IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 May 2025, accepted 8 July 2025, date of publication 14 July 2025, date of current version 18 July 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3588593

PERSPECTIVE

The Looming Privacy Challenges Posed by Commercial Satellite Imaging: Remedies and Research Directions

NATHANAËL DENIS AND ROBERTO DI PIETRO, (Fellow, IEEE)
King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia

Corresponding author: Nathanaël Denis (nathanael.denis@kaust.edu.sa)

This work was supported by the King Abdullah University of Science and Technology (KAUST) - Center of Excellence for Generative AI, under Grant 5940.

ABSTRACT As commercial satellites proliferate and data-capture technologies become more diverse, accessible, and high-resolution, new privacy concerns emerge. Additionally, emerging trends such as direct-to-consumer image sales and AI-enhanced computer vision strongly impact the satellite imaging industry. While these technologies benefit applications such as natural disaster monitoring and precision agriculture, they also introduce novel privacy risks. This perspective paper provides several contributions: we start by analyzing privacy risks using the LINDDUN privacy framework, categorizing threats like linking, identification, and data disclosure. Moving on from these findings, we introduce and discuss a few mitigation strategies, including inpainting and access control. Finally, we highlight some research directions to address these emerging challenges. Overall, this work characterizes the major issues in the evolving privacy landscape of satellite imaging, provides actionable solutions to mitigate these privacy risks, and highlights future research directions, positioning itself as a reference for researchers, policymakers, and industry stakeholders.

INDEX TERMS Privacy, satellite imaging, remote sensing, SAR imagery, inpainting, access control.

I. INTRODUCTION

Satellite imagery has become a vital tool for addressing global challenges. For instance, environmental organizations now routinely use commercial satellite data to monitor deforestation in remote regions like the Amazon rainforest [1]. With high-resolution, frequently updated images, these groups can detect illegal logging activities in near real-time, enabling faster interventions and greater transparency. This illustrates the benefits of space-based imaging in fields such as environmental protection, natural disaster response, and pollution tracking. However, the same capabilities have become a growing privacy concern, especially when such technologies are employed by non-state actors or deployed for surveillance without consent [2], [3]. As the quality and resolution of satellite-sensed data continue to increase, and the cost of accessing and deploying these technologies lowers, the private sector is taking a relevant role in the space domain, a sector that has been the secluded playground of military entities or military-backed corporations until recently [4]. Indeed, since the 1990s, many governments have allowed commercial satellite companies to market satellite-harvested data to both governmental and non-governmental clients. However, while relaxing the controls over satellite technology has undoubtedly accelerated innovation, and making satellite-provided data a commodity has created brand new markets, novel risks have been generated as well. In particular, in this contribution, we will focus on the privacy risks posed by commercial-grade satellite technology.

Although satellite imaging platforms like Google Earth are common, direct-to-consumer commercial satellite imaging raises distinct privacy and security concerns as it provides unaltered images on demand and has a higher imaging frequency. In Google Earth, the time between two images of the same spot is relatively reduced. Commercial firms can now collect images of any location multiple times a day, sometimes based on customer requests [5].

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

© 2025 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

Traditional optical imaging, which is commonly employed in applications such as Google Maps, has inherent limitations that indirectly preserve privacy. Notably, this depends on sufficient daylight, rendering it ineffective at night. However, commercial companies are now offering alternative forms of imaging that potentially introduce new privacy concerns. These include thermal imaging, synthetic aperture radar (SAR), and off-nadir imaging, each of which can capture data under conditions where traditional optical methods fail. These imaging techniques, as well as their increasing resolution, are gradually creating new privacy risks for individuals and companies. While privacy concerns of satellites and remote sensing are well-studied in the literature, the privacy risks associated with the diversity of imaging techniques provided by commercial satellites are still a relatively unexplored segment.

In addition to privacy concerns, the increasing use of commercial satellites raises significant cybersecurity issues [6]. Satellites are vulnerable to hacking and cyberattacks, which can lead to data leaks and unauthorized access to sensitive information. For instance, in 2018, a group of Chinese hackers reportedly targeted satellite operators and defense contractors in the United States, stealing sensitive data and compromising satellite communications [7]. Such incidents highlight the potential for cyberattacks to disrupt satellite operations and compromise the security of the data they collect.

A. CONTRIBUTIONS

Given the aforementioned problem, in the sequel to this perspective paper, we provide the following contributions:

- We highlight the evolution of remote sensing, imaging satellites, and how it brings privacy issues up to date;
- Following the LINDDUN framework, we identify several families of privacy threats raised by imaging satellites;
- We assess different mitigation strategies for the introduced threats and discuss their current limitations; and,
- We provide future research directions to address the forthcoming issues regarding privacy-sensitive satellite images.

B. OUTLINE

This paper is structured as follows: Section II provides an overview of satellite imaging technologies, highlighting the advancements beyond traditional optical imaging, including thermal and synthetic-aperture radar (SAR) imaging. Section III applies the LINDDUN privacy threat modeling framework to identify and analyze the key privacy risks introduced by modern satellite imaging. Section IV discusses potential countermeasures, including technical solutions such as inpainting and access control, as well as non-technical approaches to mitigating privacy threats. Section V presents a broader discussion of the limitations of current mitigation strategies, future privacy risks, and emerging trends in satellite imaging. Section VI concludes the paper by summarizing key findings and outlining directions for future research on privacy-preserving satellite imaging.

II. SATELLITE DATA CAPTURE: BEYOND OPTICAL

Commercial satellite imaging companies now have very diverse and advanced instrumentation and tend to individually specialize in a specific imaging technique for both practical and marketing purposes. In addition to the classic optical capabilities, high-resolution imaging is now possible in *thermal infrared* and *radar* imaging. Thermal infrared imaging captures the thermal radiation emitted by objects on the Earth's surface. Unlike optical imaging, which relies on reflected sunlight, thermal infrared imaging uses the infrared part of the electromagnetic spectrum to detect the heat emitted by objects, allowing it to operate day or night and under all weather conditions. Thermal imaging is therefore useful for use cases such as monitoring temperature changes and discrepancies, e.g., wildfire detection or urban heat island analysis. However, due to longer wavelengths, thermal imaging can not compete with optical imaging in terms of spatial resolution.

A. RADAR IMAGING

Radar imaging satellites use radio waves to capture images. They can penetrate clouds and work at night, making them ideal candidates for weather monitoring and mapping terrain under all conditions. In particular, synthetic aperture radar (SAR) takes advantage of the satellite's motion to synthesize a much larger radar antenna, or ''aperture'', than what is physically possible with a single, stationary antenna. This synthetic enlargement dramatically improves image resolution, allowing SAR to produce detailed pictures of the Earth's surface even through darkness or dense cloud cover [8].

Unlike optical cameras, which rely on sunlight, SAR actively emits microwave pulses and measures their reflections. As the satellite moves along its orbit, it collects multiple radar echoes from the same target at slightly different angles. By combining these echoes through advanced signal processing, SAR effectively mimics a giant antenna hundreds of meters long, far larger than any real antenna. The longer this synthetic antenna, the finer the details visible in the resulting image [9]. Figure 1 illustrates the basic principles of Synthetic Aperture Radar (SAR) imaging. A satellite flying at an altitude h emits radar pulses toward the Earth's surface at an incidence angle θ. As it moves forward along the nadir track, it continuously illuminates the ground, synthesizing a large antenna aperture. The motion direction defines the azimuth axis, while the perpendicular direction on the ground is referred to as the ground range. The red imaged area represents the radar's resolution cell, which lies within a larger swath illuminated during data acquisition. Additionally, SAR can detect not only the intensity of reflected signals but also their phases, enabling applications such terrain elevation mapping and subtle ground movement

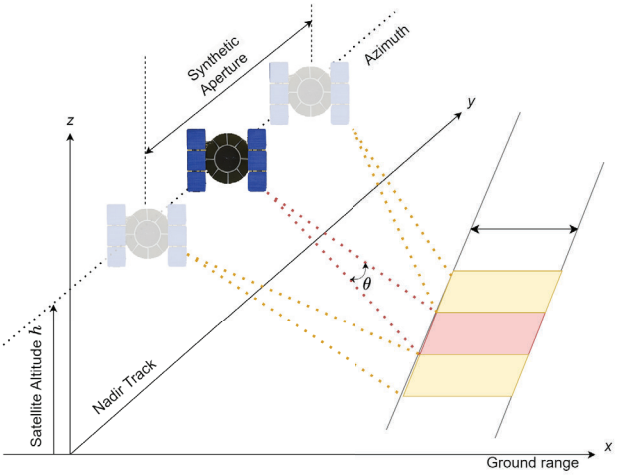


FIGURE 1. Illustration of Synthetic Aperture Radar (SAR) imaging geometry. The satellite moves along its nadir track and emits successive radar pulses at an angleθ relative to the ground. The satellite's movement synthesizes a long virtual antenna, i.e., synthetic aperture, enhancing resolution in the azimuth direction.

