and scientific literatures also use the term 'thermal camera'.*

Recommendations

- **Operators should receive training on the use of TI systems and understand their limitations**, in particular when and how imagery is degraded and the issues that arise when interacting with a guard force or other personnel. Thermal imagery is a computer representation of heat within a scene and can therefore have a number of false colour techniques applied: white hot, dark hot or differential colours. Users should understand the differences these effects can give and what a "normal" scene looks like.

- **Site-specific methods to ensure reliable identification of friend or foe should be developed**. These should be detailed for proactive monitoring, alarm activation and during an event. During a genuine threat situation where will be considerable stress and possibly fear. Identification of friend or foe will be increasingly difficult with thermal imagery as the stress of the situation increases and the scene becomes busier.

- **Quantitative understanding of the real operational characteristics of TI installation from a Human Factors (HF) perspective should be obtained**. What are the false alarm and the false positive rates as well as the correct detection performance? Analytics combined with thermal imagers, used over longer ranges, should be compared with humans carrying out active CCTV monitoring at shorter ranges with visible band cameras. Once the quantitative data for these scenarios are fully detailed, a cost benefit can be calculated for the thermal imager system.

Thermal imagers

Thermal imagers are camera systems which collect radiation from that part of the spectrum where objects emit heat. They operate in the infra-red part of the spectrum, at longer wavelengths than visible light. The images they produce use differences in the thermal radiation emitted by the objects in the scene. These camera systems have found numerous applications in the defence and security sectors (military, border guards, police, etc.) and the civilian sector (industrial non-contact temperature measurement, non-destructive thermal testing, and tests of electrical power lines, building industry, medical applications and fire services).

Thermal security cameras operate under low or zero lighting conditions. When conditions are ideal, thermal cameras allow an operator to 'see' what the eye cannot, even in complete darkness (see Figure 1). However, the systems rely on temperature differences: no difference, no image. Outdoor conditions are rarely ideal:

- daytime thermal images often appear white and blurry, lacking scene details (see Figure 2)
- rain, heat and humidity degrade image quality
- thermal cameras may 'miss' intruders due to outdoor conditions, even at night
- the imagers introduce noise and blur
- the imagers have lower resolution compared to visible band systems
- depth information is lost or is limited.

An added limitation is that thermal images may not provide 'friend or foe' information (see Figure 3). Guard force personnel cannot be distinguished from intruders except by adding spatial patterns created by heat differences on the guard force clothing. Even then this could be duplicated by intruders or the imager may fail to resolve the pattern. As a result, many thermal cameras are unable to provide important details and situational context for making quick and effective security decisions.

Some of these limitations can be overcome by adding image processing technologies which aim to enhance the contrast using relatively standard image processing methods, as illustrated in Figure 4.

Figure 1: Typical surveillance thermal image. It contains fencing, walls, sea and a roadway.

Figure 2: Two images of the same scene (mooring and jetty viewed over water). On the left an image under good conditions, on the right reduced thermal information.

Figure 3: Example of lack of 'friend or foe' information. Two human figures can be seen on the right of the picture on the jetty. There is no information on whether these are intruders or not. Additional information – radio communication or knowledge of patrol schedules – must therefore be used to confirm identity.

Figure 4: How image processing can increase contrast in a thermal image to provide greater detail.

Further performance enhancements are possible with additional Video Analytics. A typical system might, for example, claim to provide the following capabilities:

- individual alarm zones with unlimited number of rules
- motion tracking
- control of alarm detection according to time of day
- from/to zones
- target size filtering to eliminate objects smaller or larger than a specific height/specific width
- target size filtering to eliminate objects smaller or larger than a specific aspect ratio
- wrong-way direction monitoring
- loitering
- track certain sized objects, but do not alarm on them.
- ‘object left behind’ detection
- speed alarm detection (either above or below a user-specified threshold)
- automated pan-tilt-zoom (PTZ) control
- selectable tracking priority

These capabilities appear to provide a sophisticated and robust intruder alert system. In reality this is almost certainly not the case. Operationally such systems need continual fine tuning to set appropriate parameters. This is mainly due to seasonal variations in the site. Drift and changes in the camera systems add to the problem. Any modifications to the video analytics software will generally require a specialist from the manufacturer and can therefore add significantly to the through-life cost.

