sciendo

Transport and Telecommunication, 2025, volume 26, no. 2, 118-132
Transport and Telecommunication Institute, Lauvas 2, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2025-0010

SPREAD SPECTRUM DATA TRANSMISSION SYSTEM FOR USER UNMANNED AERIAL VEHICLES

Somia Zellal[1], Adda Ali-Pacha[2], Mohand Lagha[3], Mohamed Krim[4]

[1]Aeronautics and Space Study Department, Coding and Information Security Laboratory (LACOSI)
Blida 1 University 1, Algeria
zellal_somia@univ-blida.dz
[2] Electronic USTO Department, Coding and Information Security Laboratory (LACOSI)
Blida 1 University, Algeria
a.alipacha@gmail.com
[3]Aeronautics and Space Study Department, Aeronautical Sciences
Blida 1 University, Algeria
laghamohand@univ-blida.dz
[4]Aeronautics and Space Study Department, Coding and Information Security Laboratory (LACOSI)
Blida 1 University, Algeria
krimusto_31@yahoo.fr

In today's world of unmanned aerial vehicle (UAV) telecommunications, data transmission is both important and delicate. Various organizations have used special techniques to ensure reliable transmission and stable communication. At this stage, we propose a method that enhances security and makes the transmission of data and image more resistant to interference and eavesdropping while improving signal reliability; this method is based on the Direct Sequence-Spread Spectrum (DS-SS) technique with a new pseudo-noise PN sequence created by merging chaotic and Barker sequences. MATLAB simulates these results for different spreading factors of the new sequence, and we evaluate the performance of the system in a user context on the Additive White Gaussian Noise (AWGN) channel. As a result, the new DS-SS technology improves the quality of data transmitted by UAVs.

Keywords: Unmanned aerial vehicles, direct sequence spread spectrum, chaotic sequence, Barker sequence, additive white Gaussian Noise

1. Introduction

Spread spectrum is becoming increasingly important due to its integrated advantages (Viterbi, 1979), such as noise immunity, and its useful uses in short-range data transceivers, which include GPS, satellite navigation systems, 3G mobile telecommunications, wireless local area networks (IEEE 802.11) (Sajid *et al*., 2019), and Unmanned Aerial Vehicles (UAV) (Anusha & Sreedhar, 2022; Krim *et al.*, 2017). Spread spectrum technology also contributes to the endless race between Terrestrial Control Station (or Ground Control Station GCS) of transmission specifications of data and the availability of drone radio frequencies in situations where spectrum is scarce and therefore a costly resource. In order to facilitate the simultaneous transmission of signals from several users in the same frequency band while maintaining a reasonably low interference rate that is tailored to the specifics of each user's communication style, each technique employs is Direct Sequence-Spread Spectrum (DS-SS). Safety is a highly significant goal in the design of a drone communication system, so how to secure a UAV and GCS communication system using the DS-SS technique based on a Barker code combined with a chaotic map sequence? Encryption systems for drones are essential to protect the data transmitted between the drone and its controller. Spread Spectrum (SS) technology was first used as an encryption scheme. The type of data transferred, the communication technology used, and the controller used must all be taken into consideration when designing the DS-SS system. By understanding the basic principles of spread spectrum systems for UAV communications, users can ensure that their data is secure.

A number of research studies have examined the technologies and strategies used in drone communications systems to guarantee data security by protecting it from unauthorized access and ensuring that only authorized users can access the data, and to reduce the size of data transferred or stored by finding and removing duplicate evidence or data patterns. However, data spreading and cryptography are closely related and useful, as they can be used independently of each other. In addition, to ensure the reliability of

drone communication systems in the air, DS-SS can transmit and control precise data with a minimum of collisions. DS-SS features, such as multiple access and anti-jamming, are useful for obtaining accurate data with a minimum of collisions, the main advantage of Direct Sequence-Spread Spectrum is that security is enhanced without any additional hardware. But when the amount of data increases, DS-SS may not be sufficient to transmit and control the data and also the acquisition time is too long with the serial search system because of this DS-SS, the system is slow. So, the sequence that is created by the output of the PN sequence generator must have a high throughput. So, because of this length of this sequence must be long enough to make the sequence truly random. To solve this problem, we propose a new data transmission technique based on the modified DS-SS technique. The study presents a hybrid approach of combining a pseudo-noise (PN) Barker code with a chaotic map sequence, this combination is used to spread the DS-SS spectrum, with the new technique of spreading the spectrum, the information security will be much stronger than that of the existing DS-SS technique and the anti-jamming effect will also be improved. The main objective of this research project is to provide a secure communication protocol that will enable safe missions between drones and the Terrestrial Control Station.

