INTERNATIONAL JOURNAL OF
Telecommunications
AIR DEFENSE COLLEGE

An Optimized Technique for Securing Modern Smart Cities Using Equipped Crowed-Sensing Unmanned aerial vehicles

Amr Aboghanem [1,2,*], **Hanan Amer** [3] **and Abeer Twakol** [4]

[1] Dept. Electronics and Communications, Faculty of Engineering, Mansoura, Egypt, Email: Amraboghanem836@gmail.com

[2] Dep. of Electronics and Electrical Communications Engineering, Air Defense Collage, Egyptian Military Academy; New Administrative Capital.

[3] Dept. Electronics and Communications, Faculty of Engineering, Mansoura, Egypt, Email:eng_hanan_2007@mans.edu.eg.

[4] Dept. Electronics and Communications, Faculty of Engineering, Mansoura, Egypt, E-mail: abeer.twakol@mans.edu.eg.

* Correspondence: Amraboghanem836@gmail.com; Tel.: (+201009434384).

Citation: Aboghanem, A.; Amer, H.; Twakol , A. *Inter. Jour. of Telecommunications, **IJT'2025**, Vol. 05, Issue 02, pp. 1-15, 2025.*

Doi: 10.21608/ijt.2025.392623.1117

Editor-in-Chief: Youssef Fayed.

Received: 13/06/2025.

Accepted date: 08/08/2025.
Published date: 08/08/2025.

Publisher's Note: The International Journal of Telecommunications, IJT, stays neutral regarding jurisdictional claims in published maps and institutional affiliations.

Abstract: Unmanned aerial vehicles (UAVs) have become a vital and indispensable tool in modern disaster management, especially in smart cities that rely on complex infrastructure and communication networks. This paper addresses the pivotal importance of UAVs in disaster prevention efforts, with a particular focus on the challenges posed by GNSS signal disturbances, which hinder accurate navigation and relief efforts. In this paper, we present an efficient and robust system that aims to establish a secure and reliable communication channel between UAVs—equipped with crowd-sensing techniques and advanced estimation filters such as Extended Kalman Filters and Particle Filters—and the ground control station. This system ensures continuous communication even in the absence of GNSS signals, enabling UAVs to efficiently perform their vital tasks. Furthermore, we propose a secure communication method based on robust cryptographic steganography, combining the Advanced Encryption Standard (AES) and stego-images using discrete wavelet (DWT) coefficients. The test results confirm the effectiveness of the proposed method, as its performance was successfully evaluated using the mean square error (MSE), maximum signal-to-noise ratio (PSNR), and correlation (COR) metrics.

Keywords: Unmanned Aerial Vehicle (UAV) ; Global Navigation Satellite System (GNSS) ; Inertial Measurement Unit (IMU) ; Extended Kalman Filter (EKF) ; Particle Filter (PF), Discrete Wavelet Transform (DWT) ; Advanced Encryption Standard (AES) .

1. Introduction

In the contemporary landscape, smart cities stand as emblematic embodiments of technological progress and sustainability, leveraging cutting-edge innovations like the Internet of Things (IoT), artificial intelligence (AI), and advanced communication networks (5G and 6G) to elevate living standards and optimize resource utilization [1-3]. In addition to making daily life easier, these urban environments have a powerful ability to protect people from natural and man-made disasters, reducing the number of deaths and injuries and the amount of damage to property [4-5]. Smart cities are excellent at preventing and handling disasters because they use integrated sensor arrays and real-time data analytics to find risks like earthquakes and floods early, send out early warnings, and make it easier for everyone to work together during an emergency [6–8]. Drones emerge as indispensable assets in the disaster relief arsenal of smart cities, offering swift and inventive solutions for crisis management [9-10]. Their versatility includes quick aerial surveys to check for damage, quick delivery of essential supplies to areas that can't be reached, and advanced search and rescue capabilities that use thermal sensors and night vision cameras to find survivors in tough environments [11–14].

The proposed framework makes the following contributions :

- We discuss the significance of UAVs in addressing crisis-related issues, particularly those such as GNSS signal disruptions that complicate normal navigation, and the suggested approach for aid operations.
- The suggested method uses a combination of crowd-sensing data and a number of nonlinear estimators to improve the navigation solution, even when GNSS signals are lost.
- The suggested method sets up a solid communication link between the UAVs and the ground control station, even when the channels are noisy. This improves operational continuity during crises by using these advanced encryptions and embedding techniques to keep data safe and private during UAV operations in crises.

The paper is organized into the following subsections: Section 2 discusses the existing work related to the proposed approach. Section 3 provides an overview of the system and scheme modeling, including its components and how it works. Section 4 presents and analyzes the experimental results obtained from the suggested system. The paper concludes with Section 5, which outlines the findings of the study.

2. Related work

Amidst the backdrop of escalating climate change impacts and a surge in natural disasters, there has been a notable flow of interest surrounding the advancement of communication networks, particularly those tailored for drones [15-16]. Concurrently, the exploration of specialized drone applications has intensified due to their pivotal role in disaster response and event support.

To improve the well-being of citizens and make sure they are ready for unplanned emergencies, smart cities need to make a big change toward using cutting-edge technologies. This means that technological progress needs to be carefully and constantly evaluated to make sure that everyone has access to the newest tools and ideas [17-18]. This article focuses on the network-centric components of multi-drone systems and their potential applications in monitoring major events and pandemics. It also talks about how to set up a strong communication link between UAVs and the ground control station, even over noisy channels, so that operations can continue during crises. This article uses advanced encryption and embedding techniques to keep data safe and private during UAV operations during crises. Hence, Table 1 shows the important works related to the proposed method in this paper.

Table 1. the important works related to the proposed method in this paper.

Ref.	Main Contribution	Advantages	Disadvantages
18	UAV-aided 6G networks for disaster management	Real-time communication, integration with 6G	No security focus, lacks image encryption or classification
19	AI-based object detection in UAV rescue missions	Uses CNN models for object detection, improves rescue targeting	No encryption, lacks robust response time analysis
20	Lightweight encryption for IoT-UAV communication	Focus on speed and low energy consumption	No image classification, limited real-time UAV field testing
21	Secure drone video streaming using hybrid encryption	Improved video privacy, strong AES-RSA mix	High computational cost, no benchmark with modern detectors

22	EfficientNet for UAV-based object recognition	High accuracy, low computational demand	Doesn't consider encryption or system-level response time
23	Secure video transmission over UAV networks	Uses AES + RSA encryption	No compromise on system performance or response time
24	Using AI at the Edge with UAVs	Reduces Processing Time	Lacks Strong Encryption Technologies
25	Maintaining data integrity using blockchain	Preventing data tampering	Does not cover message analysis or real-time encryption

3. System and scheme modeling

This section gives a thorough explanation of the suggested approach and presents the system model .