Thermal imagers provide a ‘different’ view of the world. Interpretation of the imagery is not straightforward and as a result the human operator becomes an even more critical element of the threat management chain.

Thermal imager security cameras allow a person to ‘see’ what the eye cannot, even in complete darkness. In general, manufacturers present imagery acquired under ideal conditions to potential purchasers. This can give a misleading view of the effectiveness of such systems. Typical imagery is not perfect and under some conditions can be severely degraded. When poor imagery is combined with the limitations of the visual and cognitive processing capabilities of a human operator, performance is downgraded, compromising site protection.

Operation and environment

Our eyes work by seeing **contrast** between objects which are illuminated by the sun or another source of light. Thermal cameras work by sensing **heat energy** from objects. Temperature differences between different parts of a scene are converted into different grayscale values in an image which is then displayed to an operator. The degree to which objects emit heat is called emissivity. All objects – living or not – have an **emissivity**[*] and temperature that thermal cameras can use to detect an image.

[*] The **emissivity** of a material (ε) is the relative ability of its surface to emit energy by radiation. It is dependent on a wide range of factors.

- **The primary benefit to sensing heat is that heat is always available at any time of the year, day or night.**
- **Thermal imagers can operate at all times, even in complete darkness, without the aid of natural or man-made lights.**

In order to present heat in a format useful to the human eye, thermal imagers convert the temperature of objects into shades of grey which are darker or lighter than the background. These shades of grey are displayed as an image. The sensitivity of the camera is typically described by the minimum resolvable temperature difference that can be detected. For these reasons, thermal cameras have become a useful tool for surveillance because generally, at night, background objects tend to be cooler than a person. Under ideal conditions, people are clearly emphasised at night because they appear brighter than the background and stand out, even in zero light.

Figure 5: Comparison of visible band and thermal camera images for two scenes. For the scenes on the left there is generally no particular advantage of thermal over visible. However in the scenes on the right the individual would not be visible at night with the visible band camera.

The imagery created by thermal cameras is different from visible as shown in Figure 5. Even this simple situation is more complex than that found with ordinary cameras and vision. In the normal visible band, objects typically maintain the same contrast polarity whereas in thermal images object contrast polarity can alter depending upon prevailing conditions.

*(Note that we refer here to the **physical** contrast polarity. **Perceived** contrast polarity can be modified as a consequence of context, particularly in scenes that are sparse compared to natural or man-made environments*.)

- **On a cold day a person stands out as lighter because they are hotter than the background.**
- **On a hot day a person stands out as darker because they are cooler than the background.**

Outdoor conditions are rarely ideal. Problems occur when the environment is such that background temperatures are close to the temperature of objects which represent a security concern, such as a person entering an unauthorised area. When background temperatures closely match the heat of a person, the temperature differences become too small for the imager to measure them effectively. This converts to an image with very little contrast so that the intruder blends into the background and becomes concealed, even when they are close to the camera, while the overall image appears blurry and poorly defined.

Atmosphere and weather

The aim of any surveillance system is to detect a threat at sufficient distance (or as early as possible) to provide an appropriate and effective response.

A thermal imaging camera produces an image based on the differences in thermal radiation emitted by an object. In essence, the further this infrared signal has to travel from the target to the camera, the more of that signal is lost along the way. This **attenuation factor** needs to be taken into account. Humid air acts as a 'shield' for infrared radiation. Summer month atmospheres usually have a higher attenuation compared to winter months due to increased humidity levels. Therefore, assuming clear skies and good weather conditions, you will be able to see further with a thermal imager in winter than in summer.

Humid air is just one example of how infrared radiation can be lost. Other climatic conditions are far more detrimental to the range of a thermal imager: fog and rain can severely limit the range of a thermal imaging system due to scattering of light off droplets of water. The higher the density of droplets, the more the infrared signal is diminished. An important question is how much rain or fog will limit the range performance of a thermal infrared camera, and how does this compare to the range in the visible region of the spectrum. In the UK climate this can be highly significant.