This research study uses MATLAB simulations to analyse the behaviour of the signal as it is transmitted of data and images from the transmitter to the receiver via an Additive white Gaussian noise (AWGN) channel. We use the direct sequence-spread spectrum method to spread this signal. This is done using pseudo-noise sequences PN. Our suggestion is to combine the Barker sequence and the Chaotic map sequence.

There are six sections in this research study. An introduction is given in the first section, followed by a description of the drone communication system in the second section. Section three is devoted to the proposed method based on a new Code of DS-SS technique that enhances the quality of data and image transmission. Simulation and analysis of the results with the all-important static test (BER, NPCR, UACI, IE, CCA, NA and PSNR) measurements of the proposed system are then presented in Section 4. In Section 5, we then go over the advantages of the suggested system. Conclusions are in Section 6 at finally.

2. Communication system between UAVs and GCS

Drones are frequently used for surveillance, broadcasting real-time information of the area they are flying over. They come in handy in industrial districts, as they have the ability to reach high-risk areas requiring observation. They are capable of flying over high-risk areas, which would otherwise be unsafe for employees, in order to obtain information. In addition, drones offer greater flexibility, have an extended field of vision and are capable of tracking moving elements. Drone broadcasting capability is also limited by factors such as limited power and flight autonomy. The use of drones for surveillance is therefore reserved for very specific purposes. Since drone data contain sensitive information, it is imperative to protect them before transmitting them via wireless communication technologies. The structure of a safe surveillance drone for a monitored area is shown in Figure 1. Drones are useful for monitoring dangerous locations because they are full of obstacles, risks, and problems. The framework consists of a communication link, a GCS, and a drone. An attacker who was able to listen in on the unsecured connection may launch a man-in-the-middle assault. Therefore, a spreading algorithm is needed to spread data transmitted by the drone.

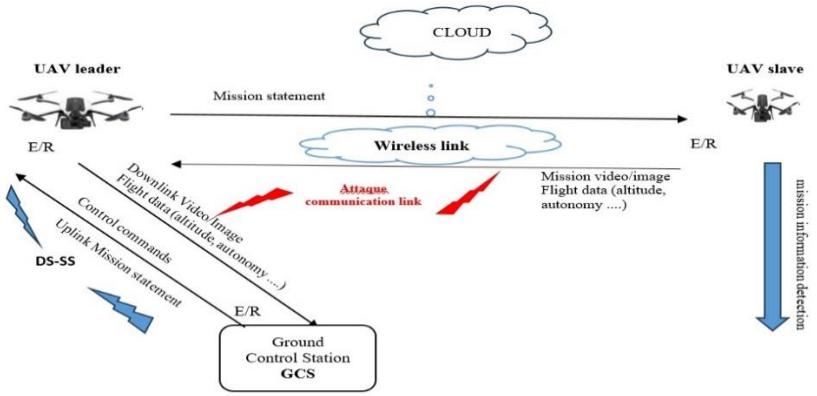


Figure 1. The UAV communication system and the secure UAV control environment (Alawida *et al.*, 2023; 13. Ismael and Al-Ta'i, 2021)

The proposed system's basic block diagram is depicted in Figure 1, which also shows three primary parts of the UAV communication systems: A Terrestrial Control Station for flight management; a UAV-GCS communication link (uplink and downlink) that enables the GCS to send control to the UAV and receive flight data downlinked; and an Unmanned Aircraft Vehicle (UAV) leader and slave that collects the requested data.

As drones exchange information over a wireless channel, they are exposed to threats and cyber-attacks (Faraji-Biregani & Fotohi, 2021), including network layer attacks such as:

- The jamming attack causes service disruption by transmitting jamming signals.
- The impersonate attack is an attack that uses a false identity, such as a personal identity, to gain unauthorised access to a system.
- The Replay and Eavesdropping attacks share the same characteristics; although the Replay and Eavesdropping attacks barely change location, they can still be affected by connected drones. It is therefore important to have real-time data updates without any delay. Time is crucial both for the transmission of data and to prevent replay attacks, which can lead to failures in the authentication process for legitimate drones.

2.1. Unmanned Aerial Vehicles

Unmanned Aerial Vehicles (UAVs), also known as drones by the International Civil Aviation Organization (ICAO), are aircraft that are installed with sensors, an automatic controller, data processing units, and communication systems that enable them to fly autonomously without the need for a human pilot (Cai *et al.*, 2011). Drones are becoming increasingly important in many fields. Because of their versatility and ease of deployment, they can be utilized for a variety of jobs, such as delivery services, animal monitoring, surveillance, and even conflict situations. The Command-and-Control connection technology is what enables the drone's seamless functioning and such adaptability : The command link is the channel of communication that connects an unmanned aerial vehicle to its remote controller.