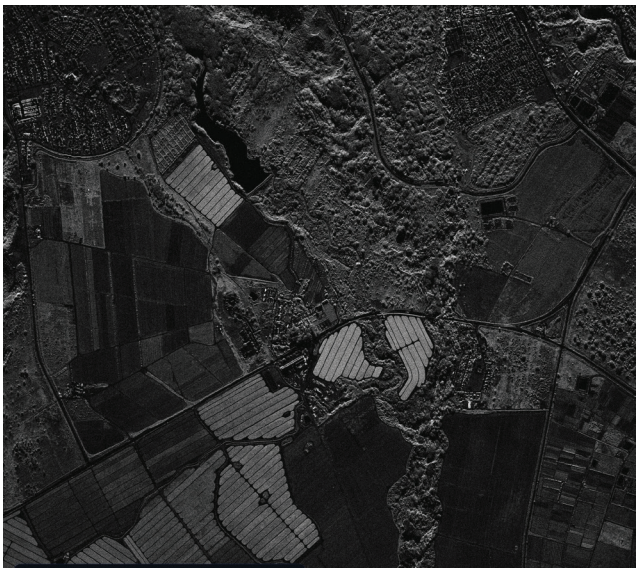


FIGURE 2. 16-cm resolution Synthetic Aperture Radar (SAR) image from Umbra Space commercial satellite company (Creative Commons). SAR satellites operate day and night and are weather-independent.

detection, including sinking cities or shifting glaciers [10], [11], [12]. Figure 2 shows a 16-cm resolution SAR image, demonstrating the technology's ability to resolve fine details and its unique advantage of all-weather, day-and-night operability.

B. SATELLITE IMAGING RESOLUTION

Two main metrics are used to assess the quality of the data captured by imaging satellites: *spatial* and *temporal* resolution. Spatial resolution refers to the size of one pixel when reported to the ground. For example, a spatial resolution of 1 meter means that one pixel on the image corresponds to a square of 1 by 1 meter on the ground. As a consequence, a finer resolution means one can see more accurate details in the images. Temporal resolution is defined as the amount of time needed to revisit and acquire data for the exact same location [13]. High temporal resolution is critical for monitoring and detecting temporally-dependent patterns of events on the ground, such as traffic and environment monitoring [14], [15]. Historically, there has been a trade-off between the spatial and the temporal resolution of satellite images. In other words, as the resolution of images increases, the frequency at which they are captured proportionately decreases [13], [16].

Observation satellites have come a long way in terms of imaging resolution. On 15 April 1999, Landsat 7 was launched as part of the first space-based Earth observation program intended for civilian purposes. Landsat 7 has a spatial resolution of 15 meters and may acquire between 440 and 500 images per day [17]. Twenty years later, commercial satellites can now capture optical images with a resolution as fine as 15 centimeters [5]. Thermal satellite imaging resolution has been improving as well to 3.5m (Satvu), which is still modest compared to the optical capacities in terms of resolution. SAR imaging can achieve a resolution down to 16cm (Umbra), which used to be reserved for the government by the US law and is now open to commercial use. Figure 3 depicts the evolution of spatial resolution of commercial satellites, including expectations for the near future.

The temporal resolution of a satellite constellation changes significantly depending on the instruments, altitude, swath, and spatial resolution of its satellites. It can vary from 30 seconds to one hour for NASA's satellites in geostationary orbit, i.e., where the satellite appears in a fixed position from a ground observer. NASA's Multi-angle Imaging SpectroRadiometer (MISR), which takes pictures with nine different angles and four wavelengths, has a temporal resolution of six to eight days [18]. Commercial satellite constellations such as Maxar's constellation can provide daily revisits for a spatial resolution of 50 cm. Maxar's constellation operates in low Earth orbit. LEO satellites offer expansive coverage and resiliency, both for communication and sensing purposes [19].

Temporal resolution is a major privacy concern, because frequent revisits make detecting patterns easier, e.g., inferring the occupancy hours of a house from car observation with hourly revisits. Figure 4 illustrates the evolution of the temporal resolution of imaging satellites, defined as the estimated time between consecutive passes. This interval can vary significantly depending on the region of interest and may also fluctuate for the same location over time.

III. UNVEILING REMOTE SENSING PRIVACY THREATS

Considering the diversity of technologies and inference risks, satellite imaging privacy requires a fine-grained and exhaustive analysis. LINDDUN is a privacy threat modeling framework, developed by privacy researchers at KU Leuven. We will use this framework to provide a complete analysis

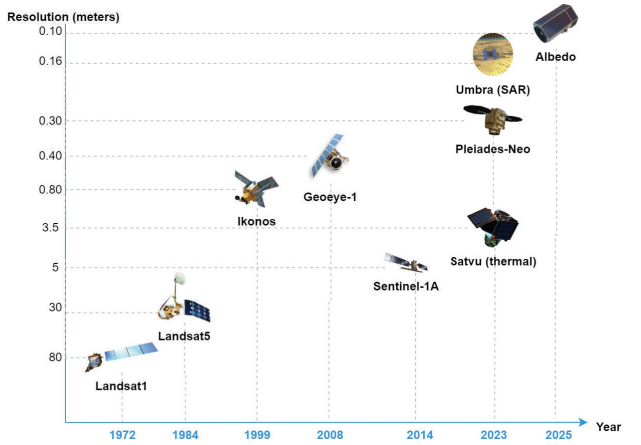


FIGURE 3. Evolution of the spatial resolution of remote sensing satellites. Resolution is given in meters and reflects the capacities of either radar or optical imagery if the payload includes both. The scale is arbitrary, and the resolution does not grow linearly.

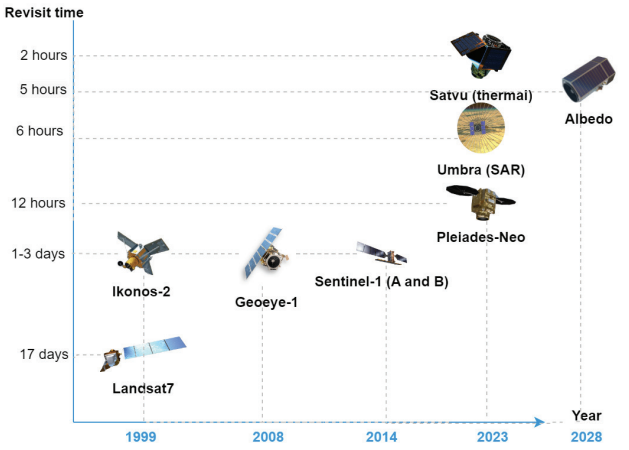


FIGURE 4. Evolution of the temporal resolution of remote sensing satellites. Resolution is given as the (estimated) time between revisits, in days or hours. Revisit time is correlated to the number of satellites in a constellation as well as the area considered for revisit. Scale is arbitrary.

of the satellite imaging privacy risks, as well as to derive insights.

A. LINKABILITY

Linkability is the possibility for an adversary to identify links between actions or different individuals. Rarely a threat when it is considered alone, it becomes an issue when combined with other privacy threats, such as identification. An example of a linking threat with satellite imaging is to link an individual with his or her car, and then monitor his or her movements. Li et al. [20] developed a vehicle detection and tracking solution for satellite videos, effectively enabling the real-time monitoring of vehicles using low-orbiting video satellites. Similarly, ships can be linked to specific behaviors through the analysis of satellite imagery. Even when vessels anonymize or spoof their Automatic Identification System (AIS) broadcasts, adversaries can use optical or SAR satellite data to correlate movement patterns and physical characteristics, linking vessels (objects) to activities such as illegal fishing or smuggling (actions) [21].

B. IDENTIFICATION

To identify individuals without any need for inference, facial recognition is the most natural technique that an adversary would consider. However, facial recognition faces several challenges that make it improbable with current commercial satellite capabilities.

For accurate identification using images, between 40 and 80 pixels per face are required under challenging conditions. This corresponds to a spatial resolution of at least 2.5 pixels per cm [22], implying that the satellite must achieve a millimetric resolution. Achieving such a fine resolution is constrained by fundamental physical limits, particularly those related to the wavelength of the light and the aperture size of the imaging system. Specifically, Dawe's limit, which determines the angular resolution θ of a telescope based on its aperture D (in cm) is given by:

$$\theta = \frac{11.6}{D} \tag{1}$$

Using Eq. 1, we can estimate the minimum aperture size required for a satellite to resolve features with the required precision for facial recognition. The required aperture size would be extraordinarily large, far exceeding what currently exists for commercial satellites, especially in very low Earth orbit (VLEO). With 40 pixels, a human face of 20cm wide (5 mm resolution), and a very low Earth orbit at 200 km as parameters, the resulting angular resolution is (Eq. 2, 3 and 4):

$$\theta_{\text{arcsec}} = \left(\frac{\text{size of the object}}{\text{distance from the object}}\right) \times \frac{180 \times 3600}{\pi} \tag{2}$$

$$\theta_{\text{arcsec}} = \left(\frac{0.005}{200000}\right) \times \frac{180 \times 3600}{\pi} \tag{3}$$

$$\theta_{\text{arcsec}} \approx 0.00515662\ arc \tag{4}$$

Dawe's limit (Eq. 5):

$$D = \frac{11.6}{\theta_{\text{arcsec}}} \approx 22.5\ m \tag{5}$$

indicates that a 22.5-meter diameter telescope would be required in a very low Earth orbit. A satellite equipped with such a telescope would be much bigger, likely visible to the human eye at this altitude.