Human vision and images

The ‘human in the loop’ of a surveillance system brings limitations which must be understood. The human vision system is not perfect and has limitations on how much information it can attend to.

Limitations on human vision include the following:

- fine picture details (high frequencies) are less visible
- errors in textured regions are difficult to see
- errors near high contrast edges are difficult to see
- visibility threshold increases as background luminance increases
- reduced visibility of one detail in the presence of another
- low sensitivity to high frequency noise
- below 50Hz flicker effects are noticeable
- high luminance increases perceived flicker
- low spatial frequencies reduce sensitivity to flicker

In addition to these inherent limitations there are optometric factors. In some individuals there is a need for visual correction (spectacles/contact lenses). In addition, a significant proportion of the male population (8%) has some degree of colour vision deficiency, which must be considered when any coloured graphical overlays are used. On top of this visual function deteriorates with age – in particular glare in the eye increases and contrast sensitivity declines.

Prolonged viewing of display systems causes visual fatigue. This is exacerbated by having to view images which primarily comprise low contrast areas – such as TI imagery.

Threat detection

Using a surveillance system to detect a threat is never completely reliable as there are always uncontrollable factors, and therefore errors occur. This is true for any sensing system, including imagers, irrespective of whether it is a person or a video analytics system analysing the images. It is accepted amongst the community of researchers in this field that an individual can look at a clearly visible target and yet not register its presence.

For any particular surveillance situation when an event occurs there are four possible outcomes once a decision has been made. These are illustrated in Figure 6.

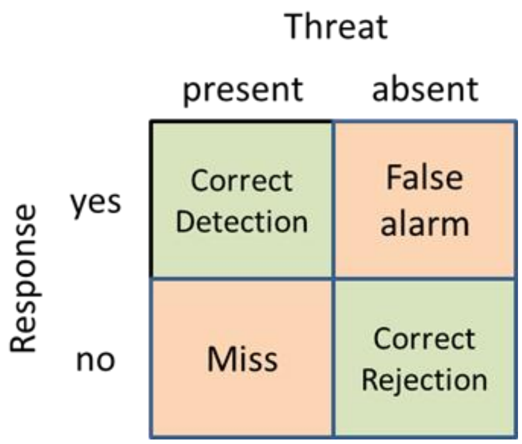


Figure 6: Matrix of event classifications.

With the increasing use of video analytics we have two processes which operate in the way outlined in Figure 6. Firstly, the analytics system, and secondly the operator. Although the overall performance of the image analysis system combined with the human operator can still be described using the formalism of Figure 6 there is an interaction. If we consider an extreme example where the analytics system misses every event then the human operator can never detect an event **if only relying on the analytics alerts**. Alternatively if the analytics system reports everything as an event then the performance of the system is then solely dependent on that of the operator. These are obviously unrealistic scenarios and in fact real systems operate in some middle region. The analytics system may miss an event such as people walking in a forbidden area, but the operator may detect them. The analytics system may detect an event invisible to the operator but the alert can still be acted upon even if the operator cannot see a visible event. This changes when the operator is required to verify every alert and the false error rates are a combination of both the misses of the analytics plus those of the operator.

The key aspect to understand is that the four events in Figure 6 interact. Simply driving down the false alarm rate will increase the number of missed events and vice versa.

Even if the analytics system operates simply as an ‘alarm’, this will still have to be processed by a human operator interpreting the images and this will be affected by the imperfections and illusions described in the remainder of this document.

When CCTV or Thermal Imaging is being used by human operators the minimum target size, as a percentage of screen height, which will enable an attack to be recognised and detected should be maintained at 10%. This is a limit of the human vision system; any smaller image size is not reliably recognisable or detectable by a human.

Contrast

The fundamental property of the visual world that determines detection and identification of objects is contrast. **Contrast determines performance in all visual tasks**. It can be based on luminance, colour, motion, texture or stereo, or combinations. Currently pure stereo contrast is not found in TI images. Examples of varying contrast and its effects are given in Figures 7 and 8.