2.2. Communication links between GCS&UAV

There are two communication links between UAV and GCS: the uplink connects the control station to the UAV, and the downlink connects the UAV to the control station. The information transmitted through this channel pertains to the management of the aircraft, regardless of whether it is produced by the operator giving instructions or gathered by the drone using its on board sensors while it is in flight. A UAV uses a data connection that operates in the 150 MHz to 1.5 GHz frequency range to transfer data between the vehicle and the ground station. However, approximately 90% of the frequency range is used by 2.4GHz and 5.8GHz (Atoev *et al.*, 2018), which determines the communication link between transmitter and receiver with modulation type are: FH-SS (Frequency Hopping-Spread Spectrum) or DS-SS (Direct Sequence-Spread Spectrum), and data transmission is generally carried out by telecommunications systems in this study the technic DS-SS modulation system is important in communication UAV and has been recommended (Stojanovic *et al.*, 2024). This DS-SS is due to the need for high reliability and resistance to interference. The communication approach of the proposed system is based on the new DS-SS technique; for the reliable communication between the GCS and the UAV leader, this protocol helps the control management to transmit the mission orders to the UAV leader, the second communication is used to accomplish the mission by transmitting the mission orders to the slave for this purpose, then broadcasting the results to the leader, then the leader transmits this data to the GCS, as illustrated in Figure 1.

2.3. The Terrestrial Control Station

The purpose of the terrestrial control station (or Ground Control Station GCS) is to direct and/or observe the drone's flight and mission. The airplane has a receiver that picks up signals from the controller, and the controller has a radio transmitter. In a way that is recognized as state-of-the-art, the received signals in turn regulate the functioning of digital servomotors to control the aircraft's flight. DS-SS is the digital data stream used by most of these radio transmitters and receivers. The native band signal is produced at the receiving end of a direct sequence system by spreading the spread spectrum signal (Atoev *et al.*, 2018). The drone is controlled by commands sent from the base station, commands such as "Landing", "Take-off", "Gain altitude" will directly affect how quickly the propellers rotate; the control of the drone is achieved by individually controlling the rotation speed of its propellers driven by motors. We can therefore conclude that the "Control Drone" case includes the "Control Motors" case (DMS, 2010). Through a wireless link, a

GCS and the drone can communicate and coordinate flight operations, give and receive commands, and monitor network traffic in real time (Kristanto & Indriyanto, 2023). The working principle of the GCS-UAV communication includes the following steps:

- Step 1: The GCS transmitter sends flight control data or mission commands to the UAV receiver for data acquisition.
- Step 2: The UAV receiver receives the acquisition data from the UAV's sensors and combines the data. Processing, dissemination and distribution (Anusha & Sreedhar, 2022).
- Step 3: Broadcast information distribution and storage. The ground server is used to store data and voice communications between the UAV commander who coordinates the mission.
- Step 4: Scheduling of air traffic information between the air traffic information and the drone's area of operation.
- Step 5: Analysis of the data and transmission of commands with the human-machine interface.

The station machine control interface with human to monitor the operating conditions of mission the telemetry information, sensor information. And to provide information in the form of communication network conditions, both via radio frequency and Internet networks.

3. Spreading technique of data transmission between UAV and GCS

3.1. Direct Sequence-Spread Spectrum (DS-SS)

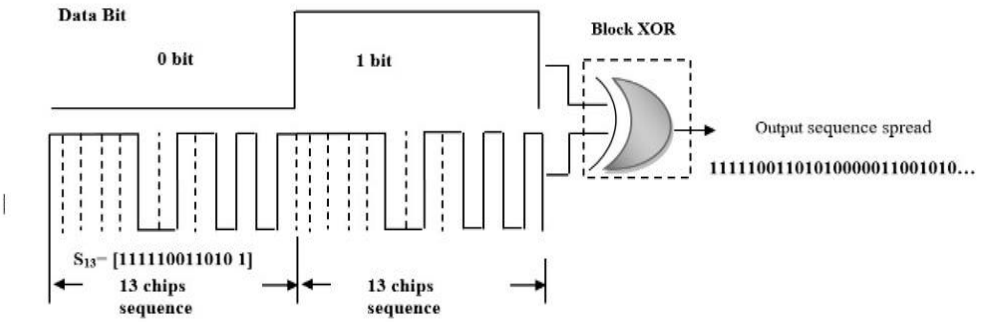
The modulation method used in telecommunications to lessen signal interference during transmission is called Direct Sequence-Spread Spectrum (DS-SS). This approach, known as spread spectrum, creates a signal with a broader frequency band. Signals transmitted over broadband are less vulnerable to inadvertent interference and data loss or corruption. The information bandwidth is the original signal's bandwidth prior to frequency spreading. The information bandwidth is recovered at the receiver after the signal is subjected to DS-SS modulation suppression or dispreading. In DS-SS transmissions, a pseudo-noise spreading sequence with a bit rate significantly higher than the original data rate multiplies the data signal. The original data is reconstructed by multiplying the broadcast signal by the same spreading sequence, which is known at the receiver, and the resultant transmitted signal looks like banded white noise. This procedure is equivalent to dispreading. Shannon developed encryption systems for military use in 1949 using Spread-Spectrum (SS) techniques (Scholtz, 1977). Then, as a new high-tech created by Qin (2019) and Scholtz (1982). The benefit of the spread spectrum is that it uses pseudo-noise (PN) to spread over a bandwidth that is far larger than the data rate. Shannon-theorem of spread spectrum is expressed by the following Formula 1 (Glaviaux ,1990):