3.1 System modeling

The proposed system is designed to ensure robust UAV navigation and secure communication, especially in GNSS-denied environments, by combining advanced sensor fusion and image-based steganography techniques as shown in Figure 1. First, the UAV navigates without GNSS signals using a fusion of Radar sensors (to detect targets, extract their velocity and height) and IMU, which measure position, velocity, and attitude. These inputs are processed using algorithms like EKF and PF to estimate accurate navigation parameters, enabling the UAV to remain stable and achieve reliable positioning in challenging conditions. Simultaneously, the UAV's camera (equipped with an Optical Flow Estimator) captures a cover image that will be used for secure communication. In parallel, a secret message is prepared for transmission.

The process begins with the secret message undergoing fuzzification, which transforms the message into a flexible and adaptable numerical form, making it suitable for further processing. The fuzzified message is then transformed using the DWT, which decomposes the data into various frequency components to allow efficient embedding into the image. To secure the message, it is encrypted using the AES algorithm, ensuring it remains protected from unauthorized access. After encryption, the transformed secret message is embedded into the DWT-transformed cover image using a weighted embedding function (α), where α represents the degree of embedding applied to the image. The result of this process is a stego-image—an image that visually resembles the original cover image but contains the securely hidden secret message.

In scenarios where GNSS signals are lost, such as in dense urban environments or under deliberate signal jamming, the system activates its alternative navigation strategy based on crowd-sensing fusion. The UAV collects accurate sensory data from onboard radar (for target detection, velocity, and altitude), an IMU (for position, velocity, and attitude), and a camera with optical flow estimation. These inputs are processed through advanced filtering algorithms (EKF and PF) to produce a stable and precise navigation solution in real-time, despite the absence of satellite-based positioning.

In parallel with the navigation process, the system prepares a secure message containing essential mission data. This message is encrypted, embedded within a cover image using steganography techniques, and transmitted over a potentially noisy wireless channel. Even with interference or data corruption during transmission, the ground station performs filtering and denoising operations to clean the received stego-image. It then applies DWT, de-weighting, and IDWT to extract the encrypted message, which is decrypted using the AES key and defuzzified to recover the original readable data. This ensures accurate and secure data transmission even when GNSS is unavailable.

The stego-image is then transmitted from the UAV over a noisy communication channel, such as wireless transmission prone to interference and noise. At the Earth Station, the received stego-image undergoes multiple processing steps to extract and recover the secret message accurately. First, the stego-image is processed through filtering techniques to remove any noise that may have been introduced during transmission. The filtered image is then decomposed using DWT to isolate the embedded data. To retrieve the original secret message, the weighted embedding function is reversed through de-weighting ($1/\alpha$), effectively scaling the embedded message back to its original state.

Once the weighted message is extracted, the Inverse Discrete Wavelet Transform (IDWT) is applied to reconstruct the hidden message. At this stage, the message remains in its encrypted form, so it is decrypted using the AES decryption key, which restores the original encrypted content. To convert the decrypted message back into a readable form, the system applies defuzzification, which reverses the earlier fuzzification process. The fully recovered message is then displayed at the Earth Station, where it is validated and compared against a fingerprinting database to verify its accuracy and integrity

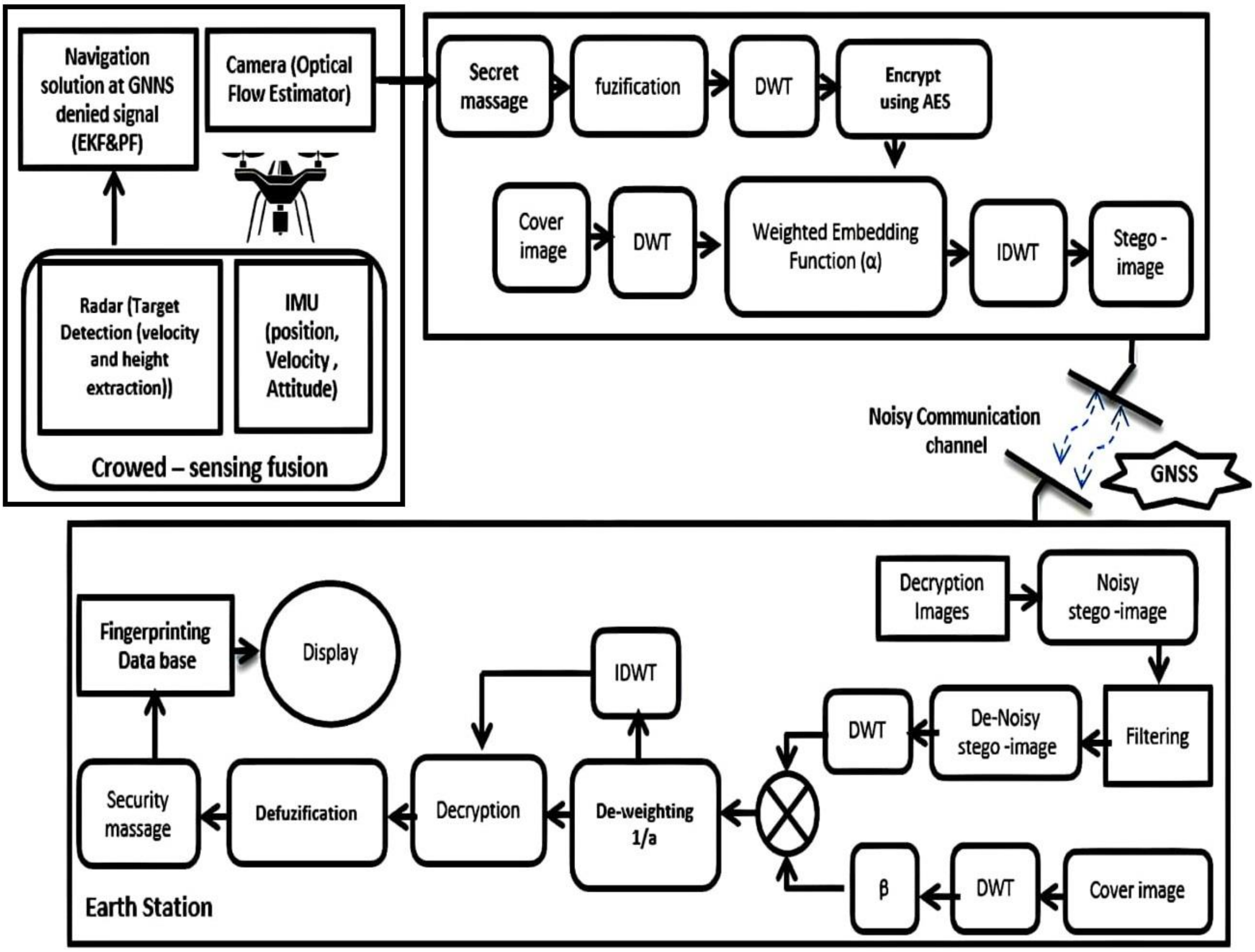


Figure1, the proposed system

Noise can occur intentionally or unintentionally during data transmission (the image carrying the message) from the drone to the ground station. This can affect the quality of the stego-image, alter some pixels in the image, compromise accurate extraction of the hidden message, and add an additional challenge to verifying the reliability of the data.

