Radiance: A Multispectral Imaging based Automatic Surveillance System
(Technical Topic)

Ethical Concerns Surrounding the Widespread Collection and Use of Biometric Data
(STS Topic)

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By
Minsol Kim

November 3, 2023

Technical Team Members:
Kouske Tapia
Ethan Cha
Joshua Yu
Kiki Wong

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Prof. Pedro Augusto P. Francisco, Department of Engineering and Society

Adam Barnes, Department of Electrical and Computer Engineering

Introduction

In an era where security is of paramount importance for individuals and institutions alike, the development of advanced security systems leveraging cutting-edge technologies has become increasingly vital. This necessity spans a broad spectrum, ranging from protecting livestock from wildlife to securing sensitive government facilities against espionage or terrorist threats. The technical challenge here lies in developing a security system that is robust and versatile enough to function effectively under various environmental conditions such as extreme weather, varying light conditions, and against attempts at camouflage.

Modern security systems largely rely on cameras that capture images using visible light, frequently supplemented with motion-activated lights for low-light operation, or employ short-wavelength infrared cameras, to record footage. This footage then requires either real-time or retrospective examination by a person to identify any incidents that warrant further investigation.

Radiance is an automatic surveillance system that employs multispectral imaging to capture data across various segments of the electromagnetic spectrum. This approach offers a much more detailed and comprehensive perspective compared to traditional imaging methods, often revealing information normally invisible to the naked eye (Yuen & Richardson, 2010). Furthermore, the system autonomously processes this information and notifies the user of any potential threats, eliminating the need for continuous monitoring.

As surveillance technology continues innovate and advance, the sociotechnical concerns regarding the ethical collection and use of biometric data within these systems grow as well. On one hand, these systems represent a significant leap in the technical capabilities of surveillance and security, offering enhanced detection and analysis that transcend the limitations of traditional methods. On the other hand, however, the integration of biometric data into security systems, a rising trend in the field, presents complex sociotechnical concerns, particularly in terms of personal privacy infringement and the potential for misuse of sensitive data (Ritchie et al., 2021).

This intersection highlights a critical aspect of technological advancement: the necessity to consider not only the efficiency and capabilities of new systems but also their societal and ethical implications. Especially in sensitive areas like security, technological innovation must be accompanied by a responsible and ethical approach to data management and privacy concerns.

This prospectus will explore the implications of the widespread collection and use of biometric data, beginning with an analysis of a system that capitalizes on the benefits of this cutting-edge technology, followed by an examination of the ethical considerations associated with its use.

Radiance – Automatic Surveillance using Multispectral Imaging

Traditional security systems, which often rely on standard cameras and sensors, face limitations in environments with poor lighting, adverse weather conditions, or against camouflage techniques (Lin et al., 2023). The integration of multispectral imaging technology offers a promising solution to these averse conditions. This section delves into the technical aspects of Radiance, an automatic surveillance system leveraging multispectral imaging.

Multispectral imaging is a technology that captures image data at various regions across the electromagnetic spectrum(Coffey, 2012).. Radiance specificly employs cameras capturing frames in visible light, short wavelength infrared (also known as night vision), and long wavelength infrared (also known as thermal). This combination enables the system to detect intruders or anomalies by analyzing a broader range of wavelengths, making it possible to identify threats that would otherwise go unnoticed with standard imaging (Zaman, Jensen, & McKee, 2011).

Another notable limitation of traditional security systems is their reliance on continuous human monitoring for real-time threat detection. Often, the responsibility falls on one or two individuals who must oversee numerous camera feeds simultaneously, most of which display uneventful scenes for extended periods of time. This monotonous task can lead to fatigue, significantly increasing the likelihood of errors in threat identification and response.

In scenarios where real-time monitoring is not critical, incidents still require manual review of hours of footage, which is both time-consuming and labor-intensive. While some systems have adopted motion-activated cameras that record only when activity is detected, these often utilize passive infrared (PIR) sensors, which are relatively unreliable. This makes the system susceptible to missing crucial events, defeating the entire purpose of it being there in the first place.

Radiance addresses this issue by utilizing an automatic threat detection and alert system. When a heat signature is detected in the designated perimeter, the user receives a notification from the system. Furthermore, the system continuously tracks and illuminates the object with a spotlight, enabling users to engage with the target, even in low light conditions. The user also has the ability to remotely monitor the processed camera feed, which has bounding boxes around any detected targets, allowing them to easily assess threats without being physically present at the scene.