$$C = B.log_2(1 + SNR), \quad (1)$$

where C is the channel capacity, B is the channel band width and SNR is the Signal-TO-Noise Ratio.

3.2. Principle of operation the UAV communication system based on DS-SS technology

Each data bit is transformed into multiple bits known as "chips" by the pseudo-noise (PN) sequence; the steps in the DS-SS process are illustrated below. A signal that occupies a larger band than the initial narrow-band signal is produced by this method, called chipping (see Figure 2). This pseudo-noise is used to chip the data signal, which is then disseminated across a large frequency range. Pseudo-noise synchronization is accomplished at the receiver by multiplying the broadband signal that was received by the same PN sequence that was used for transmission. To use the precise pseudo-noise which guarantees exact recovery of the original data stream, the transmitter and receiver must be synchronized. The original data, which has been shielded from disruption by spreading, is recovered by the receiver by demodulating the signal. This spreading approach, which is based on the PN code generated by a pseudo-random generator Barker sequence, joins the user's binary data to the spreading code sequence with a chip to separate it from the smallest unit of subscriber information with method or exclusive (XOR). The high-speed {0 and 1} sequence makes up the spreading code. Barker code, M-sequence, gold code, Walsh code, and chaotic code are examples of PN spreading codes. In this study, the PN is based on the Barker and chaotic sequences. The concept of distributing an information frame by the Barker sequence of length equal to 13 chips (or $L_{\text{Barker code}}$=13) mixed with the data bits by the logical operator XOR is demonstrated in the following example (Figure 2). The DS-SS technology's working principle is depicted in Figure 3.



*F*igure 2. Spreading code or spreading sequence when the length of the Barker code is equal to 13 chips ($L_{Barker\ code}$= 13) combined with sequence data a_k= {0,1} bits. Each data bit in the message includes the full PN sequence (Krim *et al.*, 2017)