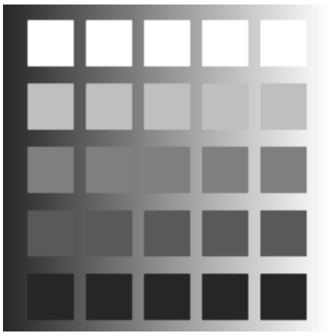


Figure 7: Luminance contrast. Along each row the squares have the same luminance but due to varying contrast the human vision systems views the squares as differing.

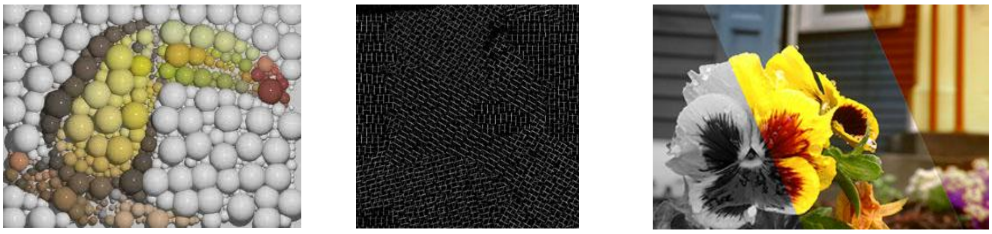


Figure 8: Illustration of alternative contrast types. Left to right: pure colour contrast, texture contrast and simultaneous luminance and colour contrast.

It is important that any TI system delivers sufficient contrast at the scale of the object that is to be detected. This will typically be a human figure and the scale will depend upon the amount of magnification applied to the scene. If the human figure is small then the system must deliver more contrast.

Light adaptation and brightness perception

The retina does not simply record light intensities. Rather, the signals from the eye which are passed to the brain depend on the surrounding context:

- The sensitivity of the cells in the eye which detect light depends on the average/ambient light intensity. This is referred to as **light adaptation**.
- The outputs from the eye to the brain depend on the difference between light intensity in the centre and that in the immediate surround.

Impact on perception

Human vision has evolved to deliver as constant a perception of the world as is feasible. We still do not understand how most of these computations are carried out by the brain.

Consider two pieces of paper, one black and one white. If they are viewed inside they look black and white. When they are viewed in bright sunshine they still look black and white. The image of the black paper outdoors is actually more intense than the image of white paper indoors. This phenomenon is called *brightness constancy*. It **helps the visual system achieve *perceptual constancy*: white looks white and black looks black regardless of the level of illumination.** The visual stimulus that reaches the eyes depends both on the illumination level (indoor light vs. outdoor light) and the reflectance of the surfaces. In thermal images however, it is emissivity and not reflectance that determines how light or dark an object is. So our visual system must apply rules that were not developed for our physical process. There may therefore be some additional cognitive component in interpreting thermal scenes when object lightness may be unstable.

Simultaneous brightness contrast

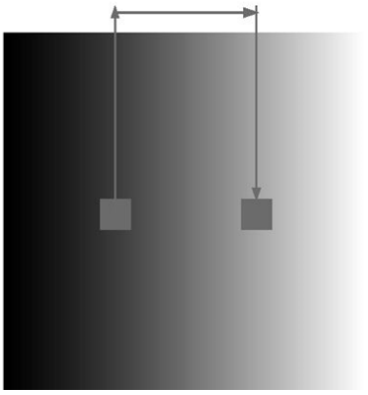


Figure 9: Illustration of simultaneous brightness contrast.

Compare the brightness of the two grey squares. The one on the left should appear brighter to you. In fact, this is a visual illusion; the two central grey squares are physically identical. This illusion can be explained by what we know about the visual processing in the retina. Retinal responses depend on the local average image intensity. On the left, the background is black so the average intensity there is very small.

The implication of Figure 9 is that there is an intermediate region where, because of the background, the square will be invisible. TI systems deliver contrast polarities which are different from normal visual systems, so hot objects are typically lighter. The figure illustrates that even if a TI camera produces a white object of a given luminance the object may still be invisible due to the local context.

Human visual perception is not 'truthful' but achieves a view of the world by making calculations. The calculations attempt to generate a stable picture of the world and are in turn based on internal assumptions about the properties of objects in the world. The example above provides the same grayscale as that produced in TI images. The brain has evolved to make these calculations in a world where surface reflectance determines the properties of a surface. However this is not the case in thermal images.