The system handles noise at the ground station by receiving the noisy stego-image. Filtering is the first step after reception, removing the noise generated by the wireless channel using techniques such as Gaussian Filter, Median Filter, or Wiener Filter. Denoising is then performed as a more precise filtering step. The removal of changes that specifically affect the embedded message can be achieved using algorithms such as Wavelet Thresholding and Non-Local Means. DWT analyzes the frequencies of the cleaned image and separates the image components, including the component carrying the message. De-weighting ($1/\alpha$) reverses the process by which the message was hidden, helping to reduce the impact of noise. IDWT: The frequencies are recombined to extract the encrypted message. AES Decryption: The message is decrypted (if the keys are unaffected). De-fuzzification: The message is recovered in its final, understandable form.

In summary, the system combines UAV navigation (through GNSS-denied signal fusion) with secure communication techniques using image steganography and encryption. The UAV achieves robust navigation in harsh conditions by fusing radar and IMU data through advanced filtering techniques like EKF and PF, while the secure communication process involves fuzzification, DWT, AES encryption, and weighted embedding to securely transmit a message hidden inside a cover image. The Earth Station processes the received stego-image through noise removal, de-weighting, and IDWT, followed by AES decryption and defuzzification to recover and display the original message, ensuring security, accuracy, and reliability in data transmission.

3.2 scheme modeling

The proposed system has been developed to enable dependable UAV navigation and safeguarded communication in modern smart cities during natural disasters that lead to unavailable GNSS signals. This is achieved by integrating cutting-edge sensor fusion mechanisms with image-based information security techniques like steganography. Hence without GNSS signals, the UAV undertakes navigation tasks by amalgamating data from radar sensors, which identify targets and extract their velocity and altitude, alongside IMU sensors that record position, velocity, and attitude

Utilizing algorithms such as the EKF and PF, these inputs are processed to ascertain precise navigation parameters, ensuring the UAV's stability and accurate positioning even in challenging environments. Concurrently, the UAV's camera, equipped with an optical flow estimater, captures a cover image for secure communication purposes, while a confidential message is readied for transmission. Figure 2 shows the flight path when there is a GNSS network outage.

The encryption process commences with the confidential message undergoing fuzzification, a procedure that converts the message into a versatile numerical format, optimizing it for subsequent processing stages. This fuzzified message is then subjected to transformation via the DWT, which dissects the data into distinct frequency components, facilitating efficient embedding into the image. To reinforce the message's security, it undergoes encryption using AES algorithm, safeguarding it against unauthorized access. Following encryption, the transformed secret message is integrated into the DWT-transformed cover image through a weighted embedding function (α), where α denotes the level of embedding applied to the image.

The encryption process commences with the confidential message undergoing fuzzification, a procedure that converts the message into a versatile numerical format, optimizing it for subsequent processing stages. This

fuzzified message is then subjected to transformation via the DWT, which dissects the data into distinct frequency components, facilitating efficient embedding into the image. To reinforce the message's security, it undergoes encryption using AES algorithm, safeguarding it against unauthorized access. Following encryption, the transformed secret message is integrated into the DWT-transformed cover image through a weighted embedding function (α), where α denotes the level of embedding applied to the image.

The outcome of this process is a stego-image—a visually similar image to the original cover image, concealing the securely hidden confidential message. Figure 3 shows the flowchart of the proposed system