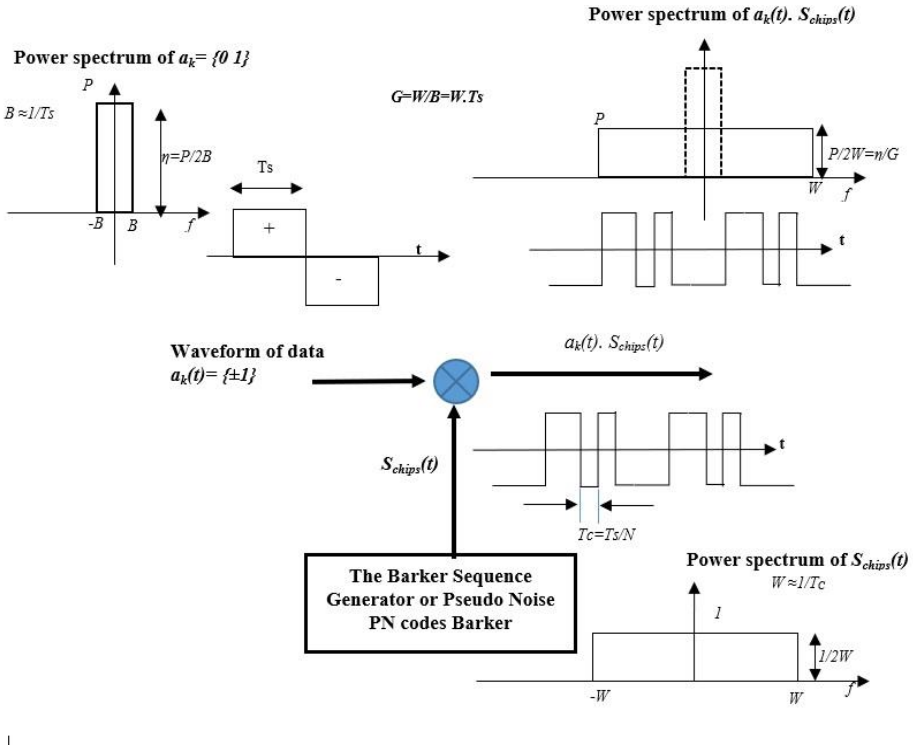


Figure 3. Scheme the principle of operation the DS-SS technology

Typically, spectrum spreading (SS) is based on a pseudo-random or pseudo-noise (PN) sequence generated by a pseudo random generator or Barker code, to convert the narrowband signal into a broadband signal by means of a pseudo-noise (PN) multiplication is the data signal. The receiver obtains the initial signal by correlating the received signal with a repetition of this sequence, as shown in Figure 3. This Figure represents the principle of technic operation DS-SS as provides the spreading data such as each bit is transmitted using or exclusive logic operation (XOR) with a binary sequence of the Barker PN code of length L. The output of the spread information is obtained using a spreading technique based on a small sequence of chips, such as the module with the Binary Phase-Shift Key (PBSK) or the non-return to zero (NRZ) modulation.

3.3. Using DSSS to enhance the quality of data transmission in a drone communication system

Figure 4 shows how the spectrum can be spread and despread in the UAV transmitter and GCS receiver, respectively.

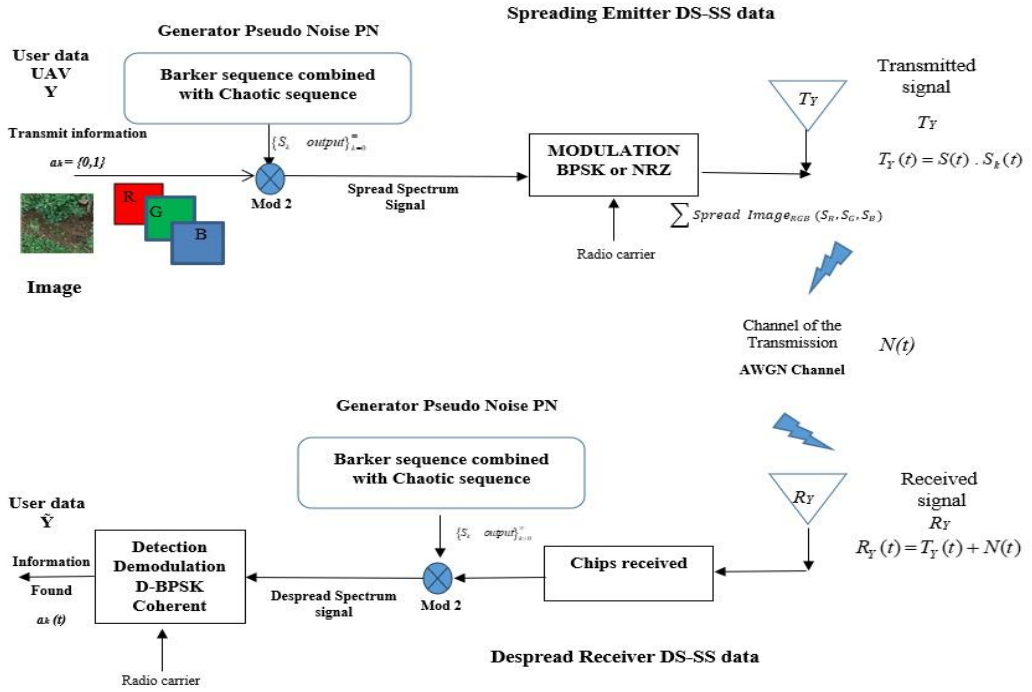


Figure 4. DS-SS data/image spreading and dispreading with AWGN channel and Pseudo Noise (PN) code synchronization

The process shown in Figure 4 is the spreading of a transmitter and the dispreading of the receiver of the DS-SS system block; this process consists of two points such as spreading with a pseudo-noise code and dispreading mechanisms using the same pseudo-noise.

Spreading data with a pseudo-noise sequence at the transmitter, as shown in Figure 4. The data is then modulated into symbols using Binary Phase Shift Keying (BPSK) modulation with a sequence amplitude of $a_k = \{\pm 1\}$. Each information bit is initially repeated 'N' times to create the DS-SS system. The repeated information bits use a spreading factor (SF) using a pseudo-noise (or $S_{chips}(t)$) sequence. The standard mathematical equation for spreading with a larger capacity band and transmit the signal $T_Y(t)$ can be written as Formula 2 (Krim *et al.*, 2017):

$$T_Y(t) = S(t) \,.\, S_k(t), \tag{2}$$

where $T_Y(t)$ is the spreading signal transmitted, $S(t)$ is the transmit signal, $S_k(t)$ spreading factor (or SF) using PN code.