Attention

We are aware of only a small portion of the information that continually bombards us. Conscious experience seems to have a limited capacity; we can only attend to one thing at a time. Attention helps us decide where to move our eyes next. Our perception of a scene is developed by a combination of attention, eye movements and memory.

Eye movements occur approximately three times per second and are generally involuntary. Figure 10 shows examples of eye movements from two individuals looking at the same scene.

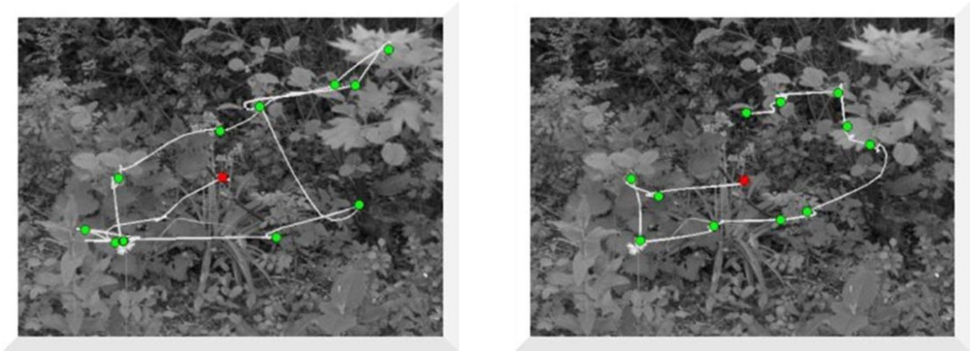


Figure 10: Fixations of two subjects. Red square shows first fixation. Green dots show computed fixations. White line shows the 'raw' eye movement trace.

What determines where we look? There are two elements: so called 'bottom-up' factors which are effectively aspects of the scene we are looking at, and 'top-down', i.e. cognitive factors.

- bottom-up factors comprise **colour, luminance contrast, motion, and orientation**.
- top-down factors are typically **tasks or goals, context and memory.**

Again this emphasises that human vision has a limited capacity in what can be processed.

Thermal images will influence attention through the bottom-up components. The motion cues in the images are similar to normal CCTV images but other cues may well be reduced. The author is unaware of any work undertaken to specifically compare eye movement patterns in thermal images compared with CCTV.

Thermal versus CCTV systems

CCTV combined with traditional lighting

CCTV systems have been an effective tool for security and surveillance applications for many years. However, just like the human eye, CCTV cameras do not function in total darkness. In order to detect intruders at night they require additional lighting. Although some lamps (fluorescent lamps, high intensity discharge (HID) lamps) are more efficient than others, the operational cost is very high. Light can only penetrate a certain distance, and completely illuminating an area so that it can be kept within the range of CCTV cameras is not always possible, or adds significantly to the cost. Moreover, lights can act as glare sources for personnel patrolling on foot. Advantages and disadvantages are set out in Table 1.

Technology	Advantages	Disadvantages
CCTV with traditional lighting or LED	• Good resolution during daytime • Provide friend/foe identification • Relatively low initial cost • Imagery is familiar	• Degraded imagery under low light levels • Limited detection at night. Light illuminates only certain small area • Limited capabilities in fog, rain, and other adverse weather conditions • High power consumption • Need to maintain both lights and cameras
Thermal imaging	• Full awareness • Can be used day and night • Works in practically all weather conditions • Can see through some fog, rain, smoke • Extremely difficult to hide from since thermal contrast is practically impossible to mask	• Thermal contrast may be low • Potential intruders are detected but not identified

Table 1: Comparison of CCTV and TI systems

Lights can even provide assistance to intruders. Lighting an area essentially lays out a route of attack, and potentially creates shadows in which intruders can hide.

There may also be significant labour and material costs associated with lamp replacement. CCTV systems with traditional lamp lighting require lamp replacement every 2000 to 4000 hours or about every 8 months. Compared to any standard light bulb, light-emitting diodes (LEDs) provide significant savings on electrical consumption. LEDs have a long life performance with little on-going maintenance cost. Infrared illumination with LEDs (also called Active Infrared) beam infrared radiation into the area in front of a camera. The LEDs are often placed around the lens of the camera. LED illumination is compromised by limited range performance.