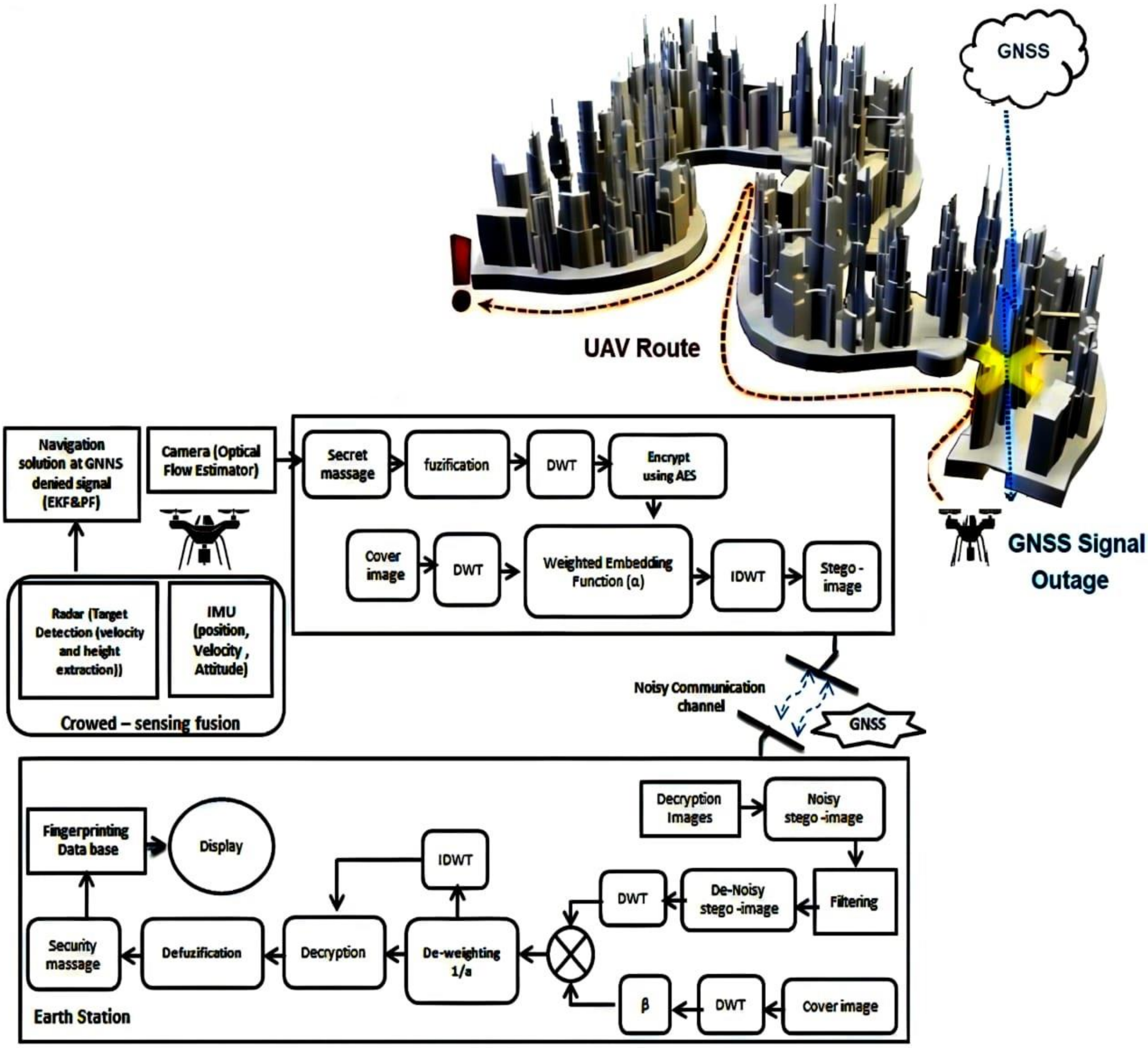


Figure2, Unmanned Arial Vehicle (UAV) in a GNSS denied environment

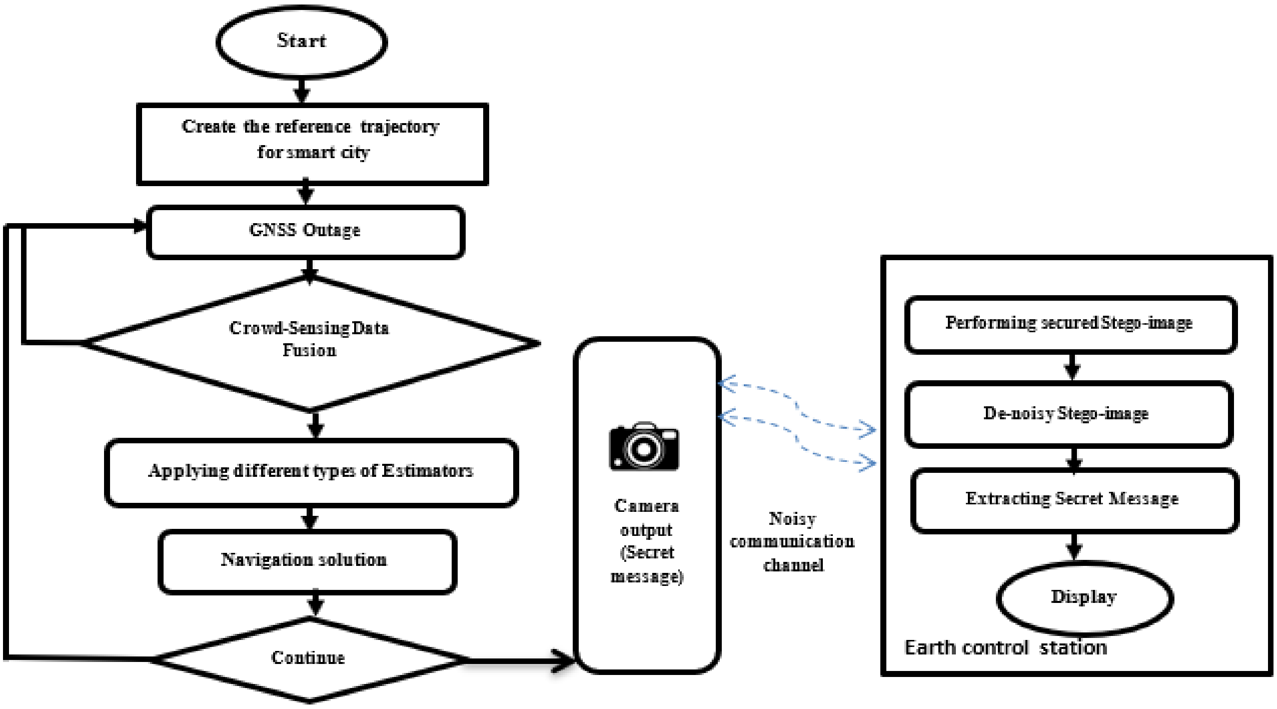

Start
Create the reference trajectory for smart city
GNSS Outage
Crowd-Sensing Data Fusion
Applying different types of Estimators
Navigation solution
Continue
Camera output (Secret message)
Noisy communication channel
Performing secured Stego-image
De-noisy Stego-image
Extracting Secret Message
Display
Earth control station

Figure 3, The flowchart of the proposed system.

3.2.1.The navigation solution Algorithm Using types of linear and nonlinear estimators

The proposed navigation solution relies on a combination of linear and non-linear estimators like the Extended EKF and PF. The PF, a probabilistic estimator employing random samples to estimate non-Gaussian and non-linear processes, approximates the target distribution through a large set of weighted samples known as particles. This approach is essential to the system because it provides benefits like the ability to estimate complete probability density functions, effective particle guidance towards high-probability areas, and efficient management of non-linear state and observation models. Understanding the fundamental operations of the PF within the system is vital, and the derivation of its basic equations is essential for implementation and comprehension.

- State representation or initialization

The state values' (probability density function (pdf)) is described using (n-particles) rather than the second-order statistical description. As a result, the (pdf) is:

$$p(x) = \int_{i=1}^{n} w_i \, K(x - x_i) \tag{1}$$

w_i : weight of i^{th} particle, and K( ): basis function. If K(x) assumed to be the Dirac's delta, so the equation will:

$$p(x) = \frac{1}{n} \int_{i=1}^{n} \delta(x - x_i) \tag{2}$$

- Prediction

$$p\left(x_{k+1}/y_{0,\dots} y_k\right) = \int p(x_{k+1}/x_k) p(x_k/y_{0,\dots} y_k)\, dx_k \tag{3}$$

$$p\left(x_{k+1}/y_{0,\dots} y_k\right) = \sum_{i=1}^{n} w_{k,i}\, p(x_{k+1}/\bar{x}_{k,i}) \tag{4}$$

After sampling $\{\hat{x}_{k,i}\}$ the equation of prediction will be:

$$p\big(x_{k+1}/y_{0,\dots}\, y_k\,\big) = \textstyle\sum_{i=1}^{n} \frac{1}{n} \delta(x_k - \hat{x}_{k,i}) \tag{5}$$

- Update

When the likelihood is concentrated on a few small state values, the new weights may approach zero, resulting in a very low probability. To solve this problem, we replace a high-weight particle that is more likely to be drawn repeatedly with a low-weight particle that is unlikely to be drawn at all using the resampling step. The final equations for the update step can be written as (n-particles) $\{\bar{x}_{k,i}\}$:

$$p(x_k/y_{0,\dots}\, y_k\,) = \textstyle\int_{i=1}^{n} \frac{1}{n} \delta(x_k - \bar{x}_{k,i}) \tag{6}$$

$$p(x_{k+1}/y_{0,\dots}\, y_{k+1}\,) = \textstyle\int_{i=1}^{n} \frac{1}{n} \delta(x_{k+1} - \bar{x}_{k+1,i}) \tag{7}$$

- Particle Resample

The To address the degeneracy issue in particle filtering, where a small number of particles carry significant weight while the majority have minimal weights, a resampling step is employed. This technique helps mitigate the problem by redistributing the particle weights. The severity of this problem can be gauged by estimating the effective sample size through a specific equation.