Dispreading mechanisms using a pseudo-noise sequence are like spreading processes, but in the opposite direction. The received spread signal $R_Y(t)$ by an AWGN channel is:

$$R_Y = T_Y(t) + N(t), \tag{3}$$

where $R_Y(t)$ is the received spread signal and $N(t)$ is the Gaussian White Noise.

3.4. Choosing binary codes

In a dynamic system, Barker sequences and chaotic sequence represent persistent random behaviours that respond effectively to changes in initial conditions. In this section, we briefly introduce the Barker code, and the chaotic map used to spread the suggested system by DS-SS technique.

3.4.1. The Barker sequences

The Barker sequences is a finite sequence of numerical values with a sequence length *N* bit a perfect autocorrelation property has great importance for data security. They are particularly well suited to large-scale applications involving drone communication systems (Anusha & Sreedhar, 2022). Barker sequences offer several advantages over other PN sequences (Jain & Ogale, 2018; Anil Kumar *et al.*, 2007). The block

architecture of the Barker sequence generator is a variant with a logical XOR arithmetic unit of sequence length *X* of order *N* bits (X_N). They are used in practice for spread spectrum (SS) and pulse compression binary sequences (Anil Kumar *et al.*,2007; Kiranmai & Rajesh Kumar, 2014). Figure 5 illustrates the schematic architecture of the Barker sequence generator. And Table 1 shows the Barker sequence generator produces difference codes of length *n bits (*or $L_{Barker\ code}$*=n bits).*

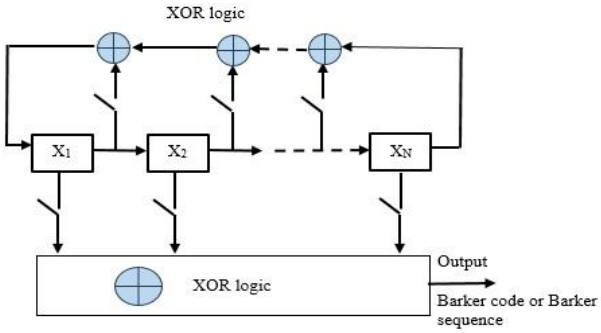


Figure 5. The scheme block of Barker sequence generator

Table 1. The Barker Sequence S_n with the Length Barker Sequence *L* equal *n bits* (Mitra, 2007; Balaji *et al.*, 2012)

The Length Barker sequence n (bits)	**The Barker sequence S_n**
$L_{Barker\ Code}$ =2	1st : S_2= [10], 2nd : S_2= [11]
$L_{Barker\ Code}$ =3	S_3= [110]
$L_{Barker\ Code}$ =4	1st : S_4= [1110], 2nd : S_4= [1101]
$L_{Barker\ Code}$ =5	S_5= [11101]
$L_{Barker\ Code}$ =7	S_7= [1110010]
$L_{Barker\ Code}$ =11	S_{11}= [11100010010]
$L_{Barker\ Code}$ =13	S_{13}= [111110011010 1]

The length Barker sequence ($L_{Barker\ code}$ =11) and ($L_{Barker\ code}$ = 13) are used in DS-SS because of their low autocorrelation properties. The Autocorrelation Code Function of the Barker sequence, as defined by (Mitra, 2007; Alamgir *et al.*, 2012; Golomb & Scholtz, 1965):

$$C_k\ (t) = \sum_{j=1}^{N-k} X_j\ X_{j+k}, \tag{4}$$

where $C_k(t)$ *is* the Autocorrelation Code Function of length *N bits*, (X_j) is an individual code symbol taking values {±1}, for $0 < j < N$ and the adjacent symbols are assumed to be zero.

Figure 6 represents scheme of the propriety Autocorrelation Code Function (ACF).

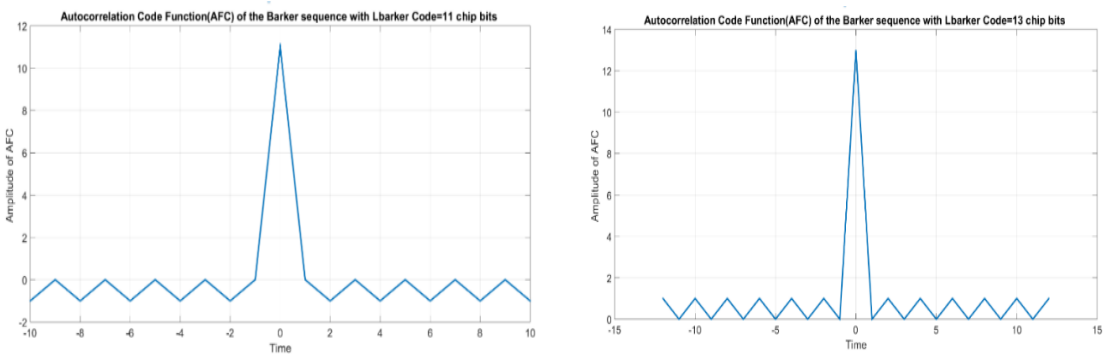


Figure 6. Scheme of the propriety Autocorrelation Code Function of Barker sequence, (a) $L_{Barker\ Code}$=11chips in the (Left) and (b) $L_{Barker\ Code}$=13chips in the (Right)