Environmental factors

Most thermal cameras have difficulty presenting good outdoor images due to the impact of the dynamic environment. Even night time applications create difficulties for thermal cameras when conditions reduce the temperature contrast between objects in the scene, leading to concealment of targets.

- Rain and humidity bring objects in the scene to a similar temperature to that of the background.
- A background that is close in temperature to a person camouflages an intruder.
- Wind cools objects.

Moisture in the air from rain and humidity can therefore easily conceal any humans within the scene. This is similar to the visual experience of looking at someone in white clothes standing in front of a white building. When there is little visible contrast between the edges of a person and the background, the person looks blurry or even 'disappears'. Likewise, when environmental conditions create a uniform temperature across a scene, the absence of contrast will cause thermal cameras to miss intrusions entirely.

Another environmental issue to consider is that Thermal Imagers cannot see through glass. Glass is a very good insulator and therefore will not 'transmit' the thermal radiation though it.

Thermal loading and white-out

During the day, darker objects absorb the sun's energy and heat up. When objects in the scene become uniformly hot in some areas, many cameras have difficulty mapping the wide range of temperature differences into a useful image. Thermal cameras display hotter objects as lighter shades of grey, resulting in areas that look white and undefined. Contrast differences which are needed to discriminate objects and people are minimal therefore wherever these areas occur.

White-out is not limited to bright summer days. In winter, the sun's energy will raise the temperature of objects such as pavements and buildings to be much higher than the ambient temperature. The temperature of the background can often exceed that of a person, creating situations where a person cannot be seen even on cold days.

Thermal crossover

Thermal crossover is a phenomenon where the temperature of two different objects in a scene is indistinguishable. For example, buildings and car parks which are heated during the day start to cool after sunset and at some point, for a period of time, they 'cross over' the temperature of an intruder (37C), becoming almost identical to the temperature of that person. When targets are very close in temperature to the background, they are displayed on the monitor as a similar shade of grey. The eye cannot distinguish between very close grey scales, and so the intruder becomes invisible against the background.

Distance

The amount of energy arriving at the thermal imager from objects that are further away is lower than the energy from objects which are closer to the camera. The air itself further reduces the energy as it travels through the atmosphere, worsening over longer distances. In addition the resolution of thermal imagers is generally poorer than conventional CCTV, so many of the finer details of distant objects are lost, resulting in backgrounds that lack clarity and appear out of focus. Lack of image clarity obviously reduces security effectiveness. Scene details such as towers, buildings or other objects provide important context about what a camera is viewing. As a consequence:

- it becomes difficult or impossible for operators to make good security decisions without context
- security personnel who have to view blurry, undefined video – even on a single monitor – can become fatigued and confused by images which are not as intuitive as they would be with daylight cameras.

What can you see with a Thermal Imager?

This section introduces concepts and methods for assessing the performance of thermal cameras based on visual performance rather than resolution measurement.

Thermal imagers extend an operator's vision because they provide advantages over human eyesight. They detect radiation that cannot be seen by the human eye and the object can be magnified; that is, the angle subtended by the object at the eye can be greatly increased, making it easier to see. This comes at a cost however; the imager blurs the target and adds noise to the viewed scene as illustrated in Figure 11.

