INTERNATIONAL JOURNAL OF Telecommunications
AIR DEFENSE COLLEGE

Using CryptoBin Encryption Algorithm in Military Applications

Ahmed H. Eltengy [1,*] and Hamed S. Zaid [2]

Citation: Eltengy, A. H.; Zaid, H. S. *International Journal of Telecommunications,* ***IJT'2021****, Vol. 01, Issue 01, pp. 1-7, December 2021.* https://ijt-adc.org/articles/2805-3044/993962

Editor-in-Chief: Yasser M. Madany
Received: 4-11-2021
Accepted: 19-12-2021
Published: 30-12-2021

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

[1] Air Defense College, Alexandria University, Alexandria, Egypt; tengy_fox@yahoo.com
[2] Air Defense College, Alexandria University, Alexandria, Egypt; dr.HamedZied.6333.adc@alexu.edu.eg
* Correspondence: tengy_fox@yahoo.com; +201203800771

Abstract: In recent years, there has been a significant increase in the use of location-based solutions. As a result, data encryption has become increasingly important in order to ensure privacy and confidentiality, especially in all domains, military and civil alike. This paper presents an application that will be used in both military and civilian situations, encrypting data on the location and movements of military personnel or civilian prospectors within a specific area using transmitting and receiving circuits controlled by a microcontroller programmed with the proposed encryption algorithm. The application will be used in both military and civilian settings. Depending on the task at hand or the nature of the immediate surroundings, the proposed application has been introduced, installed, and used in a variety of ways. The proposed technology has been tested in a variety of situations and has produced excellent results in all of them. The suggested application is confidential, authenticated, and simple to use, according to the results of frequency, speed, and security testing; this has been demonstrated by the results of these tests.

Keywords: Cryptography; location-based services; location-based encryption; CryptoBin algorithm; location security; data security.

1. Introduction

When information or data is shared across networks, it passes through a series of network devices around the world. As data travels across networks, there is a possibility that hackers will hack or steal it. To prevent this, users may install certain software or hardware to ensure the secure transmission of data or information. These operations in network security are known as "Encryption" [1]. Encryption involves converting plain text that is readable to humans into unintelligible text, which is known as ciphertext. This means taking readable data and changing it so that it appears randomly [2]. Encryption involves the use of an encryption key, which is a set of mathematical values agreed upon by both the sender and the receiver. The recipient uses the key to decrypt the data and return it to readable plain text [3]. The more complex the encryption key, the more secure the encryption, as third parties are less likely to decrypt it through brute force attacks (i.e., trying random numbers until the correct combination is guessed) [4]. Encryption is also used to protect passwords. Password encryption methods have your password to become unreadable by hackers [5].

In this paper, two uses of the proposed application will be presented and analyzed in detail, and the encryption algorithm will be applied (CryptoBin Algorithm) [6], and the main idea is to secure the movement and movement of vehicles and individuals, whether civilian or military. This idea boils down to placing a small device with the individuals or vehicles of the undercover mission [7]. The function of this device is to get the location and movements of people in the mission, encode the coordinates and send them directly to the main control center or command center, which plays the role of receiving and decoding the encrypted signals and sending them to the computer, which applies the decoding code and then displays the coordinates for each individual or vehicle on a screen similar to the radar screen is identifiable with each point in its name. And the zero position

for them is the starting point of the mission. Figure 1 shows a flowchart that describes the Cryptobin algorithm from the starting process, then receiving the keys values, after that starting a loop from 1 to 8, the received key value which archives the NOT function on bits, and creates a temporary value stores the bit value, if it's 0 then swap it to 1 and vice versa. The next step is merging swapped values with non-swapped values to combine the encrypted byte.