The object detection and tracking is achieved by first analyzing the thermal feed. This process starts by converting the image to grayscale then identifying pixels with an intensity surpassing a predefined threshold. These highlighted pixels represent heat, and the threshold can be adjusted to detect objects exceeding a specific temperature. The outcome is a binary image with only black and white pixels, where white denotes pixels were above the threshold, and black signifies those were not. Subsequently, these white areas are expanded into larger blobs through a process known as dilation. This is a crucial step to enhancing the accuracy of the algorithm due to the nonhomogeneous nature of internal body temperature in living things, where extremities are often cooler than the head or abdomen. Employing this dilation step allows the threshold to be set much higher while still allowing the system to detect the entire object. These blobs are then contoured and located. This information is used to draw bounding boxes onto the original frame in the appropriate locations. If multiple heat signatures are detected within the field of view, the system will track the first one detected until it is lost. The user also has the option to manually select which object is tracked.

Several additional image processing techniques are used to improve the detection algorithm as well as enhance the user experience. Multiple iterations of gaussian blurring filter out any noise from the thermal camera. Additionally, before the feed is displayed to the user, the resolution is scaled up from 256x192 to 1920x1440 through linear interpolation.

Upon locating an object, the corresponding pixels from the visible and night vision feeds are analyzed by an object identification neural network. This helps determine whether the detected object is a human, animal, or an inanimate, heat-emitting object, providing the user with more detailed information.

The system is remotely accessible via a web server hosted on the device itself. The user can view camera feeds, switch the tracking target (if multiple objects are detected), and manually activate the spotlight to illuminate any area within the field of view. Past footage stored locally on the system is also accessible through this server.

The physical system consists of a visible light camera, night vision camera, and thermal camera. Image processing is handled by a Raspberry Pi and the system's movement is controlled by NEMA 17 stepper motors. The spotlight is a standard 1000 lumen LED array with a focusing lens to concentrate the beam.

The cameras feed data to the Raspberry Pi, which processes the frames in real-time and hosts the web server. When an object is detected, the motors reorient the system to center the object in the frame, subsequently activating the spotlight for illumination. The system continuously adjusts its orientation to keep the object centered as it moves until it exits the user-defined perimeter. The system operates on a standard 120V AC outlet and includes an optional backup battery in case of power failure.

Ethical Considerations Surrounding the Widespread Collection and Use of Biometric Data

As a result of its accuracy and efficiency, biometric data has become a cornerstone in countless sectors, ranging from security systems to consumer electronics to medicine (Jameel et al., 2020). However, this increasing prevalence raises substantial concerns. Privacy issues emerge as a major concern, given the intrusive potential of biometric surveillance. The security of biometric databases is another critical issue, as breaches could lead to irreversible data compromises. Ethical dilemmas also surface, particularly concerning potential discrimination and human rights violations stemming from biometric data misuse. Moreover, the normalization of biometric-based surveillance can significantly shift societal norms and affect individual behaviors and freedoms (Katsanis et al., 2021).

Finding the balance between security and individual privacy is a critical area of inquiry. This section will explore the ethical concerns surrounding the widespread collection and use of biometric data in security systems in addition to potential measures for mitigating the negative impacts of this technology.

Analysis of these issues begins with the exploration of previously implemented technologies that also grappled with handling similarly sensitive data. Notable among these are satellite imagery and GPS technology, both of which have raised significant privacy concerns (Iqbal & Lim, 2010).

Satellite imagery, for instance, has evolved to a point where it's possible to identify individuals from images, especially when supplemented with additional data (Coffer, 2020). This advancement has led to privacy concerns, prompting regulatory actions. In response to these concerns, both the United States and the European Union have set limitations on the resolution of publicly available satellite imagery. Similarly, corporations like Google have faced legal challenges over privacy issues. As a result, Google Earth now implements measures like blurring faces and other identifiable information to safeguard individual privacy.

GPS technology presents another pertinent example. While it offers immense benefits to users, the data collected during operation has raised alarms regarding privacy and surveillance. The ability of governments and corporations to track individuals through GPS data enables them to model personal habits, target individuals with personalized advertising, and even influence insurance rates based on driving patterns (Iqbal & Lim, 2010).

The potential parallels with biometric data are extensive. If biometric data were to be collected and utilized in similar ways, the concerns extend beyond mere privacy breaches. There is also significant risk of socioeconomic discrimination, as this data could be used to profile individuals in various detrimental ways. This scenario underscores the need for stringent measures and ethical considerations in the collection and use of biometric data to prevent such adverse outcomes.