Moreover, the images obtained would likely be off-nadir, i.e., not directly beneath the satellite, reducing image quality and further complicating facial recognition. Additionally, due to the low temporal resolution of satellite imagery, the face must be oriented approximately towards the satellite at the time of capture, which is highly unpredictable. This combination of factors makes facial recognition via satellites highly unlikely, despite ongoing discussions in the literature [23].

C. NON-REPUDIATION

Non-repudiation is the ability to attribute a claim to an individual. This is considered beneficial from a security perspective (e.g., STRIDE model), as security administrators want to attribute malicious actions to the corresponding user. Yet, from a privacy perspective, it is relevant to consider the ability to repudiate claims, e.g., the claim one does not own a valuable car even if it can be true. Satellites can be used to attribute ownership to individuals, which might be valuable information for several actors [24]. For instance, insurance companies can use satellite imagery [25], [26] with a high temporal resolution to check if a customer has a garage and genuinely uses it to park his or her car, and then adjust the insurance premium accordingly.

D. DATA DISCLOSURE

Data disclosure is the sharing of personal data, but it also includes excessive data collection, storage, and processing.

Several current practices in satellite companies are troublesome when considering data disclosure. First, *direct-to-consumer* satellite image sales may represent a risk if privacy-sensitive images are forwarded to malicious actors without further control and image post-processing. Besides, emerging companies such as Skyfi or Arlula not only provide direct-to-consumer images but are also *distributors* for other partner companies. Multiplying the providers virtually increases the temporal resolution of a target by removing the need for the end user to fetch images from different providers.

Finally, diverse actors, both open-source and commercial, tend to accumulate images and constitute satellite image *archives*, often without any privacy-preserving mechanisms in place. The compounding storage of satellite images will be a problem if privacy-sensitive pictures start to be collected. Another major concern (especially for companies) regards law compliance, in particular, the EU-enforced GDPR's right to be forgotten—lack of compliance can result in fines up to 2% of a company's entire global turnover.

E. DETECTION

Detection is the possibility for an adversary to discriminate whether an item of interest exists or not, even without actually observing the item. A troublesome detection threat for satellite imagery is the possibility of spotting blurred areas. Without seeing the actual item of interest, the blurring hints towards a highly sensitive area. Cheng et al. [27] designed an automatic blur detection tool for optical images, spotting every possible area of interest with minimal omissions.

Thermal imagery can detect heat signatures from underground structures or facilities intended to be concealed, notably the heat emitted by air ventilation systems, without seeing the actual facility. SAR imaging satellites can be used for the same purpose, due to their ability to penetrate through the ground and detect buried structures [28].

F. UNAWARENESS AND UNINTERVENABILITY

In contrast to drones or UAVs that bear similar privacy threats with high-resolution satellite imaging, satellites are mostly undetectable to the human eye or low-tech detection means, which can be helpful against drones (e.g., acoustic, optics, etc) [5]. This exacerbates the related privacy risk, as people may take appropriate countermeasures when aware of drone surveillance while they cannot when confronted with satellite imaging [5]. Moreover, while a drone pilot is usually close when operating and takes the risk of being detected, a satellite company can not be detected until it releases the images [5]. Besides, the individuals are never involved in the processing of their data, and can not prevent the satellite company from taking pictures at any point. Companies may apply blur when asked by individuals or companies, such as Google Maps, for houses. As of now, it does not apply to satellite images, except for state-sponsored entities.

The use of non-optical imaging techniques even increases the threat of unawareness, as individuals may falsely believe that they cannot be observed at night, under trees, or in cloudy weather, which is not true for SAR and thermal imaging.

G. NON-COMPLIANCE

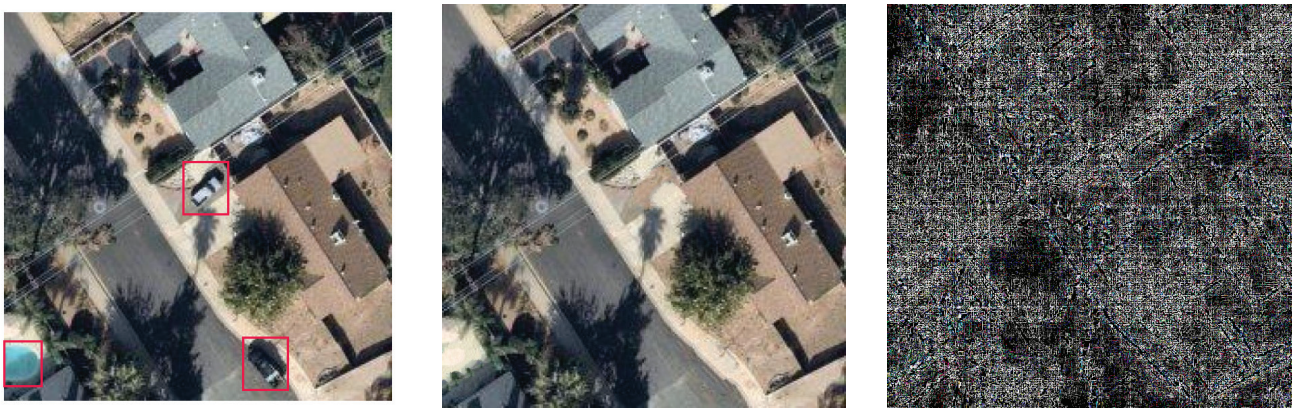
In contrast with privacy risks associated with satellite imaging, in particular non-optical, legal predicaments have been highlighted frequently [23]. Satellite imaging privacy regulations vary widely depending on the country considered. In the United States, privacy protection relies on self-regulation and sector-specific laws. The Fourth Amendment does not extend to aerial or satellite surveillance, and NOAA licensing controls commercial satellite operations, with ITAR restrictions limiting image exports [30], [31]. People's Republic of China, in contrast, enforces strict state control. The Personal Information Protection Law (PIPL) and Data Security Law (DSL) mandate data localization and restrict high-resolution imagery sharing [32], [33]. All satellite imaging is regulated by CNSA and the State Council. The EU's GDPR on data protection has triggered a series of legal challenges for commercial imaging. Among these non-exhaustive risks, GDPR's article 7 specifies rules regarding consent [34]. To comply with the law, the users' consent is required to process and store users' data, unless the data is anonymized, requiring proper identification of the privacy-sensitive data and proper mitigation tools to anonymize imagery. Neither topic has yet been addressed for very high-resolution imagery.

H. BEYOND LINDDUN

Along with specific privacy risks, satellite images face additional threats stemming from their medium, i.e., the satellite ecosystem, and the use of geospatial data with the satellite images.

1) SATELLITE COMMUNICATIONS

In addition to privacy risks proper to images and their dissemination, satellites face specific cybersecurity risks that



(a) Raw image with sensitive items highlighted. Source: Roboflow Open Source dataset [29]

(b) Inpainted image, the cars, and the swimming pool have been removed using Stable Diffusion.

(c) Noise level image. Inpainted areas can not be spotted with ease using noise.

FIGURE 5. High-resolution optical satellite image of a residential area and its derivatives: (a) raw image with sensitive items highlighted, (b) inpainted version with removed objects, and (c) corresponding noise level analysis.

increase the likelihood of privacy leaks. In particular, images have to be forwarded to the ground. Satellite communications (SATCOM) systems are gaining momentum, and in consequence, they are increasingly targeted by cyberattacks [35], [36], [37]. Yet, satcom systems remain vulnerable, due notably to the absence of universal cybersecurity standards [38]. Satcom systems are controlled from the ground and are designed to ease data transmission both for uplink and downlink, creating vulnerabilities [38], [39].

2) GEOSPATIAL DATA

Geospatial data is data about objects, events, or phenomena that have a location on the surface of the Earth [40]. In the context of satellite imaging, this includes not only the visual or radar-derived imagery itself but also embedded metadata such as GPS coordinates, timestamps, orbital parameters, sensor angles, and resolution metrics. When satellite images are combined with external datasets (e.g., cadastral maps, social media geotags), they can reveal sensitive information, such as property ownership, activity patterns, or infrastructural vulnerabilities. These risks are amplified by high spatial and temporal resolution. Sophisticated attacks based on geospatial and surveillance data have been carried out in the literature. Zhang et al. [41] designed a real-time reidentification model that identifies individuals across multiple surveillance cameras. Surveillance data were fused with geographic information and mapped onto a 3D geospatial model to track movement trajectories.