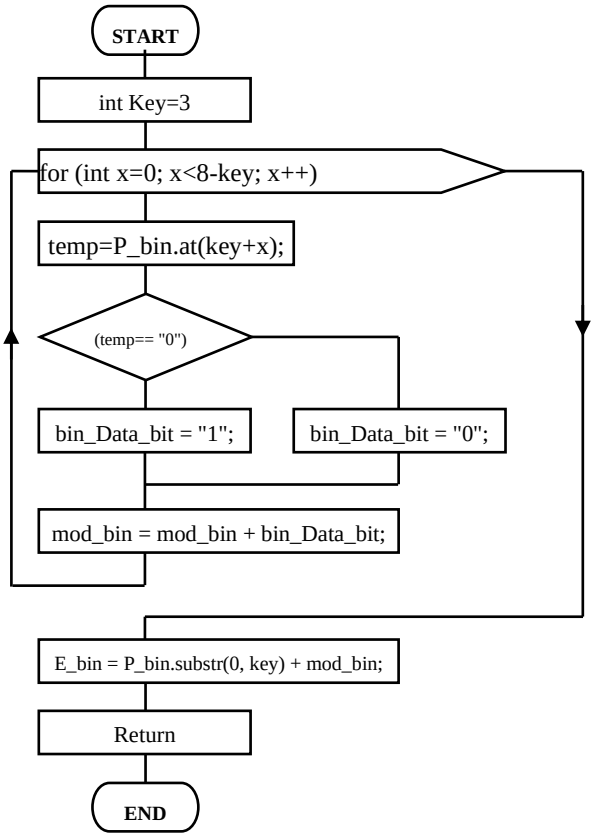

Figure 1. Flow Chart for CryptoBin Algorithm Structure.

2. Positioning and Navigation Systems

Positioning is important and is used in many applications, such as moving from one place to another, as well as being used in emergency services and tracking. GPS devices provide either binary coordinates such as longitude and latitude or triple coordinates, including altitude. these systems can be classified into [8]:

- Network-based positioning system;
- Handset-based positioning system;
- Hybrid-positioning system.

In this study, a low-cost inertial measurement unit (IMU). It is suggested as a motion sensor for areas outside the coverage area of GPS satellites, while these devices are used in areas with coverage [9].

2.1. The inertial navigation system (INS)

The inertial navigation system is a navigation device used to guide missiles, aircraft, submarines, and other vehicles [10]. Unlike other means of navigation, inertial guidance does not rely on observations from the Earth or the stars, radio and radar signals, or any other information that comes from outside the vehicle. Instead, a device called an inertial navigator provides orientation information [11]. This device comprises gyroscopes (overhead wheels) that determine direction, and accelerometers (devices that measure changes in speed and direction). An electronic computer uses this information to locate and direct the vehicle [12].

The IMU contains three single-axis accelerometers and three single-axis gyroscopes. The accelerometer detects the acceleration signal of the object in the vector's three-axis independent coordinate system, while the gyroscope detects the vector's angular velocity signal relative to the navigation coordinate system to measure the object's angular velocity and acceleration in three-dimensional space and use that to calculate the body's position [13]. It has a very important application value in navigation. To improve reliability, it is also possible to equip more sensors for each axis. The IMU should be fixed to the center of gravity of the measured object [14].

2.2. Global positioning system (GPS)

It is a navigation system based on satellites. It is owned by the United States of America and operated by the United States Space Forces (USSF) [15]. It is one of the global navigation satellite systems (GNSS) that provides geolocation and time information for any receiver on or near the surface of the earth around the clock, if it has a direct line of sight of four or more satellites, obstacles such as mountains or buildings Blocks relatively weak system signals [16]. GPS satellites orbit the Earth twice a day in a precise orbit. Each satellite sends a unique signal and orbital coordinates that it decodes then uses to calculate the exact location of that satellite based on the time needed for the signal to arrive [17]. The receiver uses that information and the triangulation process to calculate the user's location. Where areal triangulation allows calculating the absolute or relative position of points based on distance measurements using circular, triangular, and spherical geometric shapes [18]. It is used for positioning, navigation, tracking, mapping, and timing. It is relied upon in many fields by surveyors, scientists, pilots, sailors, miners, civil defense forces, and others. The system is available for civilian use free of charge all over the world from now on [19].

3. The Proposed System

The proposed application uses positioning and navigation systems to determine the coordinates of an individual or a group of individuals or vehicles during implementing a specific civilian or military task in a specific area. The Cryptobin algorithm application is used to encrypt the coordinates, and this system has achieved high performance in the results of encryption operations and achieved an increase in performance by over 20% when compared to some well-known systems in encryption.

3.1. System components

This system comprises Transmission Circuit and Receiver Circuit as shown in Figure 2.