$$N_{eff} = \frac{1}{\int_{i=1}^{n} (w_k^i)^2} \tag{8}$$

3.2.2 Performing the Stego-Image Process

Figure 4 illustrates the process of encrypting secret messages using the AES algorithm

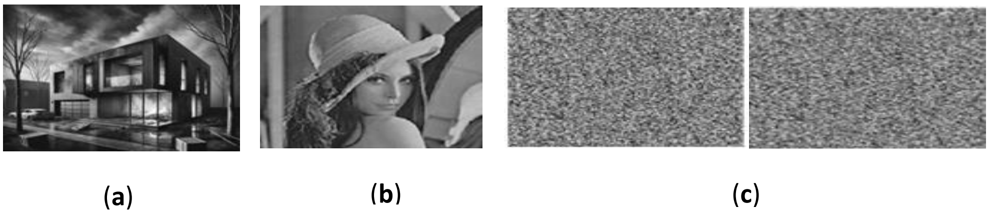


Figure4. (a) Presents the original images like (burned House) that utilized as secret messages, (b) presents the secret messages before the encryption process and, (c) presents the encrypted secret message utilizing the (AES) Algorithm

Figure5 shows the block diagram of the steganography system. The weighted DWT coefficients for the corresponding sub-bands of the cover image are combined with the encrypted secret message using the AES technique using an adjusted embedding weighting function. This process can be represented as :

$$S\ (j,\ k) = \beta\ C\ (j,\ k) + \alpha\ M\ (j,\ k) \tag{9}$$

where

$$\beta + \alpha = 1 \tag{10}$$

The DWT of the encrypted confidential message (M) and the cover images (C) have two weighting intensity factors, α and β, respectively, and the modified DWT coefficients of the Stego-image are represented by (S).

When the Sego-image undergoes transmission through the communication channel, it is susceptible to distortion caused by various types of noise. To mitigate the impact of this noise diversity without compromising the crucial edge details of the Stego-image, a range of filters, both linear and nonlinear, are employed. This strategy, as illustrated in the block schematic of the proposed system, involves applying the DWT to the cover image to create LH, HL, HH, and LL bands

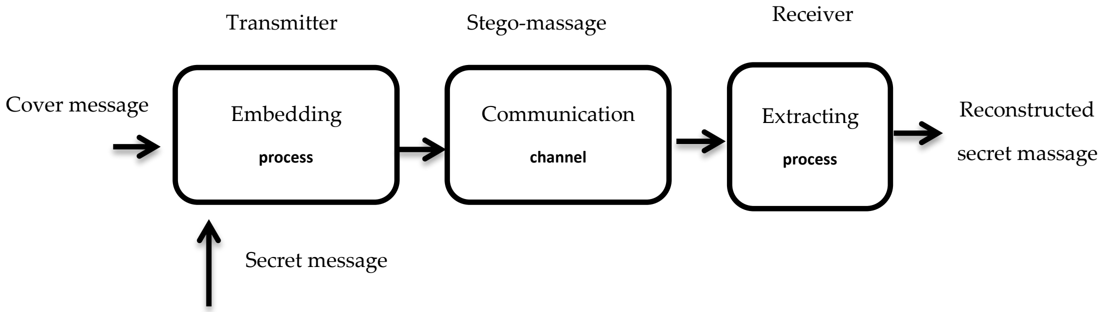


Figure 5. The block diagram of stenographic system.

Subsequently, the secret message is squeezed through fuzzification, processed using the DWT, and then established into the cover image based on a weighted embedding function. The IDWT is then utilized to reconstruct the Stego-image, demonstrating the importance of the weighting embedding function in managing noise interference within the system.

$$S\ (j,\ k) = \beta\ C\ (j,\ k) + \alpha\ M\ (j,\ k) + N\ (j,\ k) \tag{11}$$

where (N) is noise model.

4. Experimental Results and discussion

The results were extracted from the proposed method in three stages:

4.1 The navigational solution for UAV

The actual data was collected using a 3DR Solo quadcopter equipped with a set of crowd-sensing tools, including an inertial measurement unit (IMU), micro-FMCW radar, and a high-resolution camera. An enhanced Kalman filter was used to improve the accuracy of sensor data fusion. The experiments were conducted over two days, with the radar mounted at a 60-degree angle from the vertical axis of the drone to optimize coverage during flight. In the first phase, the GNSS was intentionally disabled to simulate a signal-denied environment, and the flight path was recorded without applying the proposed method to serve as a baseline for comparison. In the second phase, a flight mission was carried out, involving two full rotations of the drone and traversal through 10 predefined waypoints at a maximum speed of 5 m/s, over two durations: 40 seconds and 120 seconds. During this mission, the proposed technique—based on crowd-sensing data fusion—was applied to compare the drone's actual forward speed with the radar-derived speed estimates, aiming to validate the method's effectiveness in the absence of GNSS. Table 2 presents a comparison of the root mean square error (RMSE) values for position estimates obtained from the standalone inertial navigation system (INS) and the proposed navigation method under different durations of GNSS signal loss. This comparison highlights the accuracy and efficiency of the proposed approach in enhancing UAV navigation performance in GNSS-denied environments.

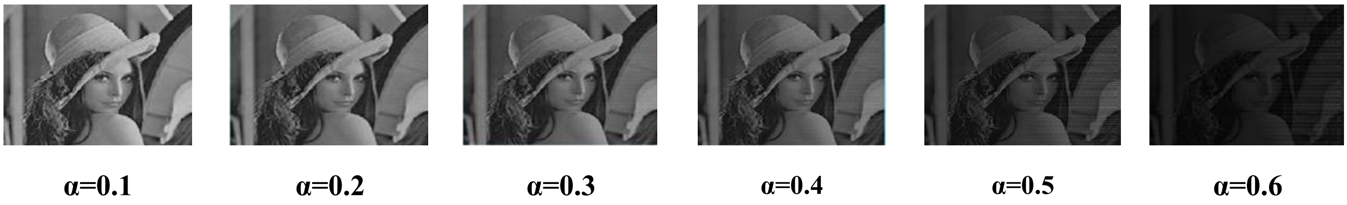
Table 2: Comparison of RMSE Values for Location States Recorded by the INS and the Proposed Navigation System

RMS Error (m)	**Symbol**		**Initial Trip Outage**	
			(40 sec)	**(120 sec)**
North direction (m)	INS Only		138.68	138.68
	Crowd-sensing	Using EKF	1.05	2.95
	System	Using PF	0.58	1.47
East direction (m)	INS Only		140.65	140.65
	Crowd-sensing	Using EKF	1.89	2.94
	System	Using PF	1.03	1.49
Height direction (m)	INS Only		219.21	219.21
	Crowd-sensing	Using EKF	2.19	2.28
	System	Using PF	1.11	1.55
Percentage of Improvements from INS %	Crowd-sensing	Using EKF	94.66	96.136
	System	Using PF	96.59	97.94

4.2 Extracting the secret message by the ground control station

The experiment utilized using a set of standard gray scale images as cover images and secret images encrypted using AES with size (256×256). Then, the secret images were hidden inside the cover images to generate secure stego-images. The secure stego-images were exposed to various types of noise to simulate noisy communication channels, such as Gaussian white noise (mean=0 and variance = 0.01), salt and pepper and speckle noises with (mean = 0 and variance = 0.05).

