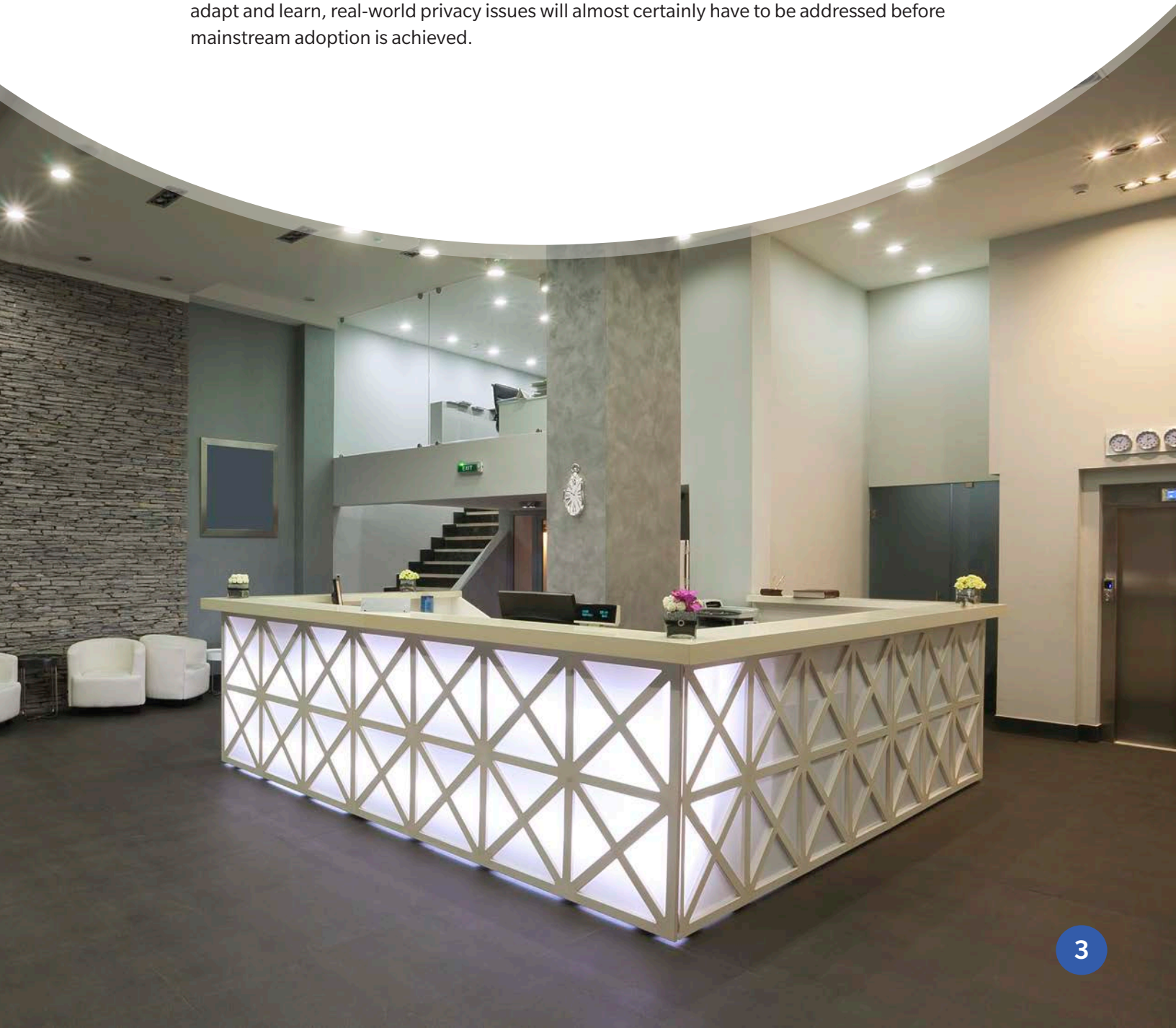
Ensuring Privacy in Next-generation Room Occupancy Sensing

Rambus

- Introduction
- **Part 1:** Conventional Occupant Sensing Technologies
- **Part 2:** The Problem with Cameras
- **Part 3:** Lensless Smart Sensors (LSS)
- Conclusion

Introduction

The long-awaited promise of smart homes and buildings adapting to occupant preferences and requirements is slowly becoming a reality. Traditional sensing technology is still somewhat limited in this context, with sensors primarily designed to detect motion rather than occupancy. Fortunately, new smart sensor technology offers the promise of true occupancy detection, along with an improved understanding of space utilization and occupant traffic patterns. Smart sensors can also help save power consumption by enabling truly responsive lighting and facilitating efficient HVAC utilization. Although next-generation sensor technology offers a glimpse of an exciting future in which buildings adapt and learn, real-world privacy issues will almost certainly have to be addressed before mainstream adoption is achieved.