We may see the propriety ACF of the Barker sequence from this figure that was obtained using MATLAB. These findings demonstrated the Barker sequence's good appropriateness of orthogonality.

3.4.2. The chaotic sequence generator bits

Discrete-time dynamical systems are a particular type of non-linear dynamical systems generally described as an iterative map by the state Formula 5 (Lynch, 2014):

$$x_{n+1} = M(x_n) \qquad and \quad n = 0,1,2,...N, \tag{5}$$

where n denotes the discrete time, x_n is the state of the system at time n, and x_{n+1} denotes the next state.

The used discrete chaotic map system, as shown in formula (6) (Xue *et al.*, 2013) below:

$$x_{n+1} = f_{\lambda,K}(x_n) = \lambda.x_n - x_n^2 / K, \tag{6}$$

where $\lambda=3.99\approx4$, the value of the parameter K is determined at any unbounded non-negative value.

The sequence binary of the chaotic map system as defined by method proposed. This principle consists of the following phases in MATLAB:

- First Phase: The sequence $\{x_n\}$ is generated by the chaotic map logistics method, which must be amplified by a scale factor (10^2) and round to integer sub-sequence, the following Formula 7:

$$G_k(x_n) = \mathrm{mod}\left((roundn(\lfloor f_{\lambda,K}(x_n) \quad, n \rfloor, -n) * 10^2, 2)\right), \tag{7}$$

with n number of places, $\lfloor . \rfloor$: Whole number.

- Second Phase: Encoded sequence chaotic map with sequence binary $G_k(x_n)$ given by Formula 8:

$$G_k(x_n) = \begin{cases} 1 & if \quad G_k(x_n) \quad pair \\ 0 & if \quad G_k(x_n) \quad old \end{cases} \quad and \quad k \in [0,N], \quad N: Iterations, \tag{8}$$

3.4.3. A new random bit generator proposed

In this research, a new algorithm was used to create a new pseudo-random or pseudo-noise (PN). The block XOR operation is a combination between of the chaotic sequence and the Barker sequence is used to generate this new pseudo-noise (PN) generator. Depending on the starting values (λ, K, x_0) a chaotic sequence is generated, and a set of secret keys is created by combining techniques. The suggested generator configuration illustrated in Figure 7. The chaotic map generates chaotic real numbers defined with a specific margin, based on the initial status chosen. These real numbers are subsequently converted into binary numbers, which are used as a chaotic pseudo-noise bit sequence. The second generator, the Barker code or Barker sequence used to generate a pseudo-noise (PN) with length of n bits.

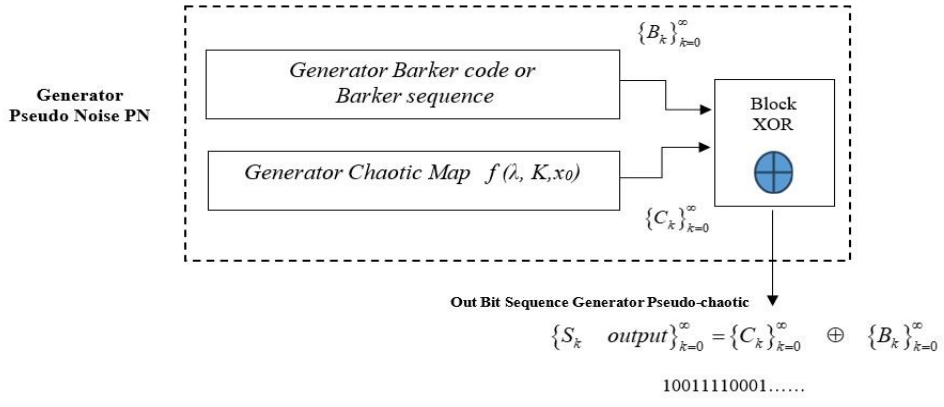


Figure 7. Pseudo chaotic bit sequence generator (proposed method)

The pseudo-noise proposed (S_k *output)* illustrated in Figure 7 is defined by method bitwise between bit sequence chaotic map (C_k) and out bit Barker sequence (B_k), that is given by Formula 9:

$$\{S_k \quad output\}_{k=0}^{\infty} = \{C_k\}_{k=0}^{\infty} \quad \oplus \quad \{B_k\}_{k=0}^{\infty}, \tag{9}$$