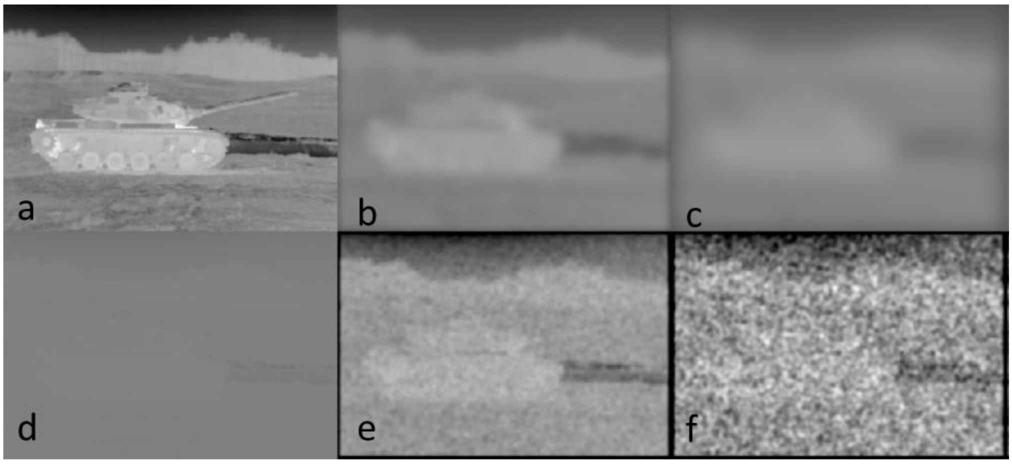


Figure 11: Thermal image of a tank showing effects of blur and noise.

(a) Pristine image; (b) blurred by imager; (c) further blurred;

(d) low-contrast image; (e) and (f) increasing gain to improve detection of the low contrast object amplifies detector noise.

Figure 11 shows the issues with degraded image quality and the difficulties in viewing attenuated images (images a-d). Many Thermal Imager systems attempt to increase contrast by adding image enhancement. Images e and f show the 'noise' and artefacts generated by image enhancement.

A key consideration to improve image quality will be the image resolution. Across all imagery the smaller the detail that can be resolved (higher resolution) the better the end image quality will be.

To benchmark a Thermal Imager system, surveillance-relevant test targets are currently available and should be used to check the area covered by each camera view. Figure 12 shows a visible band image of a Thermal Imager Test Target developed at the National Physical Laboratory (NPL).

Figure 12: Visible band image of NPL test target 50% screen height.

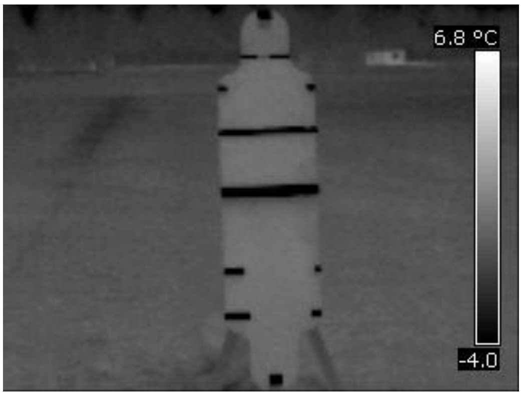


Figure 13: Thermal image of the same NPL test target 100% screen height.

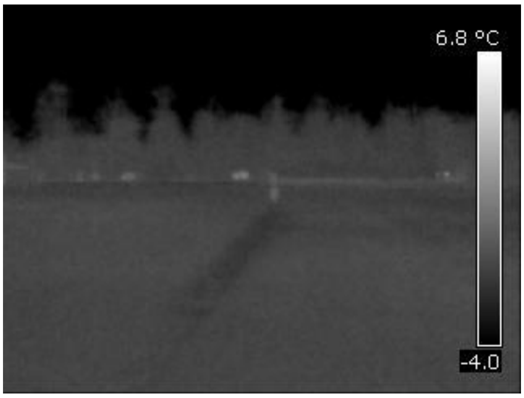


Figure 14: Thermal image of the same NPL test target at increased range (10% screen height). This illustrates the reduced contrast, even at a relatively short range to the target.

Ultimately, the installer of a thermal camera wishes to know how well it can provide detection, recognition or identification information. To meet this goal, an image quality metric is needed as a link between quality of vision and task performance.

Johnson Criteria

A large body of research exists on determining a meaningful metric. It is usually the case that a set of values called the Johnson Criteria are used. A number of manufacturers of thermal camera systems report their performance for visual tasks using Johnson Criterion metrics for instance. However these are based on military requirements and not recommended for surveillance requirements.

Interaction with the guard force

The previous sections have discussed visual perception and image quality issues in performing surveillance tasks. There are additional 'human factor' implications which arise when there is a switch from CCTV cameras to thermal ones due to the type of imagery these systems produce. One of the most obvious differences is that there is no ability to identify individuals as 'friend' or 'foe.