IV. COUNTERMEASURES AND LIMITATIONS

Mitigating the diverse privacy risks of commercial satellite imaging requires a mix of technical and regulatory measures. We will first introduce inpainting (Section IV-A) as a more obfuscated alternative to blurring. Then, we will discuss access control and usage control strategies to mitigate data disclosure (Section IV-B). Solutions to non-technical issues are provided in Section IV-C whereas Section IV-D introduces a technical solution to the detection threat. Section IV-E discusses the role of encryption for privacy preservation in the context of satellite images.

A. INPAINTING

One of the most common countermeasures adopted by satellite companies to mitigate privacy-related risks is blurring, used by Google Earth and Maps at the request of individuals. However, blurring is not a neutral technique. Indeed, blurring a specific area can draw attention to it, suggesting that it is likely hiding a sensitive location [42]. Privacy-preserving image processing calls for a more obfuscated way to hide sensitive information. Inpainting is a conservation process where damaged, deteriorated, or missing parts of an artwork are filled in to present a complete image [43]. AI-assisted modern inpainting can be used to fill an image where the sensitive data has been removed. Inpainting relies upon a mask to determine which regions of an image to fill in; the area to inpaint is represented by white pixels and the area to keep is represented by black pixels. Image inpainting has three main purposes, all of them with applications to satellite images: image restoration, image editing (object removal), and image coding and transmission [43]. The resulting image must be sufficiently realistic to avoid the attention of adversaries, as in the case of blurred images. If inpainting has been studied for decades [44], modern inpainting increasingly relies on generative AI and presents new challenges for detection [43].

1) SATELLITE IMAGE INPAINTING

Satellite image inpainting is an active field of research for both optical imagery and other types of images [45], [46], [47]. Cannas et al. developed an inpainting method for SAR images while preserving the landcover content [48]. In contrast with blurring, modifications are not obvious to

TABLE 1. Privacy threat types for satellite imaging and proposed mitigation.

Threat to privacy	Example	Mitigation
Linkability	Linking car with identified individual	Blur, Inpainting
Identification	Face recognition	Blur, Inpainting
Non-repudiation	Attribute swimming pool ownership to individual [24]	Inpainting
Detection	Blurred areas of interest	Inpainting
Data disclosure	Unmonitored direct-to-consumer sharing	Access control, Encryption
Unawareness & Unintervenability	Nighttime surveillance	Not technical
Non-compliance	Processing without consent	Not technical

an adversary, but the image utility can be reduced. However, whether machine learning techniques can detect such an intervention, and to what level of confidence, is an open research question.

2) CAR INPAINTING USE CASE

As an example, we designed a privacy-preserving inpainting tool to detect and remove cars automatically using machine learning, available at https://github.com/nathanael-denis/Satellite-car-privacy. In Figure 5, we use Stable Diffusion inpainting to remove privacy-sensitive items from satellite images. Swimming pools and cars are detected and then removed using inpainting. A diversity of actors have an interest in spotting cars with commercial satellite imagery, such as 1) insurance companies to verify claims regarding parking habits; 2) criminals for occupancy habits; and, 3) state-sponsored entities for law compliance. Inpainting is harder to notice than blurring [49] and also enables modification instead of simple deletion. Therefore, a car can be swapped with another item to maintain general scene cohesion when needed [50]. Inpainting can also be used to address *linking* by removing sensitive items of interest [51], *identification* by modifying faces, *non-repudiation* by removing items that can be associated with claims, such as swimming pools or cars, and *detection* by removing the items of interest.

3) INPAINTING CHALLENGES

Inpainting is an active area of research that still faces challenges during its implementation. Inpainting involves two major issues when applied to satellite images: 1) detectability; and, 2) scalability. To ensure efficient privacy-preservation, inpainting must not be detectable with lightweight methods. As inpainting is used for document forgery, the academic literature actively studies automatic inpainting detection, and in particular its impact from generative artificial intelligence [52], [53], [54], [55]. As of now, state-of-the-art detectors remain inefficient at detecting local manipulations performed by modern generative approaches [56]. While the possibility of detecting inpainting is widely mentioned in the literature, the possibility of scaling inpainting on large databases is an emerging topic of research. The possibility to inpaint large databases [57], high-resolution images [58], and to increase the speed of the inpainting process [59] is discussed in the machine learning field. Scaling to handle larger datasets or more complex architectures increases the demand for computational resources and limits the accessibility for researchers. Generating real-time or interactive inpainting applications remains a challenge [60]. Existing works apply inpainting to satellite images, notably for image restoration more than for privacy purposes [47], [61], [62]. These works focus on demonstrating the efficiency of the reconstruction, i.e., the inpainting generates relevant images, rather than the scalability of the process. The possibility to apply inpainting to large-scale, bulky satellite image datasets, jointly with other security methods such as encryption (cf. Section IV-E), remains to be demonstrated.

B. ACCESS AND USAGE CONTROL

Data disclosure can be mitigated by enforcing data access control and data flow control, to ensure the satellite images are delivered to legitimate users. Usage control can also be used to enforce the processing of satellite images according to the satellite company or the privacy-sensitive users' policies. The main limitation to access control and usage control is the difficulty of defining policies [63], i.e., which user should not access an image in a direct-to-consumer setup, and also to enforce them as a satellite company typically has limited technical means to prevent a malicious customer from processing an image, once the customer gets it. Access control and usage control require authentication from the user, which in the context of satellites introduces some challenges.

1) PHYSICAL-LAYER AUTHENTICATION

Traditional access control mechanisms rely primarily on cryptographic methods and digital authentication schemes, which are complex to implement in satellite settings. In the context of satellite communications and remote sensing, ensuring that only authorized entities can access or control sensitive imaging data is crucial. *Physical-Layer Authentication* (PLA) emerges as a promising technique by leveraging the physical characteristics of signals to verify the identity of transmitters [64], [65]. Integrating PLA into satellite access control frameworks enhances authentication robustness with unforgeable physical fingerprints, mitigating the risk of unauthorized access. Future research should explore machine

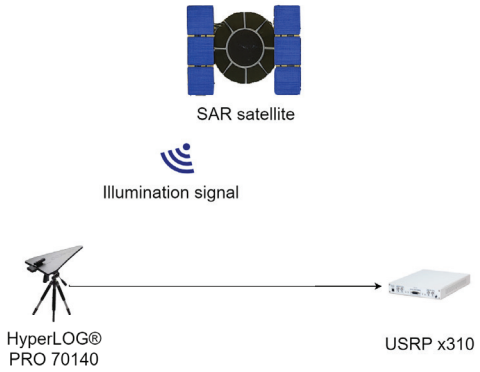


FIGURE 6. Setup for SAR illuminating signal collection. The USRP x310 software-defined radio is coupled to an Aaronia Hyperlog© antenna, collecting SAR signals in any commercial range.

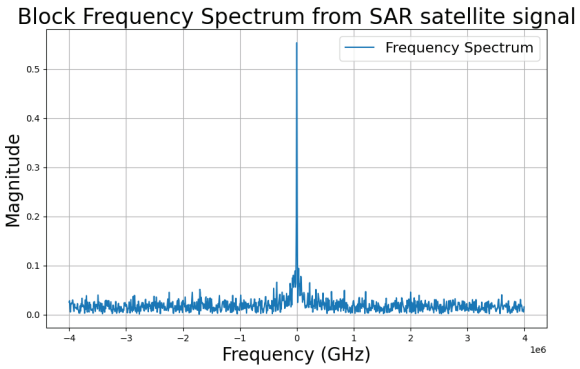


FIGURE 7. Frequency spectrum of a selected block of IQ samples from a SAR satellite signal capture, showing dominant frequency components and relative signal strength (Magnitude).

learning-driven PLA techniques well-tailored to imaging satellites, e.g., using the radar of the SAR satellites.

2) AUTHENTICATION SCHEMES

A significant number of emerging satellites operate in low Earth orbit, which presents specific constraints in terms of access control. The network typology is dynamic, the satellites are resource-constrained, and the latency can be significant [66]. Several solutions, well-tailored to LEO networks, are being investigated in the literature. Blockchains, because of their inherent decentralization aspects, are often considered for access control, as they may fit dynamic network topology more than centralized network architectures [66], [67], [68], [69]. Random access control protocols are emerging as a paradigm to manage network communications, especially for Internet of Things networks [70]. Random access protocols allow each device to transmit data over a shared resource without any pre-assigned resource or scheduled patterns [70]. These protocols handle situations where users may transmit data at random times, potentially leading to collisions and inefficient use of the shared resource. They are particularly used in IoT settings due to the importance of dynamic resource allocation [71], [72], [73]. Current limitations and future research directions include the cross-layer optimization [70], and include how to interoperate physical-layer approaches with random access control.

C. NON-TECHNICAL ISSUES

For satellite companies, *unawareness* translates into being able to inform individuals when sensitive data is being collected. If privacy-sensitive data are identified and the corresponding images are sold to a third party, the individual should be involved in the process to give his or her consent, at the very least at the beginning of the process.