Part 1:

Conventional Occupant Sensing Technologies

Currently, occupancy detection is typically implemented using a wide range of conventional sensor technology, including passive infrared (PIR), microwave, ultrasonic, vibration and acoustic.

Passive Infrared (PIR)

PIR sensors are primarily designed to detect movements or changes in heat sources within the sensor Field of View (FOV.) Although PIRs excels at sensing dynamic motion, the technology is typically unable to detect true occupancy, as the sensors require significant motion to 'trip.' In addition, PIRs are often paired with timers to activate (room) lighting systems. However, PIRs may not be able to detect movement if the occupant sits relatively still while typing, reading or watching television. This frequently results in PIRs timing out, forcing the occupant to wave a hand or create some alternative form of dynamic movement to re-activate the lighting system.

Microwave & Ultrasonic

Microwave sensors emit pulses and measure the subsequent reflection off a moving object. Similar to PIRs, microwave sensors can be used to detect motion and are typically deployed in larger areas. Nevertheless, higher manufacturing costs typically prevent wide-scale deployment of the technology. It should also be noted that PIRs and microwave sensors have been combined to reduce false alarms. Although this method facilitates a more refined signal, motion is still imperative. And while combined sensors offer a high degree of accuracy, they are considered quite costly. Ultrasonic sensors, while less prone to errors stemming from external electric forces, face similar cost issues.

Vibration & Acoustic

Vibration sensors are relatively inexpensive to produce, although they are prone to a wide range of false positives, including those caused by elevators, movement in neighboring areas, building sway from winds, natural settling and earthquakes. Building engineers may also install acoustic sensors in conference rooms to detect occupancy and approximate the number of people in a room. However, acoustic sensors are imprecise and can be erroneously tripped by background noise emitted by building environmental systems.

Limited Functionality, Limited Privacy Issues

Except for acoustic, there is little to no privacy risk associated with the above-mentioned technologies. While somewhat limited in terms of capabilities, these sensors can be deployed in grocery stores, office conference rooms and private areas such as restrooms and gym locker rooms. Nevertheless, new sensing technologies are currently being designed to significantly improve building and home automation systems. These sensors will enable buildings to intelligently and adaptively respond to occupants, rather than simply detecting them.

Part 2:

The Problem with Cameras

Cameras produce a wealth of data about their environment by forming a focused and detailed view of a specific area. Aided by off-the-shelf algorithms, cameras are routinely deployed in public areas to detect and analyze human movement. For example, airports primarily deploy cameras to identify occupants, which are also used to analyze waiting times in security lines. This allows airport personnel to leverage occupant counting and dwell data to generate metrics on average wait times. Grocery chain Kroger has adopted a similar use of the technology, with cameras helping to minimize customer wait time by deploying cameras to track the number of individuals waiting for a register.

While undeniably versatile, cameras cannot be used for occupant sensing in semi-private and private areas due to very real privacy, security and legal risks. Indeed, the installation of focused cameras in non-public spaces is strictly curtailed by certain countries. In England, for example, a homeowner may not legally deploy a security camera that has any private space within its FOV outside his or her property. In most countries, the entity responsible for deployment is also held accountable for the repercussions. For instance, of a focusing camera from an office space is hacked and the resulting stolen images or video used to commit a crime, the owner of the building may very well be deemed liable.

In addition, cameras may prompt a feeling of unease amongst many people, whether at home, on the street and at work. Workplace culture experts have stated repeatedly that trust is one of the most important aspects of any corporate environment. Lenses tend to communicate an absence of trust, no matter what their stated purpose. At home, the desire for privacy becomes even more pronounced. The widespread use of focused cameras by homeowners is often perceived as taboo, no matter how secure the deployment, since a hacked focused camera inevitably exposes private areas of our lives. Although focused cameras do facilitate occupancy tracking, they also create focused images and video which are subject to hacks.

Risks like this have provided a legal reason for the removal of, or non-installation of focused cameras in non-public areas by 3rd parties. Beyond the legal reasons however, there are also physiological 'human condition' issues.

Moving to residential installations of focused cameras, the desire for privacy becomes even more apparent. The use of focused cameras by homeowners is often seen as not acceptable, no matter how secure the deployment, since a hacked focused camera exposes private areas of our lives.