To remove noise, a spatial linear filter like (3×33) Average and (3×33) Wiener filters, then spatial nonlinear filter like (3×33) median filter. while Figure 6 shows the Stego- images Prior to entering the scrambled communication channel, where Lena image was utilized as cover and burned House image was utilized as the confidential message with various ESF factors (α=0.1to α=0.6).



α=0.1 **α=0.2** **α=0.3** **α=0.4** **α=0.5** **α=0.6**

Figure6. The Stego-image for various amounts of ESF.

Figure 7 illustrates the Stego-images after being sent through the scrambled communication channel, subjected to various noise classifications (Gaussian, salt-and-pepper, and speckle) and various values of the steganography ESF factor.

Figure 8 illustrates the Stego-images that have been de-noised using filters (Mean, Median, and Wiener) at the most common type of noise (Gaussian Noise) with various ESF factor, where the results showed that the median filter was the most effective compared to the other filters.

Lastly, the following equations have been utilized to assess the accuracy, efficacy, and resilience of the suggested system utilizing a variety of scales and parameters, such as MSE, PSNR, COR, and entropy.

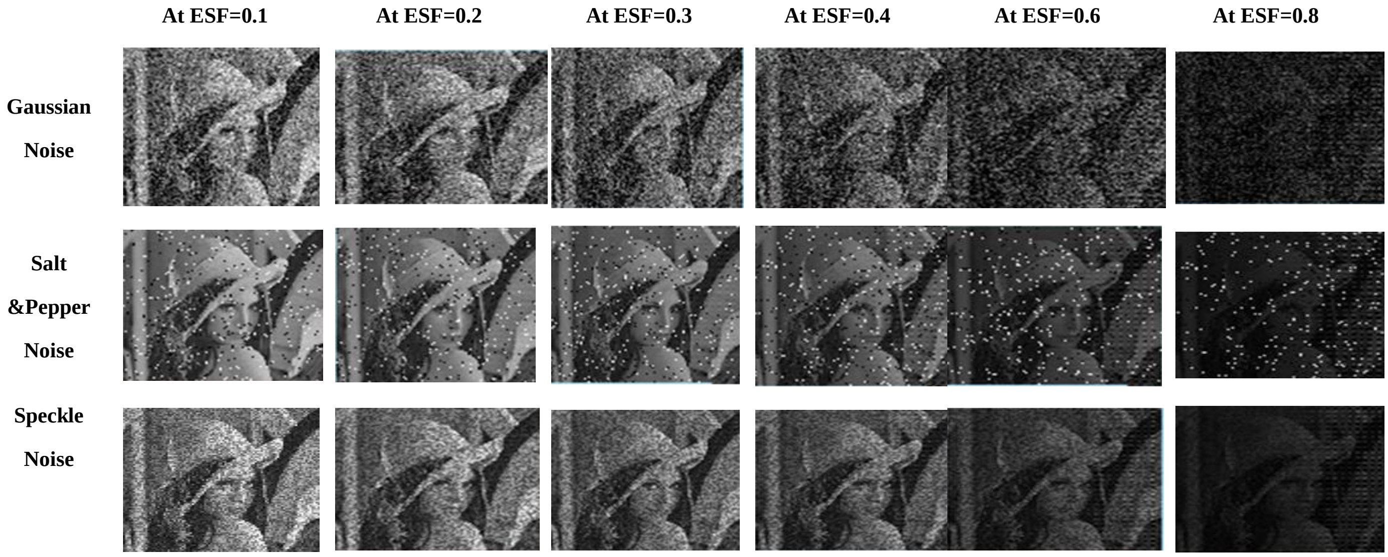


Figure7. Noisy stego-images containing various forms of noise.

- Mean Square Error (MSE):

$$\text{MSE} = \sum_{J=1}^{M}\sum_{K=1}^{N}\frac{(C(j,k)-S(j,k))^2}{M*N} \quad (12)$$

where: C (j, k), represents the cover image, S (j, k) represents the stego- image and M, N is the Size of the image.

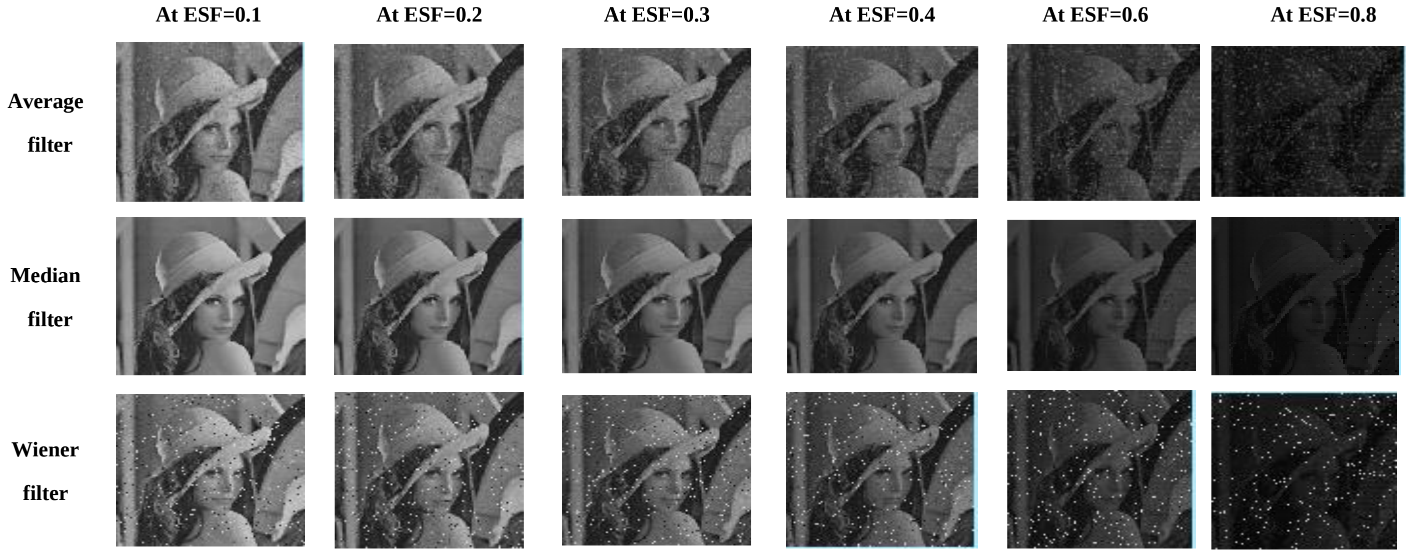


Figure8. The Denoised Stego-images

- peak signal to noise ratio(PSNR):

$$\text{PSNR} = 10\log_{10}\frac{(255)^2}{\text{MSE}} \quad (13)$$

- Cross Correlation coefficient (COR):

$$COR = \frac{\sum_0^{N-1}(C(j,k)-m1)(S(j,k)-m2)}{\sqrt{(\sum_0^{N-1}(C(j,k)-m1)^2(\sum_0^{N-1}(S(j,k)-m2)^2}} \quad (14)$$

where: m1 represented the average pixel count of the cover image and m2 represented the average pixel count of the Stego.