Regarding non-compliance, companies should consider both legal and security best practices. This threat focuses on organizational and operational management and should be addressed at these levels [74]. Mitigating non-compliance typically requires penalty enforcement in employees' contracts and external audits, to ensure conformity with internal policies and regulations [74].

D. DETECTING AND JAMMING

Detecting when an optical or thermal satellite captures images of an area is not straightforward. Conversely, synthetic-aperture radars rely on electromagnetic waves in well-known frequency bands, the L-band (1.27 GHz), C-band (5.4 GHz), and X-band (9.6 GHz). It is therefore possible to detect a SAR satellite imaging an area, by monitoring these frequency ranges. To show that this is feasible, we used a general-purpose software-defined radio (SDR) USRP X310 and a Hyperlog©Pro 70140 antenna covering all the SAR bands (cf. Figure 6). SAR satellites emit strong, characteristic radar signals that are backscattered toward the emitting satellite. These signals can also be detected by a ground antenna and appear as spikes in the frequency spectrum (Figure 7). Detecting SAR illuminating signals is particularly relevant as countermeasures exist to interfere with the image capture, known as *jamming*.

Jamming disrupts the SAR signal by introducing noise or other signals into the radar's operational frequency, reducing image quality or rendering it unusable [81], [82]. This form of electronic warfare can hinder the satellite's ability to capture clear, high-resolution images, providing a method for obscuring sensitive areas from surveillance. However, jamming is typically beyond the capabilities of ordinary citizens, limiting this countermeasure to military or company purposes.

E. ENCRYPTION OF SATELLITE IMAGES

Encryption on board Earth observation satellites aims to secure the data transmitted to the ground station [83], or when being stored. Encryption is also the basis of secure authentication schemes [84]. Therefore, in addition to being an essential tool for security, it can address privacy-related threats. Notably, it mitigates the data disclosure threat by limiting the impact of hazardous data collection and sharing practices, while providing authentication protocols to prevent

TABLE 2. Overview of revisit frequency across Earth observation modalities and inferred data types relevant to privacy risks. Persistent revisit, even at coarse resolution, enables behavioral inference and time-series surveillance.

Imaging Type	Provider	Typical Revisit Time	Inferred Data
Optical	Maxar	1–3 days (orbit-dependent) [75]	Urban expansion, vegetation health, infrastructure growth
Synthetic Aperture Radar	ICEYE	Multiple times per day [76]	Vehicle routes, construction activity, land deformation [77], [78]
Thermal Infrared	SatVu	Daily in select areas [79]	Facility usage, industrial activity, energy consumption
Very High Resolution Optical	Albedo	5 hours (planned) [80]	Object tracking, movement patterns, site monitoring

unauthorized access. Assuming that attackers can not break encryption, it severely limits their ability to identify people, detect items of interest, and find links between them. This makes encryption a valuable tool for privacy preservation.

Image encryption for space-borne objects faces unique challenges. Standard data encryption algorithms, such as AES or RSA, are not scalable enough to encrypt bulky satellite image databases [83]. As a consequence, dedicated image encryption methods are being investigated in the literature. Chaotic encryption leverages the principles of chaos theory to create highly unpredictable and complex sequences. Chaotic maps have been used as an effective solution for image encryption due to their attractive features such as high sensitivity to initial conditions, unpredictability, pseudo-randomness, and ergodicity [85]. To this date, two main approaches are discussed in the existing literature: improving chaotic-based encryption schemes [83], [86], [87], [88] and chaotic-enhanced other encryption methods [89], [90], [91]. For instance, Dua et al. [91] used different chaotic maps in conjunction with DNA-inspired operations. DNA encoding further enhances image encryption security through its complexity and error correction capabilities.

Chaotic encryption is a powerful tool to curb the consequences of data leaks. While chaotic encryption is a promising avenue for efficient image protection, it alone has limited application to address the broader spectrum of privacy threats. Notably, encryption is effective only during transmission and storage phases, offering no protection once the image is decrypted and accessed by an authorized user — yet potentially malicious. As such, it does not mitigate inference risks, linking, or unawareness, nor does it fulfill regulatory demands. Therefore, chaotic encryption should be viewed as a component of a broader, multi-layered privacy strategy rather than a standalone remedy.

V. DISCUSSION

In the previous sections, we have highlighted a broad diversity of privacy risks related to the different satellite imaging techniques. In the following, we recap the key takeaways and the resulting future research directions.

A. INCREASED RESOLUTION AGAINST INCREASED IMAGING DIVERSITY

Due to physical limits, it is unlikely that the spatial resolution of commercial satellite images will increase the possibility of identifying individuals. More pressing privacy risks are related to the booming availability of cheap or free satellite images. The diversity of imaging techniques as well as an increased temporal resolution, enables anyone to infer data, especially when combined with other data sources. It is complex to forecast to what extent each technology can be used to acquire data on a target since the privacy threats are also use-case dependent, encompassed in general privacy threat families that have been highlighted using LINDDUN, which stands out as a relevant framework to address privacy issues.

B. THE ROLE OF MITIGATION AND GOOD SECURITY PRACTICES

To date, image modification mostly consists of blurring and the more recent inpainting enabled by generative AI progress. These solutions do not cover all privacy-threat families and have significant limits regarding their efficiency. Blurring can be detected easily, while inpainting is more unreliable and resource-consuming. Current trends in satellite image providers, e.g., direct-to-consumer sale archiving, require consideration for privacy best practices and privacy regulations such as the European GDPR.

C. FUTURE THREATS

As satellite imaging technology continues to evolve, emerging trends are introducing new privacy concerns and amplifying existing risks. Below, we introduce the impact of continuously increasing resolution and super-resolution imaging methods.

1) TIME AND SPATIAL RESOLUTION

Due to the currently high cost of satellite images, including the cheapest archival optical images, the threat of having a wide-scale use of satellite imagery for privacy violations from commercial companies and their customers is not immediate. However, there are several phenomena to consider that may drastically change this fact in the future. First, the spatial and temporal resolution of satellites is likely to keep improving in the future, and the cost of current resolution images to decrease. Second, satellite image archives may leak, as a result of negligence, malicious sharing, or cyberattacks, providing unintended (possibly malicious) users with plenty of insightful satellite images, potentially for free. Also, there is an unpredictable threshold both in spatial and temporal resolution, over which the privacy risks related to satellite imagery will go from moderate to critical. For

TABLE 3. Research gaps and directions for satellite privacy and security.

Topic	Research Gaps	Research Directions
Imagery Types	- Specific impact of imagery types on privacy risks. - Impact of temporal resolution	1) Investigate how different imagery types affect privacy exposure. 2) Develop targeted countermeasures based on imagery type, e.g., thermal image inpainting
Inpainting	- Detectability of inpainting. - Scalability across databases. - Potential privacy leaks after inpainting.	1) Develop detection or obfuscation methods for inpainting. 2) Improve scalability for large satellite image datasets. 3) Assess the possibility of reconstructing removed information.
Access Control	- Need for specific physical-layer authentication. - Need for dedicated protocols for satellites and IoT.	1) Apply PLA techniques to SAR and thermal satellites. 2) Optimize PLA and access control for LEO and IoT networks. 3) Design new, lightweight access control protocols for space communication.
Data Disclosure	- Risk of aggregation and inference attacks. - Geospatial data threats	1) Investigate the feasibility of cross-data inference attacks targeting satellite imagery.
Jamming	- Jamming can be mitigated by counter-jamming.	1) Develop AI-powered counter-jamming strategies for satellite communication systems.
Encryption	- Limitations of chaos-based encryption. - Need for computation over encrypted images. - Authentication challenges in LEO and IoT networks.	1) Improve chaotic encryption schemes for LEO satellites. 2) Design homomorphic encryption techniques enabling computation on encrypted images. 3) Develop authentication protocols adapted to LEO and IoT environments.
Super-Resolution	- Privacy risks and benefits of super-resolution.	1) Study the privacy impact of super-resolution imaging. 2) Evaluate super-resolution techniques for sensitive item detection or removal.
Non-Technical	- Lack of user awareness. - Non-compliance with regulations and best practices.	1) Develop technical and non-technical methods to identify users facing privacy risks and increase awareness. 2) Create automated auditing tools to identify privacy risks in satellite imagery.

instance, Albedo Space Corporation successfully launched a satellite, Clarity-1, with a stunning 10 cm optical resolution and 2 m thermal resolution for very low Earth orbit (VLEO) satellite(s) in March 2025, matching aerial imaging capabilities [92]. Albedo is also expected to reach 5 revisits per day with the full 24-satellite constellation.