Gaining a precise understanding of how biometric data is collected and used is essential for a thorough analysis of related issues. An in-depth knowledge of the technological aspects, particularly how this data is stored and secured, along with a comprehensive review of legal frameworks applicable to technologies of similar sensitivity, will shed light on the prevailing state of data protection and privacy challenges. Moreover, examining public perception through surveys will provide critical insights into the societal stance and apprehensions about biometric data, which is instrumental in shaping more informed, effective policies and practices.

Effectively addressing the concerns surrounding biometric data will require a multi-faceted approach. This includes developing robust legal frameworks that ensure transparency and accountability in biometric data collection, use, and sharing. Ethical guidelines must be established, emphasizing respect for privacy and non-discrimination. Public awareness and education campaigns are vital for enhancing understanding of biometric technologies, their risks, and individual rights. Implementing advanced security measures will protect biometric data from unauthorized access and breaches. Finally, international cooperation is essential for establishing universal standards and best practices for biometric data handling.

Research indicates that the public's perception of a technology is greatly influenced by how transparently its extent of use is communicated (Ritchie et al., 2021). Through open discussions about the use of biometric data, the public becomes better informed and empowered to advocate for appropriate regulations and implementations. Such a balanced approach is crucial in maximizing the benefits of biometric technologies while minimizing its risks.

Conclusion

The adoption of biometric data across diverse sectors such as personal electronics, security, and medicine is accelerating rapidly. While this trend offers immense potential benefits, it also raises significant ethical concerns due to the sensitive nature of the data involved. The Radiance project has been developed as a robust, automated surveillance solution, showcasing the advantages of utilizing multispectral imaging and biometric data. This research delves into both the technical capabilities and ethical considerations of Radiance, thereby illuminating the wider implications of biometric data in contemporary technology.

Upon completion, the parallel exploration of Radiance's development and the ethical considerations of biometric data usage will collectively offer an in-depth perspective on the future trajectory of biometrically-enabled technologies. The Radiance initiative serves as a testament to the technical viability and benefits of multispectral imaging. Concurrently, the ethical inquiry underscores the societal implications and need for conscientious application of these technologies. This integrated approach is designed to inform and influence future advancements in technology, striving to harmonize the advantages of cutting-edge technological innovations with a strong commitment to ethical standards.

References:

Yuen, P. W., & Richardson, M. (2010). An introduction to hyperspectral imaging and its application for security, Surveillance and Target Acquisition. *The Imaging Science Journal*, *58*(5), 241–253. https://doi.org/10.1179/174313110x12771950995716

Coffer, M. M. (2020). Balancing privacy rights and the production of high-quality satellite imagery. *Environmental Science &amp; Technology*, *54*(11), 6453–6455. https://doi.org/10.1021/acs.est.0c02365

Zaman, B., Jensen, A. M., & McKee, M. (2011). Use of high-resolution multispectral imagery acquired with an autonomous unmanned aerial vehicle to quantify the spread of an invasive wetlands species. *2011 IEEE International Geoscience and Remote Sensing Symposium*. https://doi.org/10.1109/igarss.2011.6049252

Coffey, V. C. (2012). Multispectral imaging moves into the mainstream. *Optics and Photonics News*, *23*(4), 18. https://doi.org/10.1364/opn.23.4.000018

Ritchie, K. L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., Kramer, R. S., Edmond, G., Martire, K. A., San Roque, M., & White, D. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PLOS ONE*, *16*(10). https://doi.org/10.1371/journal.pone.0258241

Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J., Lee, M. K., Anderton, J., Weinberg, S. M., & Wagner, J. K. (2021). A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PLOS ONE*, *16*(10). https://doi.org/10.1371/journal.pone.0257923

Jameel, S. M., Rehman Gilal, A., Hussain Rizvi, S. S., Rehman, M., & Hashmani, M. A. (2020). Practical implications and challenges of multispectral image analysis. *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. https://doi.org/10.1109/icomet48670.2020.9073821

Lin, Y., Peng, X., Yu, J., Chen, W., Wu, Y., & Liu, H. (2023). Real-time UAV localization and tracking in multi-weather conditions using multispectral image analysis*. *2023 IEEE International Conference on Real-Time Computing and Robotics (RCAR)*. https://doi.org/10.1109/rcar58764.2023.10249284

Demars, C. D., Roggemann, M. C., & Havens, T. C. (2015). Multispectral detection and tracking of multiple moving targets in cluttered urban environments. *Optical Engineering*, *54*(12), 1. https://doi.org/10.1117/1.oe.54.12.123106

Iqbal, M., & Lim, S. (2010). Privacy implications of automated GPS tracking and profiling. *IEEE Technology and Society Magazine*, *29*(2), 39–46. https://doi.org/10.1109/mts.2010.937031