- Entropy

$$\text{Entropy} = -\sum_j \text{Pj Log(Pj)} \tag{15}$$

where: Pj refers to the probability of two adjacent pixels.

Figure 9 presents the entropy of the Stego-images for varying embedding factor values while utilizing the Lena image as a cover and the burned house as a confidential message following the passage through the cluttered communication channel.

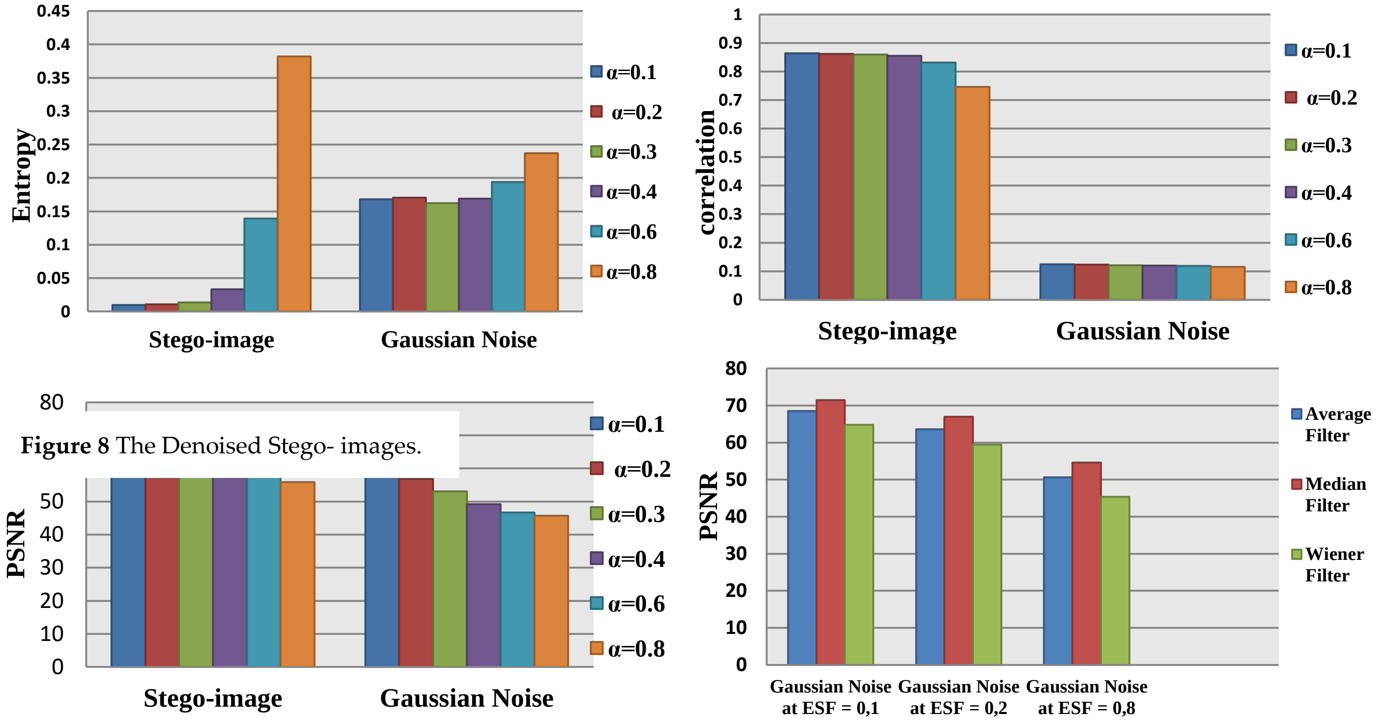


Figure 8 The Denoised Stego- images.

Figure9 Stego-image with many noises kinds

4.3 Performance Comparison with Existing Methods

Table.2 shows a detailed comparative analysis of the performance of the proposed method with other traditional and modern approaches. The proposed method does not rely on GNSS, making it ideal for disaster situations or hostile environments. It provides a dual layer of security: encryption (AES) + data hiding (steganography). It uses nonlinear fusion algorithms (EKF + PF) to increase accuracy. It is flexible in dealing with loss of communication or interference across wireless channels. This makes the proposed method clearly superior in environments with poor GNSS coverage or interference, and it also provides an integrated solution that combines secure navigation and encrypted communication. While traditional methods remain limited in performance outside of GNSS coverage, modern methods face challenges related to cost, the need for pre-maps, and reliance on suitable lighting conditions.

Table.2 Comparative analysis of the proposed method versus existing approaches

Comparison Aspect	Proposed Method	Traditional GNSS-Based Methods	Modern AI-Based Navigation Methods
GNSS Signal Dependency	Low (uses nonlinear estimators and crowd-sensing)	High (GNSS-only systems fail in signal-denied environments)	Medium (some can fuse sensors but rely on training data)
Navigation Accuracy (GNSS denied)	High (uses crowd-sensing + estimation techniques)	Very Low (almost no function without GNSS)	Medium to High (depends on model and environment)
Robustness to Signal Jamming	High	Low	Medium to High
Real-Time Performance	Real-time support using adaptive estimation	High (under GNSS signal)	Depends on model complexity
Communication Reliability	Maintains link even in noisy channels	Often affected by weak signal conditions	Depends on communication module used
Computational Complexity	Moderate (nonlinear estimators and data fusion required)	Low	High
Implementation Cost	Moderate (requires UAVs with sensors + estimators + crowd-input)	Low	High
Scalability in Disaster Scenarios	High (uses distributed UAVs + dynamic data sharing)	Low	Medium

5. Conclusion

This paper introduces a resilient, robust, and inventive method for determining the navigation solution for UAVs within contemporary intelligent urban areas amidst natural calamities causing communication breakdowns, such as the absence of GNSS connectivity. This strategy leverages crowd-sensing and banks on both linear and nonlinear estimators such as the EKF and PF to anticipate the anticipated trajectory of the UAVs. Additionally, this paper also outlines a secure means of communication for sharing data between the UAVs and the ground control station by concealing and encrypting the data through DWT steganography and AES techniques, ensuring the confidentiality of data exchange and countering potential subversive activities during natural disasters within contemporary intelligent urban environments.