2) SUPER-RESOLUTION IMAGING

The progress in machine learning and computer vision is disrupting the satellite imaging field and is the source of additional risks and potential benefits for privacy. As for blurring, good-quality automated tools for inpainting detection are likely to appear in the future [52], decreasing the quality of this mitigation technique. Another concern is the possibility of using generative models to artificially increase satellite image resolution, improving the current legal and technical limits of imaging satellites. Referred to as super-resolution (SR) imaging, it has become a popular research topic in remote sensing [93]. Current solutions focus on improving the quality of low-resolution imagery, but future work may focus on higher-resolution imagery with the help of aerial and UAV images [94], [95]. The use of UAV images to improve the quality of remote sensing data has already been explored in the literature. Matsui et al. [96] improved the resolution quality of Lake Hachiroko remote sensing data with UAV images. Both UAV and satellite images were input into a machine-learning model to improve the accuracy of water quality estimations. Malamiri et al. [97] used a combination of UAV and Landsat-8 images to classify farm density and separate pistachio cultivars from weeds. While super-resolution imaging is a source of concern for privacy, it has the potential to improve privacy-preserving processes. SR could be used for sensitive-feature spotting. SR can be used to enhance small patches (faces, plates) just enough to detect them reliably, then apply blurring at full resolution. Besides, the privacy-sensitive nature of SR methods has been identified, and the existing literature studied private-by-design SR methods, not limited to satellite images [98], [99].

D. RESEARCH DIRECTIONS

In this section, we now provide future research directions, stemming from the identified privacy threats (Section III), their mitigation and current limitations (Section IV) as well as how to address future threats (Section V-C). We classify research directions according to 1) their topic; and, 2) their research gap. These research directions are provided in Table 3. In addition, in the following, we introduce several future research directions also of interest.

Related to data disclosure, the possibility of carrying out inference attacks using satellite data crossed with external data should be investigated in the literature. An inference attack or channel is "the capability to infer sensitive data from non-sensitive. Another area of research is the possibility of encrypting images and performing selected computations over them while hiding privacy-sensitive components inside images [5]. For instance, legitimate applications could perform vehicle detection on satellite images, such as counting the number of cars for traffic monitoring, while malicious actors would not infer the occupancy habits for a given house. Homomorphic encryption is a promising solution for privacy-preserving processing on encrypted images [100], [101].

VI. CONCLUSION

In this paper, we have highlighted the emerging privacy concerns associated with the increasing accessibility and resolution of commercial satellite imaging, particularly with non-standard methods such as thermal and SAR imagery. Unlike traditional optical imaging, non-optical methods can capture data under a variety of conditions. We have analyzed these risks through the LINDDUN privacy framework, discussed possible remedies, and highlighted some research directions in the domain.

REFERENCES

[1] E. L. Bullock, C. E. Woodcock, C. Souza, and P. Olofsson, "Satellite-based estimates reveal widespread forest degradation in the Amazon," *Global Change Biol.*, vol. 26, no. 5, pp. 2956–2969, May 2020.

[2] H. Kannegieter, "Privacy and veracity implications of the use of satellite imagery from private companies as evidence in human rights investigations," *Harvard Hum. Rights J.*, Nov. 2023. Accessed: Apr. 2, 2024. [Online]. Available: https://journals.law.harvard.edu/hrj/2023/11/

[3] E. Stankeviciute. (2023). *Commercial Satellite Images: Crime Fighter or Privacy Issue?*. AeroTime. Accessed: Apr. 2, 2024. [Online]. Available: https://www.aerotime.aero/articles/privacy-concerns-when-using-satellite-imagery

[4] *The Space Economy in Figures: How Space Contributes To the Global Economy*, OECD, Paris, France, 2021, doi: 10.1787/c5996201-en.

[5] R. McAmis, M. Sim, M. Bennett, and T. Kohno, "Over fences and into yards: Privacy threats and concerns of commercial satellites," *Proc. Privacy Enhancing Technol.*, vol. 2024, no. 1, pp. 379–396, Jan. 2024.

[6] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Comput. Netw.*, vol. 216, Oct. 2022, Art. no. 109246.

[7] Reuters. (Jun. 2018). *China-based Hacking Campaign is Said To Have Breached Satellite, Defense Companies*. Accessed: Apr. 2, 2024. [Online]. Available: https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html

[8] A. Moreira, P. Prats-Iraola, M. Younis, G. Krieger, I. Hajnsek, and K. P. Papathanassiou, "A tutorial on synthetic aperture radar," *IEEE Geosci. Remote Sens. Mag. (Replaces Newslett.)*, vol. 1, no. 1, pp. 6–43, Mar. 2013.

[9] G. Franceschetti and R. Lanari, *Synthetic Aperture Radar Processing*. Boca Raton, FL, USA: CRC Press, 2018.

[10] T. Toutin and L. Gray, "State-of-the-art of elevation extraction from satellite SAR data," *ISPRS J. Photogramm. Remote Sens.*, vol. 55, no. 1, pp. 13–33, Feb. 2000.

[11] L. D. Euillades, P. A. Euillades, N. C. Riveros, M. H. Masiokas, L. Ruiz, P. Pitte, S. Elefante, F. Casu, and S. Balbarani, "Detection of glaciers displacement time-series using SAR," *Remote Sens. Environ.*, vol. 184, pp. 188–198, Oct. 2016.

[12] E. Chaussard, F. Amelung, H. Abidin, and S.-H. Hong, "Sinking cities in indonesia: ALOS PALSAR detects rapid subsidence due to groundwater and gas extraction," *Remote Sens. Environ.*, vol. 128, pp. 150–161, Jan. 2013.

[13] J. Théau, *Temporal Resolution*. Cham, Switzerland: Springer, 2015, doi: 10.1007/978-3-319-23519-6_1376-2.

[14] S. Ø. Larsen, H. Koren, and R. Solberg, "Traffic monitoring using very high resolution satellite imagery," *Photogrammetric Eng. Remote Sens.*, vol. 75, no. 7, pp. 859–869, Jul. 2009.

[15] N.-B. Chang, K. Bai, S. Imen, C.-F. Chen, and W. Gao, "Multisensor satellite image fusion and networking for all-weather environmental monitoring," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1341–1357, Jun. 2018.

[16] Y. Ö. Durgun, A. Gobin, G. Duveiller, and B. Tychon, "A study on trade-offs between spatial resolution and temporal sampling density for wheat yield estimation using both thermal and calendar time," *Int. J. Appl. Earth Observ. Geoinformation*, vol. 86, Apr. 2020, Art. no. 101988.

[17] U.S. Geological Surv. (2024). *Landsat 7 Data Users Handbook*. [Online]. Available: https://www.usgs.gov/media/files/landsat-7-data-users-handbook

[18] Y. Si, L. Chen, X. Xiong, S. Shi, L. Husi, and K. Cai, "Evaluation of the MISR fine resolution aerosol product using MODIS, MISR, and ground observations over China," *Atmos. Environ.*, vol. 223, Feb. 2020, Art. no. 117229.

[19] L. Toka, M. Konrad, A. Pekar, and G. Biczók, "Integrating the skies for 6G: Techno-economic considerations of LEO, HAPS, and UAV technologies," *IEEE Commun. Mag.*, vol. 62, no. 11, pp. 44–51, Nov. 2024.

[20] M. Li, D. Fan, Y. Dong, and D. Li, "Satellite video moving vehicle detection and tracking based on spatiotemporal characteristics," *Sensors*, vol. 23, no. 12, p. 5771, Jun. 2023, doi: 10.3390/s23125771.

[21] E. d'Afflisio, P. Braca, and P. Willett, "Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 4, pp. 2093–2108, Aug. 2021.

[22] Axis Commun. (2022). *Resolution: The Key to Identification and Recognition*. Accessed: Jun. 3, 2024. [Online]. Available: https://web.archive.org/web/20221129234413,https://www.axis.com/learning/web-articles/identification-and-recognition/resolution

[23] L. Rapp and C. Santos, "Satellite imagery, very high-resolution and processing-intensive image analysis: Potential risks under the GDPR," *Air Space Law*, vol. 44, no. 2, pp. 275–295, Jun. 2019.

[24] K. Willsher. (Aug. 2022). *French Tax Officials Use Ai to Spot 20,000 Undeclared Pools*. [Online]. Available: https://www.theguardian.com/world/2022aug/29/french-tax-officials-use-ai-to-spot-20000-undeclared-pools

[25] M. Thomas, E. Tellman, D. E. Osgood, B. DeVries, A. S. Islam, M. S. Steckler, M. Goodman, and M. Billah, "A framework to assess remote sensing algorithms for satellite-based flood index insurance," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 16, pp. 2589–2604, 2023.

[26] M. M. Islam, T. Ahamed, S. Matsushita, and R. Noguchi, "A damage-based crop insurance system for flash flooding: A satellite remote sensing and econometric approach," in *Remote Sensing Application II: A Climate Change Perspective in Agriculture*. Cham, Switzerland: Springer, 2024, pp. 121–163.

[27] C. Su, Z. Xu, F. Shen, and X. Zhang, "Automatic detection of blurred areas for remote sensing imagery," *IEEE Geosci. Remote Sens. Lett.*, vol. 20, pp. 1–5, 2023.

[28] M. González-Díaz, M. García-Fernández, Y. Álvarez-López, and F. Las-Heras, "Improvement of GPR SAR-based techniques for accurate detection and imaging of buried objects," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 6, pp. 3126–3138, Jun. 2020.