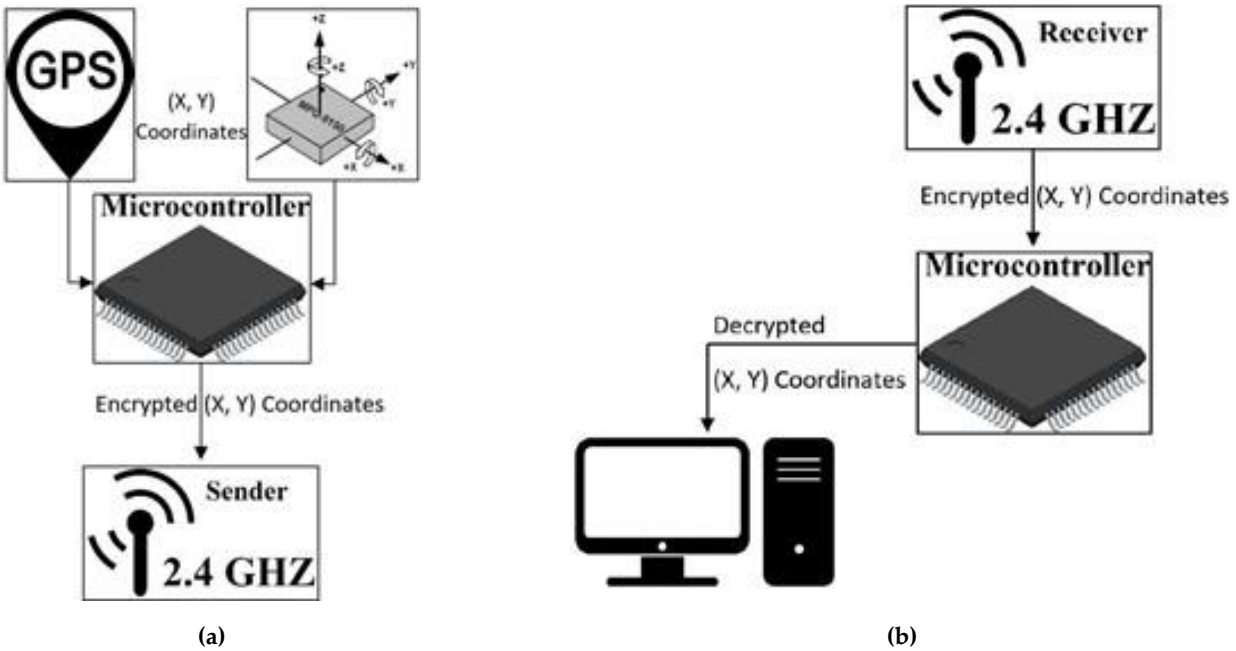

Figure 2. The transmission and the Receiver circuits. (a) The transmission Circuit (b) The Receiver Circuit.

3.2. Techniques for transferring data

This application is used to locate a person, group of people, or vehicles when performing a civilian or military mission in an area. A group of people or vehicles is launched in a specific area and their movements are followed up by receiving wireless signals from each individual or vehicle that contain the location coordinates but in an encrypted and accurate form. These received messages are encrypted using the CryptoBin algorithm, which locks the information received so that the confidentiality of the mission, as well as the safety of the personnel performing the mission, is guaranteed. The Global Positioning System (GPS) is used as a provider of information about the location coordinates of an individual or a vehicle. The encrypted information is transferred to the digital microprocessor that deals with this information and converts it from obvious information to encrypted information using the CryptoBin algorithm. The encoded information is then transmitted from the digital microprocessor to a wireless transmitter, which sends it to the major control center [20].

The major control center is the manager and controller of the entire task and manages the process and directs the people moving or taking part in the task based on the task and their locations and movements of the information received from each individual or vehicle individually. It contains a computer loaded with software that analyzes the received information and shows the mission participants on the radar screen to facilitate commanding the operation for those responsible for this operation. This system can be applied in two cases:

3.2.1. The first case

The major control center contains a computer loaded with software that analyzes the received information and shows the mission participants on the radar screen to facilitate commanding the operation for those responsible for this operation. Persons taking part in the mission move within the wireless coverage of the transmitters and receivers that are with them as shown in Figure 3 and Figure 4. Here, two options are depending on the mission area:

- If there is a coverage signal from GPS satellites, the Global Positioning System (GPS) microprocessor unit is used with the transmitter unit present with the individual or vehicle involved in the operation to send data and coordinates of the location and movements of the individual to the main command center.
- If it is not possible to get coverage from GPS satellites, the IMU, the micro-processing unit, and the transmitter unit with the person or vehicle involved in the operation are used to transmit the location data and coordinates and their movements to the major command center. Where the IMU starts the calculations and measures the angle and distance and is the starting point, in this case, the major command center.