To test the limits of how secure a focused camera would have to be, Rambus has performed the following (admittedly unscientific) litmus test. When speaking of our LSS solution (later in this document), we've proposed the alternate idea of a focused camera being placed in a 'black box', with only the lens exposed. Electronically, the only input to the box is 100-240VAC, and the only output of the box being decision data ('yes' and '5 people in the room', for instance). Asked when this solution would be acceptable for the main areas of their houses, most respondents have said "no". To those who said yes, the same camera was then moved to their bedroom

and the bedrooms of their children and/or parents. At this point, most of the "yes"s turned to "no"s quickly. The risk of privacy invasion is cited as the primary reason for a "no", regardless of how secure the solution is. Lenses (and cameras by extension) create focused images. The risk of privacy invasion through hacking is simply too great to offset the potential benefits.

While focused cameras enable a measurement of room occupancy, they fail in that they also create focused images and video which are subject to hack and exposure by nefarious parties, not to mention spooking their users.

What About De-focused Cameras?

By their nature, cameras create focused images fit for human viewing. People are accustomed to this, and our natural assumption is that all cameras are creating focused images.

However, a proposed solution to room occupancy sensing is the use of a purposely defocused camera. This involves either using a lens that is not specifically designed for the camera electronics (creating a 'fuzzy' or 'warped' image), or physically rotating the lens within the camera into a position where the image is out of focus, and then locking it in that defocused position. Since the image/video is defocused, identifying a specific person or persons within the scene would be impossible, lowering the risk of exposure of personal information. The video data from the defocused camera could still be a viable measurement in a room occupancy solution where the goal is to recognize movement and occupancy (which doesn't require a focused image).

Looking first at the technical hurdles facing de-focused cameras; the simple fact is that a de-focused image can be computationally refocused. The re-focused image may not attain the same level of image quality as a native image that was captured with a focused camera, but can likely be restored to a level of quality that is identifiable to the human eye.

The process of refocusing an image is well understood, with methods published in numerous scientific journals and papers, and available freely on the internet. Figure 1, showing before and after images, is just a single example of this:

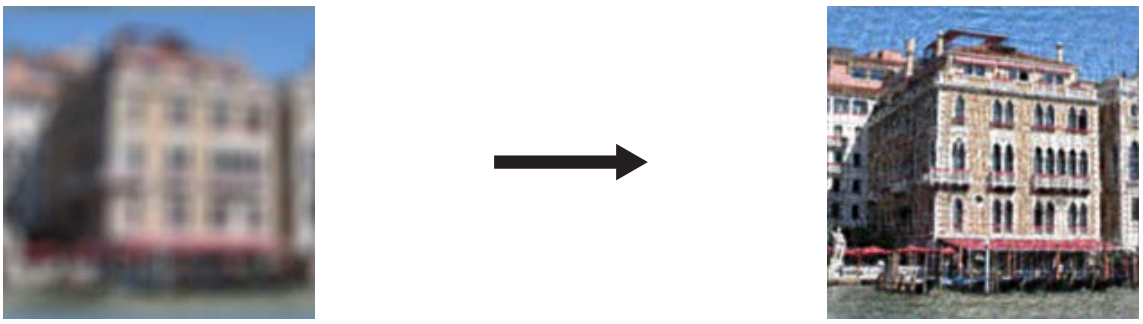


Figure 1: Defocused Camera Restoration, Source: http://yuzhikov.com/articles/BlurredImagesRestoration1.htm

It should also be noted that the complexity of refocusing is contingent upon how defocused the original image is. Even if the specific system characteristics of the defocused camera are unknown by the attacker, blind deconvolution methods often succeed in generating a refocused image. Special computing technology is not required, as off-the-shelf applications can be programmed to optimally and automatically refocus images. Although manufacturers of defocused camera-based sensing solutions may theoretically reduce privacy risks, the specter of hacks and readily available reconstructive algorithms mitigate any potential benefit offered by a de-focused camera.

Part 3:

Lensless Smart Sensors (LSS)

Lensless smart sensors (LSS) are a novel method of sensing. LSS combines a standard CMOS sensor like those found in focused and defocused cameras, but replaces the lens with an extremely small anti-phase binary diffractive grating. This grating sits in the optical path, with light passing through it intelligently spread onto the low resolution CMOS sensing element below it.

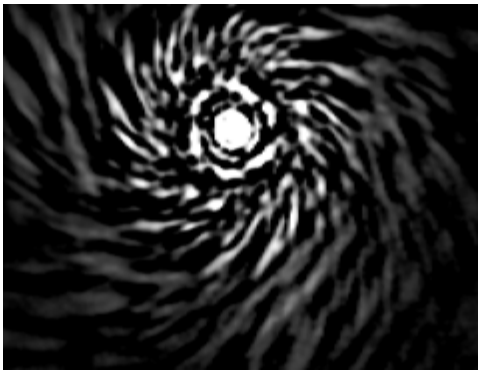


Figure 2: Single PSF

LSS does not capture focused images. LSS also does not capture purposely de-focused images. Rather, it creates what is called the 'blob' domain, which is a series of point spread functions (PSF) of light. An example of a single PSF is shown in Figure 2.