[29] A. Mutalib. (Aug. 2023). *Cars and Swimming Pool Dataset*. [Online]. Available: https://universe.roboflow.com/abdul-mutalib-wthjt/carsandswimmingpool

[30] Nat. Ocean. Atmos. Admin. (2024). *Commercial Remote Sensing Regulations*. Accessed: Feb. 2025. [Online]. Available: https://www.nesdis.noaa.gov/CRSRA

[31] U.S. Dept. State. (2024). *International Traffic in Arms Regulations (ITAR)*. Accessed: Feb. 2025. [Online]. Available: https://www.pmddtc.state.gov/ddtcpublic

[32] Standing Committee of the Nat. People's Congr. *Data Security Law of the People's Republic of China (DSL)*, Accessed: Feb. 2025. [Online]. Available: http://www.chinalawtranslate.com/en/data-security-law/

[33] Standing Committee Nat. People's Congr. (2021). *Personal Information Protection Law of the People's Republic of China (PIPL)*. Accessed: Feb. 2025. [Online]. Available: https://npcobserver.com/2021/08/20/chinas-personal-information-protection-law-pipl-finalized-translation/

[34] Eur. Parliament Council Eur. Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[35] F. Casaril and L. Galletta, "Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS," *Comput. Secur.*, vol. 140, May 2024, Art. no. 103799.

[36] A. Carlo and K. Obergfaell, "Cyber attacks on critical infrastructures and satellite communications," *Int. J. Crit. Infrastruct. Protection*, vol. 46, Sep. 2024, Art. no. 100701.

[37] J. Willbold, F. Sciberras, M. Strohmeier, and V. Lenders, "Satellite cybersecurity reconnaissance: Strategies and their real-world evaluation," in *Proc. IEEE Aerosp. Conf.*, Mar. 2024, pp. 1–13.

[38] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 1, pp. 372–425, 1st Quart., 2025.

[39] E. Erdogan, I. Altunbas, G. K. Kurt, M. Bellemare, G. Lamontagne, and H. Yanikomeroglu, "Site diversity in downlink optical satellite networks through ground station selection," *IEEE Access*, vol. 9, pp. 31179–31190, 2021.

[40] K. Stock and H. Guesgen, "Geospatial reasoning with open data," in *Automating Open Source Intelligence*. Boston, MA, USA: Syngress, 2016, ch. 10, pp. 171–204. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128029169000105

[41] B. Zhang, H. Lei, Y. Cai, Z. Zhong, and Z. Jiao, "COVID-19 contact tracking based on person reidentification and geospatial data," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 5, May 2023, Art. no. 101558.

[42] M. Korda. (Oct. 2018). *Widespread Blurring of Satellite Images Reveals Secret Facilities*. Accessed: Apr. 27, 2025. [Online]. Available: https://fas.org/publication/widespread-blurring-of-satellite-images-reveals-secret-facilities/

[43] O. Elharrouss, N. Almaadeed, S. Al-Máadeed, and Y. Akbari, "Image inpainting: A review," *Neural Process. Lett.*, vol. 51, no. 2, pp. 2007–2028, Dec. 2019.

[44] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, "Image inpainting," in *Proc. 27th Annu. Conf. Comput. Graph. Interact. Techn.*, Jan. 2000, pp. 417–424.

[45] M. A. Zaytar and C. El Amrani, "Satellite image inpainting with deep generative adversarial neural networks," *IAES Int. J. Artif. Intell. (IJ-AI)*, vol. 10, no. 1, p. 121, Mar. 2021.

[46] M. Czerkawski, P. Upadhyay, C. Davison, A. Werkmeister, J. Cardona, R. Atkinson, C. Michie, I. Andonovic, M. Macdonald, and C. Tachtatzis, "Deep internal learning for inpainting of cloud-affected regions in satellite imagery," *Remote Sens.*, vol. 14, no. 6, p. 1342, Mar. 2022.

[47] T. Panboonyuen, C. Charoenphon, and C. Satirapod, "SatDiff: A stable diffusion framework for inpainting very high-resolution satellite imagery," *IEEE Access*, vol. 13, pp. 51617–51631, 2025.

[48] E. D. Cannas, S. Mandelli, P. Bestagini, S. Tubaro, and E. J. Delp, "Deep image prior amplitude SAR image anonymization," *Remote Sens.*, vol. 15, no. 15, p. 3750, Jul. 2023. [Online]. Available: https://www.mdpi.com/2072-4292/15/15/3750

[49] R. Liu, Z. Li, and J. Jia, "Image partial blur detection and classification," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2008, pp. 1–8.

[50] H. Li, Y. Zhang, W. Wang, S. Zhang, and S. Zhang, "SwapInpaint2: Towards high structural consistency in identity-guided inpainting via background-preserving GAN inversion," *Pattern Recognit.*, vol. 158, Feb. 2025, Art. no. 110969.

[51] A. Criminisi, P. Perez, and K. Toyama, "Object removal by exemplar-based inpainting," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2, Jun. 2003.

[52] A.-A. Barglazan, R. Brad, and C. Constantinescu, "Image inpainting forgery detection: A review," *J. Imag.*, vol. 10, no. 2, p. 42, Feb. 2024.

[53] X. Ding, Y. Deng, Y. Zhao, and W. Zhu, "AFTLNet: An efficient adaptive forgery traces learning network for deep image inpainting localization," *J. Inf. Secur. Appl.*, vol. 84, Aug. 2024, Art. no. 103825.

[54] L. Huang, Y. Huang, and Q. Guan, "Improving image inpainting via adversarial collaborative training," *IEEE Trans. Multimedia*, vol. 27, pp. 356–370, 2025.

[55] V. K. Kadha, S. Bakshi, and S. K. Das, "Unravelling digital forgeries: A systematic survey on image manipulation detection and localization," *ACM Comput. Surveys*, vol. 57, no. 12, pp. 1–36, Apr. 2025.

[56] H. Mareen, D. Karageorgiou, G. V. Wallendael, P. Lambert, and S. Papadopoulos, "TGIF: Text-guided inpainting forgery dataset," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Dec. 2024, pp. 1–6.

[57] C. Shin, J. Choi, H. Kim, and S. Yoon, "Large-scale text-to-image model with inpainting is a zero-shot subject-driven image generator," 2024, *arXiv:2411.15466*.

[58] T. Sun, W. Fang, W. Chen, Y. Yao, F. Bi, and B. Wu, "High-resolution image inpainting based on multi-scale neural network," *Electronics*, vol. 8, no. 11, p. 1370, Nov. 2019.

[59] T. Mayet, P. Shamsolmoali, S. Bernard, E. Granger, R. Hérault, and C. Chatelain, "TD-paint: Faster diffusion inpainting through time aware pixel conditioning," 2024, *arXiv:2410.09306*.

[60] O. Elharrouss, R. Damseh, A. N. Belkacem, E. Badidi, and A. Lakas, "Transformer-based image and video inpainting: Current challenges and future directions," *Artif. Intell. Rev.*, vol. 58, no. 4, pp. 1–45, Feb. 2025.

[61] Y. Du, J. He, Q. Huang, Q. Sheng, and G. Tian, "A coarse-to-fine deep generative model with spatial semantic attention for high-resolution remote sensing image inpainting," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, 2022, Art. no. 5621913.

[62] D. Zhou, Y. Chen, Y. Zhang, and J. Niu, "Satellite image inpainting with edge-conditional expectation attention," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 18, pp. 10830–10845, 2025.

[63] F. Kelbert and A. Pretschner, "Data usage control enforcement in distributed systems," in *Proc. 3rd ACM Conf. Data Appl. Secur. Privacy*, Feb. 2013, pp. 71–82.

[64] G. Oligeri, S. Sciancalepore, S. Raponi, and R. D. Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 274–289, 2023, doi: 10.1109/TIFS.2022.3219287.

[65] M. Abdrabou and T. A. Gulliver, "Authentication for satellite communication systems using physical characteristics," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 48–60, 2023.

[66] B. Wang, Z. Chang, S. Li, and T. Hämäläinen, "An efficient and privacy-preserving blockchain-based authentication scheme for low Earth orbit satellite-assisted Internet of Things," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 6, pp. 5153–5164, Dec. 2022.

[67] S. Cao, S. Dang, Y. Zhang, W. Wang, and N. Cheng, "A blockchain-based access control and intrusion detection framework for satellite communication systems," *Comput. Commun.*, vol. 172, pp. 216–225, Apr. 2021.

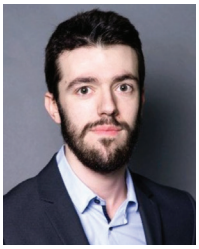
[68] M. Torky, T. Gaber, E. Goda, V. Snasel, and A. E. Hassanien, "A blockchain protocol for authenticating space communications between satellites constellations," *Aerospace*, vol. 9, no. 9, p. 495, Sep. 2022.

[69] Y. Chen, S. Chen, J. Liang, L. W. Feagan, W. Han, S. Huang, and X. S. Wang, "Decentralized data access control over consortium blockchains," *Inf. Syst.*, vol. 94, Dec. 2020, Art. no. 101590.