3.2.2. The second case

The command center is within the location of the military unit or the location that is required to be secured against any intrusion, breaches, or external attacks. Here, the radio transmitter is replaced by a GSM module, which transmits the coordinates in their encrypted form through mobile networks, and they are received in the command center. This method is characterized by not being bound by a certain range of motion in it besides securing the command post in its fixed location, as shown in Figure 5.

Figure 3. The major control center.

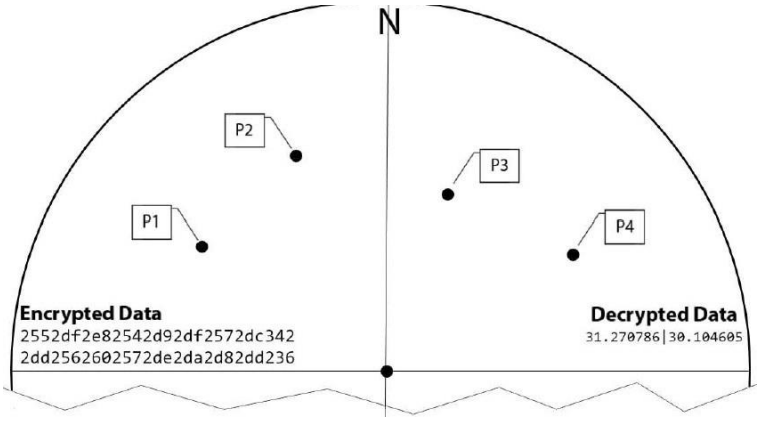

Figure 4. The radar screen inside the major control center.

The proposed system can be used as a secondary use. These devices are presented with individuals or vehicles belonging to the military unit or company in external missions away from the unit. This method is used to secure the unit and to identify persons or vehicles approaching the unit, whether it affiliated them with the unit. If it affiliated them with the unit, the Portable device would send signals showing that they are approaching their unit, making it easier to identify them.

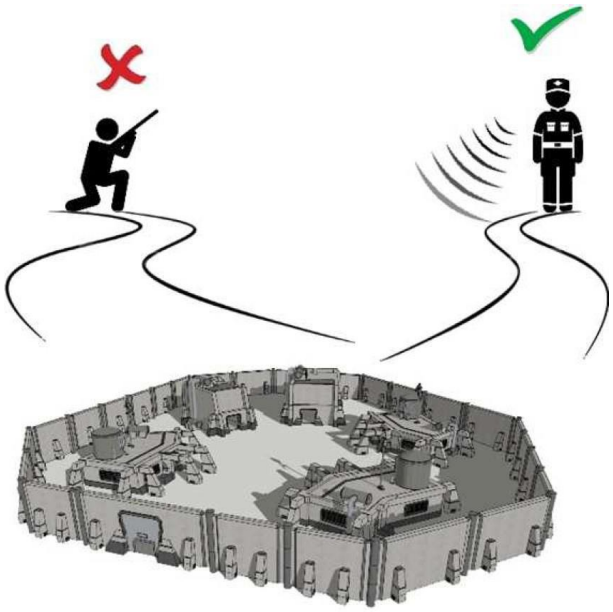

Figure 5. The identification of personnel and vehicles approach (see online version for colors).

4. Data collection and sampling

The participants in the practical experiment, 4 people out of 10 volunteers, were selected based on the physical condition of each person, as the person who can move and run easily prefers. The experiment was conducted in several climatic conditions and during different periods of the day to accurately test the efficiency of the system under different conditions. The experiment was repeated, and different results were got each time and the arithmetic mean of the received correct signals was calculated to increase the accuracy of the evaluation process.

5. Analysis of Practical Results

The experiment of sending and receiving encrypted data and decoding data was carried out using the same devices at different times and places (mountainous areas, area with buildings, area with trees) considering the following:

- The time period to complete each trial is 10 minutes.

- The transmission rate of encoded data (update of location data and coordinates) is one signal every two seconds.
- The time for each trial is 10 minutes, meaning that the data sent and received in each trial equals 10 minutes x 60 seconds / 2 seconds interval between signals = 300 encoded signals every 10 minutes.
- A specific code was added for each individual and was sent with the encrypted data to facilitate the identification of each one individually and updating his data.