The field of human factors provides a scientific understanding of what humans are physically and mentally capable of. However, it goes beyond simply understanding what a person **can** do in terms of maximal performance or even what the human **should** do as prescribed by manuals and Standard Operating Procedures. Again this is different from understanding what people **will** do in given circumstances.

The context

Although it may be assumed that CCTV/TI operators have their eyes wholly focused on the camera, the reality can be very different. Often an operator has many other tasks to perform: responding to radios, answering telephone calls, logging incidents, reacting to customer queries, dealing with car parking, responding to a door/lift/fence/escalator alarm, and so forth. How often a CCTV/TI operator has the opportunity to focus solely on the cameras is usually limited and because of this they are often reliant on the input they receive from the guard force on the ground.

It may also be assumed that the working relationship between the operator and the guard force is one of a united team. This is not always the case and a lack of trust and co-operation may exist. For example, the guard force may feel resentful of an operator in a warm control room, being paid more money or being perceived by the organisation as being of more value. The guard force may perceive themselves to be doing an equally important role but working in uncomfortable conditions, less well paid and less respected by the organisation. Other factors may also combine to prevent mutual understanding; such as the operator not knowing the site as well as the person on the ground. Additionally, if one of the parties has English as a second language or is poor at radio communications then this can be a cause for frustration and bad feeling when receiving or relaying information.

Understanding what is happening in any situation may be influenced by the information that is being received and how it is interpreted. For example, an operator viewing a scene may simply see an individual who needs to be identified as either friend or foe and so tasks the guard force member to approach and question. The guard on the ground may or may not have a greater sensory input. This means the guard will be interpreting what is being said, the manner in which it is being said and the 'feeling' from the crowd or others around. These are elements of input that the operator will be denied. What may appear as a simple conversation to the CCTV operator may sound highly threatening to the guard based on the additional verbal and other sensory information they are interpreting.

The overall understanding of a situation may be put under stress by the very different views accorded to operators and guard force. For example, landmarks used as common points of reference during the day may be completely obscured to the guard on the ground at night in limited lighting conditions. Landmarks or alternate means of way finding may need to be explored in order for the operator with the TI image to be able to direct the guard on the ground who is using a torch. Further, both parties need to make the right decision about how to deal with the situation based on information which may be more limited than that usually experienced when using CCTV images.

Interacting with the technology

With the increasing introduction of TI cameras, the interaction between the technology, the operator and the guard force may introduce additional complexities. Issues with identification of the target (what, who, where) can be compounded when trying to direct a guard force member without being able to give them any of the usual visual cues, e.g. blue basketball cap, standing by the girl with the Boots carrier bag, close to the red and green concert poster. The lack of usual visual cues available to the operator to give a guard force member on the ground also works in reverse, particularly as it is often the guard force who will inform the CCTV/TI operator of an issue.

Situational awareness can be compromised from the outset, as the guard force member may have difficulty in getting the operator to identify the correct person or the operator may believe they are tracking the correct individual when in fact they are not. This basic error may come to light too late for either the guard or operator to be able to address.

As already discussed, the images the TI operator sees will likely be more degraded, have a lower detection range, and be unable to see through glass. These factors are also frequently combined with the effects of thermal clutter in busy environments or with reflected heat. Such issues are additional to the lack of important visual cues which, as noted, are usually available via CCTV but unavailable with TI to the operator. Cues have been noted to include landmarks which may be used to help direct the guard force/operator; colour; and body language. In addition to the lack of 'usually' available visual cues comes the need to provide both the guard force and the operator with an awareness of the differences from each other's perspective, and how to give guidance to both parties with regards to detection, tracking, decision making and actions when their normal identification cues are unavailable.

The issues for human perception and understanding that arise from TI technologies mean that both operator and guard force need to learn a different skill set when using TI technology rather than CCTV. There is an awareness of key issues such as the need to adapt ways to share an understanding of the environment as viewed from TI as opposed to CCTV communication in order to maintain a common situational and spatial awareness. It is important to apply the science and understanding of human factors to derive data and evidence from real-world environments to identify specifically what that skill set needs to be and how to train it.

Terms and definitions

CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
HF	Human Factors
NPL	National Physical Laboratory
SDT	Signal Detection Theory
TI	Thermal Imaging