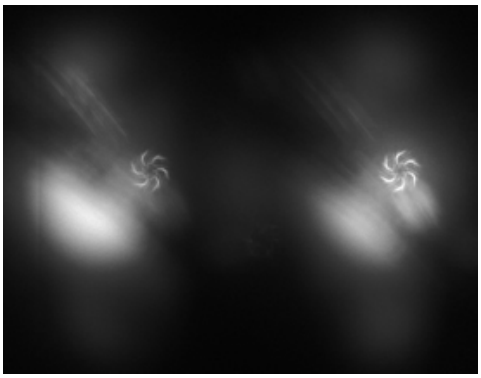


Figure 3: Blob Domain

A collection of PSFs ('blob' domain) is shown in Figure 3, demonstrating the native output of the LSS sensor. For room occupancy applications, Rambus uses multiple apertures on the sensor. For example, Figure 3, which was captured using the POD 2.0 LSS demonstration system, employs two apertures. Figure 4 is a focused image (taken with a mobile phone) of the scene the LSS sensor captured in Figure 3.

While the blob data from Figure 3 may appear to be a meaningless light pattern, it is in fact all the light from the scene captured through the LSS grating. Using custom-designed sensing algorithms (a visualization is provided in Figure 5, though not of the same scene), LSS is capable of detecting and isolating motion within specific areas of the FOV and identifying the number of occupants and their locations. This is accomplished without ever forming a human-recognizable image anywhere in the processing chain.

Figure 4: Native Scene

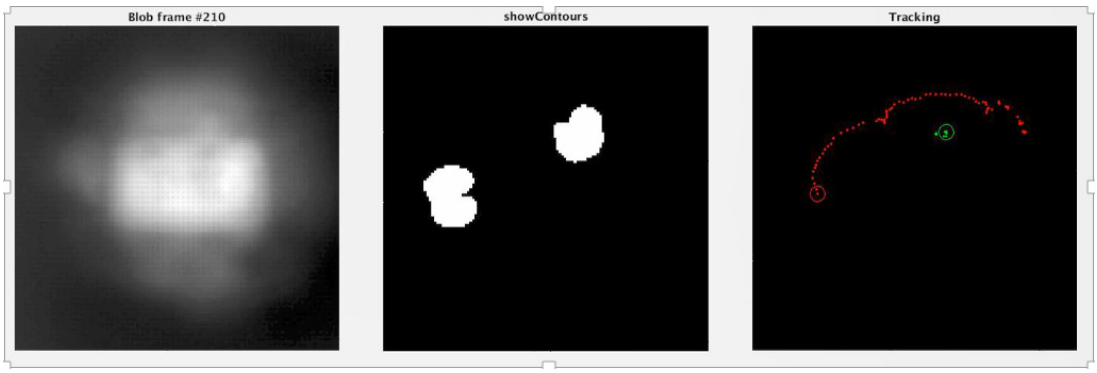


Figure 5: Room Occupancy Algorithm Visualization

Clearly, lensless smart sensors address the real-world privacy issues that focused and defocused cameras are burdened with. LSS technology captures scenes at very low resolutions, sometime as low as 320 x 320 pixels. Although methods do exist to (somewhat) reconstruct images from native LSS blob data, the quality of the reconstruction is far below that of even the lowest quality focusing camera. Additionally, the reverse engineering effort would be substantial and rely heavily on source LSS design data which Rambus does not publicly disclose. Perhaps most importantly, all processing can and should be executed at the local sensor level, with blob data never outputted or saved. These steps further reduce the level of privacy risks, making LSS a viable solution that can be deployed in both public and private smart buildings.

Conclusion

While many existing room occupancy solutions are readily available, there are few that truly address the evolving needs of building engineers for next-generation occupancy sensing. For buildings and homes to become 'smarter' and more adaptive, new sensing technology must be capable of detecting, counting and tracking occupants regardless of motion. Although focused cameras may adequately address sensing requirements, they also present a range of legal, privacy and hacking risks. These legal and technical issues, coupled with public distrust of lenses, will likely result in a limited deployment of focused cameras for room occupancy sensing tasks in offices and residences. While defocused cameras offer certain limited advantages over their focused counterparts, images produced by such devices may be easily refocused. In contrast, Rambus' lensless smart sensor technology reduces occupancy sensing privacy concerns by capturing the raw data of a scene with a diffractive grating, rather than a recognizable image with a lens. This unique ability makes LSS an ideal choice for widespread deployment in smart buildings.

© Rambus Inc. 1050 Enterprise Way, Suite 700
Sunnyvale, CA 94089 • rambus.com