Table 1. The experimental results.

Device code	No. of Signals		Received Efficiency	No. of Incorrect Signals	Incorrect Efficiency
	Sent	Received			
P 1	300	297	99.00%	3	1.00%
P 2	300	295	98.33%	5	1.67%
P 3	300	296	98.66%	4	1.34%
P 4	300	292	97.33%	8	2.67%

The results of the experiment are shown in Table 1. From Table 1, the first column in the table shows the identification code of the individual, or device used. While the second column shows the number of signals sent by the transmitter in a time of 10 minutes. The third column shows the number of valid signals received by the receiver at the time of the experiment and shows the transmission and reception efficiency, which is less than 100% because of the environmental factors surrounding the experiment which helped to lose some signals. Column 5 shows the number of received signals but has corruption during transmission or reception, which affected the percentage of valid signals. Figure 6. shows the itinerary and movement of four people or vehicles, each with a specific symbol. The proposed system automatically guesses the next movement of the moving person, ignores the incorrect signals, and returns to the correct path. The two main data are latitude and longitude.

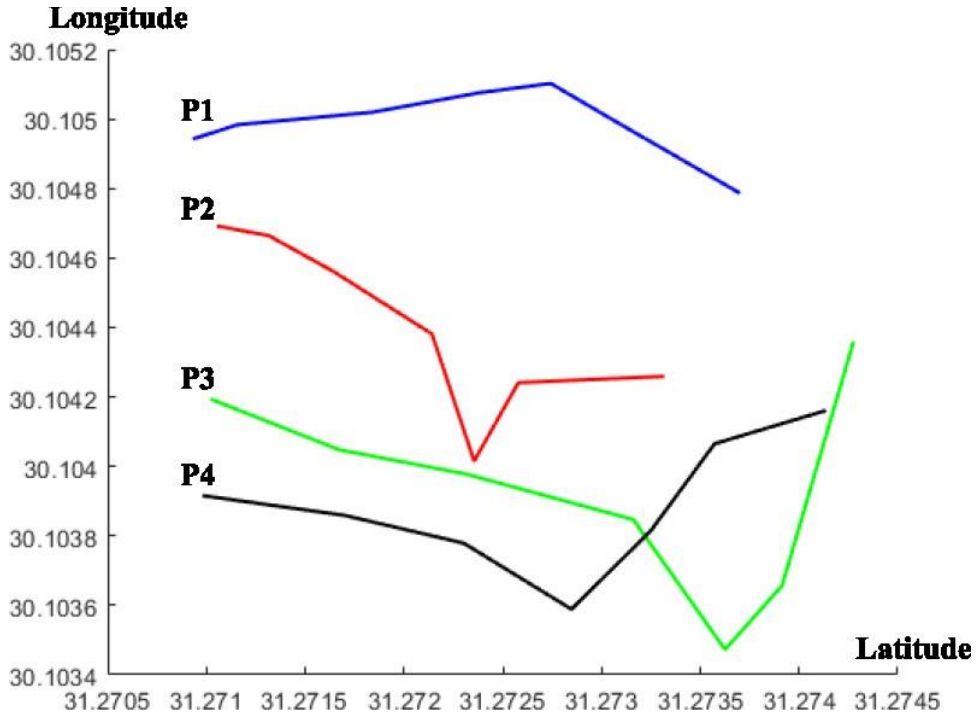

Figure 6. The path for the movement of four individuals or vehicles is identified by codes.

6. Conclusion

The application of encrypting and securing the current location information for devices was designed and implemented using a new algorithm called CryptoBin. It was used to encrypt data based on what was proven in previous research for this algorithm, its power and speed in converting information into hard-to-crack encrypted information. This application secures the locations and movements of military personnel or civilian researchers while carrying out covert missions under the command of a mobile command center. It can also be used in the secondary function of identifying personnel and vehicles approaching a military unit or civilian company to increase security and maintain the security and privacy of the facility. Several practical experiments were conducted to test the efficiency and performance of the system in different areas (residential areas, mountainous areas - areas containing trees). The proposed system had a very high success rate ranging from 97.33% to 99.00% of the successfully received signals. Increasing the system's working efficiency can be recommended by using several different navigation methods that are more accurate, and high-cost transceivers can reduce error rates. It is also possible to use over one major command and control center in different places to increase the efficiency of receiving encrypted data. Using manufacturing technology and technology to reduce the size of transmitters and receivers for easy portability and unimpeded movement.