[70] T. T. T. Le, N. U. Hassan, X. Chen, M.-S. Alouini, Z. Han, and C. Yuen, "A survey on random access protocols in direct-access LEO satellite-based IoT communication," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 1, pp. 426–462, 1st Quart., 2025.

[71] L. Zhen, A. K. Bashir, K. Yu, Y. D. Al-Otaibi, C. H. Foh, and P. Xiao, "Energy-efficient random access for LEO satellite-assisted 6G Internet of Remote Things," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5114–5128, Apr. 2021.

[72] X. Liu, H. Zhang, K. Long, A. Nallanathan, and V. C. M. Leung, "Deep dyna-reinforcement learning based on random access control in LEO satellite IoT networks," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14818–14828, Aug. 2022.
[73] J.-H. Lee, H. Seo, J. Park, M. Bennis, and Y.-C. Ko, "Learning emergent random access protocol for LEO satellite networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 257–269, Jan. 2023.
[74] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requirements Eng.*, vol. 16, no. 1, pp. 3–32, Mar. 2011.
[75] Eur. Space Agency. (2020). *Newcomers Earth Observation Guide*. Accessed: Apr. 29, 2025. [Online]. Available: https://business.esa.int/newcomers-earth-observation-guide
[76] K. Antoniadis, I. Z. Gitas, N. Georgopoulos, D. Stavrakoudis, and D. Hadjimitsis, "Investigating the potential of ICEYE-SAR data in storm damage detection in a coniferous forest with rugged terrain," *Int. J. Remote Sens.*, vol. 46, no. 4, pp. 1622–1651, Feb. 2025.
[77] M. D. Graziano, "SAR-based ship route estimation by wake components detection and classification," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Jul. 2015, pp. 3255–3258.
[78] M. Zhu, X. Wan, B. Fei, Z. Qiao, C. Ge, F. Minati, F. Vecchioli, J. Li, and M. Costantini, "Detection of building and infrastructure instabilities by automatic spatiotemporal analysis of satellite SAR interferometry measurements," *Remote Sens.*, vol. 10, no. 11, p. 1816, Nov. 2018.
[79] eoPortal Directory. (2025). *Satellite Vu Mission Overview*. Accessed: Apr. 29, 2025. [Online]. Available: https://www.eoportal.org/satellite-missions/satellite-vu#space-and-hardware-components
[80] Albedo Space. (2025). *Albedo: Aerial-quality Imagery From Space*. Accessed: Apr, 29, 2025. [Online]. Available: https://albedo.com/
[81] F. Zhou, B. Zhao, M. Tao, X. Bai, B. Chen, and G. Sun, "A large scene deceptive jamming method for space-borne SAR," *IEEE Trans. Geosci. Remote Sens.*, vol. 51, no. 8, pp. 4486–4495, Aug. 2013.
[82] B. Huang, W.-Q. Wang, S. Zhang, H. Wang, R. Gui, and Z. Lu, "A novel approach for spaceborne SAR scattered-wave deception jamming using frequency diverse array," *IEEE Geosci. Remote Sens. Lett.*, vol. 17, no. 9, pp. 1568–1572, Sep. 2020.
[83] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Adv. Space Res.*, vol. 66, no. 1, pp. 176–192, Jul. 2020.
[84] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.
[85] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *J. Adv. Res.*, vol. 7, no. 2, pp. 193–208, Mar. 2016.
[86] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Adv. Space Res.*, vol. 67, no. 7, pp. 2077–2103, Apr. 2021.
[87] H. Karmouni, M. A. Tahiri, I. Dagal, H. Amakdouf, M. O. Jamil, H. Qjidaa, and M. Sayyouri, "Secure and optimized satellite image sharing based on chaotic eπ map and Racah moments," *Expert Syst. Appl.*, vol. 236, Feb. 2024, Art. no. 121247.
[88] W. Feng, Q. Wang, H. Liu, Y. Ren, J. Zhang, S. Zhang, K. Qian, and H. Wen, "Exploiting newly designed fractional-order 3D Lorenz chaotic system and 2D discrete polynomial hyper-chaotic map for high-performance multi-image encryption," *Fractal Fractional*, vol. 7, no. 12, p. 887, Dec. 2023.
[89] M. A. Al-Khasawneh, I. Uddin, S. A. A. Shah, A. M. Khasawneh, L. Abualigah, and M. Mahmoud, "An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications," *Cluster Comput.*, vol. 25, no. 2, pp. 1–15, Apr. 2022.
[90] M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldhahri, A. Alzahrani, and A. A. Alarood, "A MapReduce based approach for secure batch satellite image encryption," *IEEE Access*, vol. 11, pp. 62865–62878, 2023.
[91] M. Dua, R. Bhogal, S. Dua, and N. Chakravarty, "Satellite image encryption using amalgamation of randomized three chaotic maps and DNA encoding," *Phys. Scripta*, vol. 100, no. 1, Jan. 2025, Art. no. 015241.
[92] Satell. Imag. Corp. (2024). *Albedo (10cm) Satellite Sensor*. Accessed: Apr. 23, 2025. [Online]. Available: https://www.satimagingcorp.com/satellite-sensors/albedo-10cm/
[93] P. Wang and E. Sertel, "Channel–spatial attention-based pan-sharpening of very high-resolution satellite images," *Knowl.-Based Syst.*, vol. 229, Oct. 2021, Art. no. 107324. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705121005864
[94] Y. Li, L. Hu, L. Dong, H. Wu, J. Tian, J. Zhou, and X. Li, "Transformer-based image inpainting detection via label decoupling and constrained adversarial training," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 3, pp. 1857–1872, Mar. 2024.
[95] Y. Yao, T. Han, X. Gao, Y. Ren, and W. Meng, "Deep video inpainting detection and localization based on ConvNeXt dual-stream network," *Expert Syst. Appl.*, vol. 247, Aug. 2024, Art. no. 123331.
[96] K. Matsui, H. Shirai, Y. Kageyama, and H. Yokoyama, "Improving the resolution of UAV-based remote sensing data of water quality of lake hachiroko, Japan by neural networks," *Ecological Informat.*, vol. 62, May 2021, Art. no. 101276, doi: 10.1016/j.ecoinf.2021.101276.
[97] H. Reza Ghafarian Malamiri, F. Arabi Aliabad, S. Shojaei, M. Morad, and S. S. Band, "A study on the use of UAV images to improve the separation accuracy of agricultural land areas," *Comput. Electron. Agricult.*, vol. 184, May 2021, Art. no. 106079, doi: 10.1016/j.compag.2021.106079.
[98] F. Zhang, C. Wu, B. Wang, and K. J. R. Liu, "MmEye: Super-resolution millimeter wave imaging," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6995–7008, Apr. 2021.
[99] Y. Han, J. Liu, X. Deng, J. Jing, and Y. Zhang, "Confidential image super-resolution with privacy protection," *Chin. J. Electron.*, vol. 33, no. 6, pp. 1447–1457, Nov. 2024.
[100] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," *Remote Sens.*, vol. 13, no. 11, p. 2221, Jun. 2021. [Online]. Available: https://www.mdpi.com/2072-4292/13/11/2221
[101] L. Montero, J. Frery, C. Kherfallah, R. Bredehoft, and A. Stoian, "Machine learning training on encrypted data with TFHE," in *Proc. 10th ACM Int. Workshop Secur. Privacy Anal.*, New York, NY, USA, Jun. 2024, pp. 71–76, doi: 10.1145/3643651.3659891.



NATHANAËL DENIS received the Ph.D. degree in telecommunications engineering from Télécom SudParis, Institut Polytechnique de Paris. He is currently a Postdoctoral Researcher at the King Abdullah University of Science and Technology, Saudi Arabia. His current research interests include satellite network cybersecurity and privacy, remote sensing privacy, and radar technologies.



ROBERTO DI PIETRO (Fellow, IEEE) is currently a Full Professor of computer science with CEMSE, KAUST, Saudi Arabia. Previously, he was a Professor of cybersecurity and the Founder of the CRI-Laboratory, HBKU-CSE, Doha, Qatar. He was also the Global Head for Cybersecurity Research of Nokia Bell Labs. In 1995, his professional journey began in the Military Sector as a Senior Technical Officer with Italian Ministry of Defense, where he served for a decade. His research interests include AI-driven cybersecurity, with applications to the protection of critical infrastructures, online social networks, distributed ledger technologies, and cryptocurrencies.

Prof. Di Pietro is a Member Academia Europaea and an ACM Distinguished Scientist. Besides being involved in M&A of startups—and having founded one (exited)—he is a board member of a few research institutions. From 2011 to 2012, he was a recipient of the Chair of Excellence from the University Carlos III of Madrid. In 2020, he was a recipient of the Jean-Claude Laprie Award for significantly influencing the theory and practice of dependable computing. In 2022, he was awarded the Individual Innovation Award from HBKU.