Acknowledgment: Dr. Ahmed Gamal Abdellatif Ibrahim, the lecturer in the Department of Communications and Electronics Engineering at the Egyptian Military Academy (Air Defense College), Egypt, for his support and help in data collection and paper revision.

Conflicts of Interest: The authors certify that they have no conflicts of interest with regard to this research.

References

1. I. Chandran and K. Vipin, “Multi-UAV Networks for Disaster Monitoring: Challenges and Opportunities from a Network Perspective,” SN Comput. Sci., vol. 5, no. 5, 2024, doi: 10.1007/s42979-024-02788-3.
2. M. Scott, “Cascading risks, interdependent rights, and the progression of vulnerability in the context of pandemic containment measures: Implications for anticipatory action and the humanitarian-development nexus,” Int. J. Disaster Risk Reduct., vol. 104, p. 104360, 2024.
3. I. Chandran, A. Ahad, Z. Jiangbina, M. Tahir, I. Shayea, and I. Chandran, “Multi-UAV networks for disaster monitoring : challenges and opportunities from a network perspective,” Internet of Things, vol. 25, no. January, p. 101068, 2022, doi: 10.1016/j.iot.2024.101068.
4. A. Ahad, Z. Jiangbina, M. Tahir, I. Shayea, M. A. Sheikh, and F. Rasheed, “6G and intelligent healthcare: Taxonomy, technologies, open issues and future research directions,” Internet of Things (Netherlands), vol. 25, no. January, p. 101068, 2024, doi: 10.1016/j.iot.2024.101068.
5. L. M. S. Bine, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, “Connecting Internet of Drones and Urban Computing: Methods, protocols and applications,” Comput. Networks, vol. 239, no. December 2023, 2024, doi: 10.1016/j.comnet.2023.110136.
6. S. Siddiqui, S. Hameed, S. A. Shah, J. Arshad, Y. Ahmed, and D. Draheim, “A smart-contract-based adaptive security governance architecture for smart city service interoperations,” Sustain. Cities Soc., vol. 113, no. December 2023, p. 105717, 2024, doi: 10.1016/j.scs.2024.105717.
7. Y. Zhang, W. Wang, and F. Shi, “Reputation-based Raft-Poa layered consensus protocol converging UAV network,” Comput. Networks, vol. 240, no. December 2023, p. 110170, 2024, doi: 10.1016/j.comnet.2024.110170.
8. D. Kemp, V. Sharma, J. Harris, N. Blitz, and D. Williams, “Disclosure hesitancy and disaster risk: A survey of tailings professionals in the global mining industry,” Miner. Eng., vol. 215, no. February, p. 108821, 2024, doi: 10.1016/j.mineng.2024.108821.
9. I. Chandran and K. Vipin, “Multi-UAV networks for disaster monitoring: challenges and opportunities from a network perspective,” Drone Syst. Appl., vol. 12, pp. 1–28, 2024.
10. H. Zied, A. Gamal, and A.Salem, “S-Box Modification for the Block Cipher Algorithms,” Przeglad Electrotechniczny, vol. 4, pp. 278–281, 2023.
11. P. Bellini, P. Nesi, and G. Pantaleo, “IoT-enabled smart cities: A review of concepts, frameworks and key technologies,” Appl. Sci., vol. 12, no. 3, p. 1607, 2022.
12. A. I. Hentati and L. C. Fourati, “Comprehensive survey of UAVs communication networks,” Comput. Stand. Interfaces, vol. 72, p. 103451, 2020.
13. Zhong, H., Duan, Y., Tao, P., & Zhang, Z. (2025). Influence of ground control point reliability and distribution on UAV photogrammetric 3D mapping accuracy. Geo-spatial Information Science, 1-21.dOI: 10.1080/10095020.2025.2451204
14. Zhu, Y., Yan, Y., Dai, A., Dai, H., Zhang, Y., Zhang, W & Li, J. (2025). UAV-MSSH: A novel UAV photogrammetry-based framework for mining surface three-dimensional movement basin monitoring. Measurement, 242, 115944. doi.org /10.1016/ j.measurement.2024.115944
15. Lee, J. S., Jeong, S. H., Park, G., Kim, Y., Tutumluer, E., & Kim, S. Y. (2025). Geotechnical Application of Unmanned Aerial Vehicle (UAV) for Estimation of Ground Settlement after Filling and Compaction. Transportation Geotechnics, 101517. doi.org/10.1016/j.trgeo.2025.101517
16. Storch, M., Kisliuk, B., Jarmer, T., Waske, B., & de Lange, N. (2025). Comparative analysis of UAV-based LiDAR and photogrammetric systems for the detection of terrain anomalies in a historical conflict landscape. Science of Remote Sensing, 11, 100191. doi.org/10.1016/j.srs.2024 .100191.
17. Bakirci, M. (2025). Vehicular mobility monitoring using remote sensing and deep learning on a UAV-based mobile computing platform. Measurement, 244,116579.doi.org/10.1016/j.measurement.2024.116579

18. Z. Qadir, F. Ullah, H. S. Munawar, and F. Al-Turjman, “Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review,” Comput. Commun., vol. 168, pp. 114–135, 2021.
19. İ. Yazici, I. Shayea, and J. Din, “A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems,” Eng. Sci. Technol. an Int. J., vol. 44, 2023, doi: 10.1016/j.jestch.2023.101455.
20. M. M. Ahmed, M. A. Shawky, S. Zahran, A. Moussa, N. El-Shimy, A.A. Elmahallawy, S. Ansari, S. T. Shah, and A. G. Abdellatif, "An experi-mental analysis of outdoor UAV localisation through diverse estimators andcrowd-sensed data fusion," *Physical Communication*, vol. 66, p. 102475,2024.
21. A. G. Abdellatif, A. A. Salama, H. S. Zied, A. A. Elmahallawy, and M. A. Shawky, “An improved indoor positioning based on crowd-sensing data fusion and particle filter,” Physical Communication, p. 102225, Nov. 2023, doi: 10.1016/J.PHYCOM.2023.102225.
22. R. J. Garnica-Peña and I. Alcántara-Ayala, “The use of UAVs for landslide disaster risk research and disaster risk management: A literature review,” J. Mt. Sci., vol. 18, no. 2, pp. 482–498, 2021.
23. A. Gamal, M. Saleh, and A. Elmahallawy, “De-Noising of Secured Stego-Images using AES for Various Noise Types,” Przeglad Electrotechniczny, vol. 2, no.2 pp. 21–26, 2023.
24. Y. Zhang, W. Wang, and F. Shi, “Reputation-based Raft-Poa layered consensus protocol converging UAV network,” Comput. Networks, vol. 240, p. 110170, 2024.
25. R. Rukaiya, S. A. Khan, M. U. Farooq, and I. Matloob, “Communication architecture and operations for SDR-enabled UAVs network in disaster-stressed areas,” Ad Hoc Networks, vol. 160, p. 103506, 2024.