References

1. Acar, Abbas, et al. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR)* 51.4 (2018): 1-35.
2. Wang, X.; Feng, L. and Zhao, H.; 2019. Fast image encryption algorithm based on parallel computing system. *Information Sciences*, 486, pp.340-358.
3. Li, C.; Lin, D.; Lü, J. and Hao, F.; 2018. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE multimedia*, 25(4), pp.46-56.
4. Kaur, M. and Kumar, V.; 2020. A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, 27(1), pp.15-43.
5. Özkaynak, F.; 2018. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, 92(2), pp.305-313.
6. ElTengy, A. H.; Shohieb, S. M.; A. E. TakielDeen, M. S. Ksasy. 2018 A new advanced cryptographic algorithm system for binary codes by means of mathematical equation, *ICIC Express Letters* 12 (2) p(300-308).
7. A. H. ElTengy 2021 Encryption Of Voice Calls Using CryptoBin Algorithm, *2021 International Telecommunications Conference (ITC-Egypt)*, DOI: 10.1109/ITC-Egypt52936.2021.9513963
8. Narain, S.; Ranganathan, A. and Noubir, G.; 2019, May. Security of GPS/INS based on-road location tracking systems. *In 2019 IEEE Symposium on Security and Privacy (SP)* (pp. 587-601). IEEE.
9. You, Y.; Wu, C.; 2021. Hybrid Indoor Positioning System for Pedestrians with Swinging Arms Based on Smartphone IMU and RSSI of BLE. *IEEE Transactions on Instrumentation and Measurement*, 70, pp.1-15.
10. Zhuo, C.; He, J.; Hao, R. and Ren, L.; 2021, June. Temperature Experiment and Compensation Algorithm Design for Fiber Gyros in Rapid Startup Inertial Navigation System. *In Journal of Physics: Conference Series* (Vol. 1887, No. 1, p. 012004). IOP Publishing.
11. Bieliakov, R.; 2021. Simulation of Platform-Free Inertial Navigation System of Unmanned Aerial Vehicles Based on Neural Network Algorithms. *Technology audit and production reserves*, 1(2), p.57.
12. Yazdeen, A.A.; Zeebaree, S.R.; Sadeeq, M.M.; Kak, S.F.; Ahmed, O.M.; Zebari, R.R.; 2021. FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. *Qubahan Academic Journal*, 1(2), pp.8-16.
13. Zhai, X.; Ren, Y.; Wang, L.; Zhu, T.; He, Y. and Lv, B.; 2021, January. A Review of Redundant Inertial Navigation Technology. *2021 International Conference on Computer, Control and Robotics (ICCCR)* (pp. 272-278). IEEE.
14. Kim, M.; Cho, J.; Lee, S. and Jung, Y.; 2019. IMU sensor-based hand gesture recognition for human-machine interfaces. *Sensors*, 19(18), p.3827.
15. Masri, J.; 2021. The Space Force: Constitutionality and International Legality. *U. Cent. Fla. Dep't Legal Stud. LJ*, 4, p.175.
16. Zenk, S.N.; Matthews, S.A.; Kraft, A.N. and Jones, K.K.; 2018. How many days of global positioning system (GPS) monitoring do you need to measure activity space environments in health research. *Health & place*, 51, pp.52-60.
17. Hauschild, A.; Montenbruck, O.; 2021. Precise real-time navigation of LEO satellites using GNSS broadcast ephemerides. NAVIGATION, *Journal of the Institute of Navigation*, 68(2), pp.419-432.
18. Gondelach, D.J.; Linares, R.; 2021. Real-Time Thermospheric Density Estimation via Radar and GPS Tracking Data Assimilation. *Space Weather*, 19(4), p.e2020SW002620.
19. Tian, Y.; Sui, L.; Xiao, G.; Zhao, D. and Tian, Y.; 2019. Analysis of Galileo/BDS/GPS signals and RTK performance. *GPS Solutions*, 23(2), pp.1-16.
20. Yang, X.; Stewart, K.; Tang, L.; Xie, Z. and Li, Q.; 2018. A review of GPS trajectories classification based on transportation mode. *Sensors*, 18(11), p.3741.