4. The simulation results using MATLAB

4.1. Measures of evaluation

4.1.1. Bit Error Rate (BER)

The Bit Error Rate is given by Formula 10 and in MATLAB, we calculate it by Formula 11

$$BER = (Bits \text{ in } Error) / (Total\ bits\ received). \tag{10}$$

$$BER = Sum\left(\frac{Abs(E_{err})}{N}\right), \tag{11}$$

where *Sum* is the addition function and *N* is the length bits of the pseudo-noise (PN) suggested, and *Abs* function is used to determine the absolute error vector (E_{err}).

The error vector is also performed directly on a channel AWGN, we calculate it using Formula 12:

$$E_{err} = Y_{Raw\ data} - \hat{Y}_{detection}, \tag{12}$$

where $Y_{Raw\ data}$ the transmitted binary data or binary data stream and $\tilde{Y}_{detection}$ the received binary data.

4.1.2. Number of Pixels Change Rate (NPCR)

The Number of Pixels Change Rate is presented in Zia *et al.* (2022) defined by Formula 13:

$$NPCR_{R,G,B} = \frac{\sum_{i,j} D_{R,G,B}}{N} * 100\%, \tag{13}$$

where (N) is the total number of pixels in the image and $D_{R,G,B}(i,j)$ defined using Formula 14:

$$D_{R,G,B}(i,j) = \begin{cases} 1 & C_{R,G,B}(i,j) = C'_{R,G,B}(i,j) \\ 0 & C_{R,G,B}(i,j) \neq C'_{R,G,B}(i,j) \end{cases}, \tag{14}$$

where $C_{R,G,B}(i,j)$ and $C'_{R,G,B}(i,j)$ are the values of the corresponding color component Red (R), Green (G) or Blue (B) in the two encoded images, respectively**.**

4.1.3. Unified Average Changing Intensity (UACI)

The Unified Average Changing Intensity mentioned in Zia *et al.*, (2022) is defined as Formula 15:

$$UACI_{R,G,B} = \frac{1}{N}\left(\sum_{i,j} \frac{\left|C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)\right|}{2^{i_{R,G,B}}-1}\right) * 100\%, \tag{15}$$

4.1.4. Information Entropy Analysis (IE)

The Entropy Information theory is mentioned in Li (1991), $H_{R,G,B}(X)$ calculated by Formula 16:

$$H_{R,G,B}(X) = -\sum_{i=0}^{2^M-1} P_{R,G,B}(x_i) \log_2 (P_{R,G,B}(x_i)), \tag{16}$$

where $P_{R,G,B}(x_i)$ represents the probability of symbol (x_i), and the entropy is expressed in bits.

4.1.5. Correlative Coefficient analysis (CCA)

The Correlative Coefficient Analysis (horizontally, diagonal and vertically) is used to establish the correspondence between the pixels located at the sides of the original image and the spread image.
Its symbols by r_{xy} are defined as Formula 17:

$$r_{xy} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij},\bar{x})(y_{ij},\bar{y})}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij},\bar{x})^2(y_{ij},\bar{y})^2}}, \quad (17)$$

where (x, y) are the values of a pair of randomized images, M is the number of randomized pairs.

4.1.6. Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio can be used to evaluate a speeding image shown in El-Iskandarani *et al.* (2008). It is defined as Formula 18:

$$PSNR = 10\ \log_{10}\frac{M\,.\,N\,.\,255^2}{\sum_{I=1}^{M}\sum_{j=1}^{N}(P(i\,,\,j)-C(i\,,\,j))^2}, \quad (18)$$

where M is the width and N is the height of digital image. $P(i, j)$ is pixel value of the represents the matrix data of our original image $P(i, j)$ and $C(i, j)$ is pixel value represents the matrix data of our degraded image in question of the spreading image or its noisy approximation.

4.2. Results

The simulation results are divided into two distinct parts: the first part concerns the spreading of binary data by the proposed DS-SS, while the second part concerns the spreading of images by the proposed DS-SS.

4.2.1. DS-SS of binary random by the proposed method with AWGN channel

The drone's wireless communication system and the local positioning system or time-of-flight-based proximity sensor will have to operate in the channel Additive White Gaussian Noise (AWGN) type, which is simulated in this work as a DS-SS system, the work can be performed using MATLAB. The results of binary random acquired by drone model spreading by the DS-SS system proposed in Unmanned Aerial Vehicle (UAV) communication via the AWGN channel with Binary Phase Shift Keying BPSK modulation are shown in Figure 8.

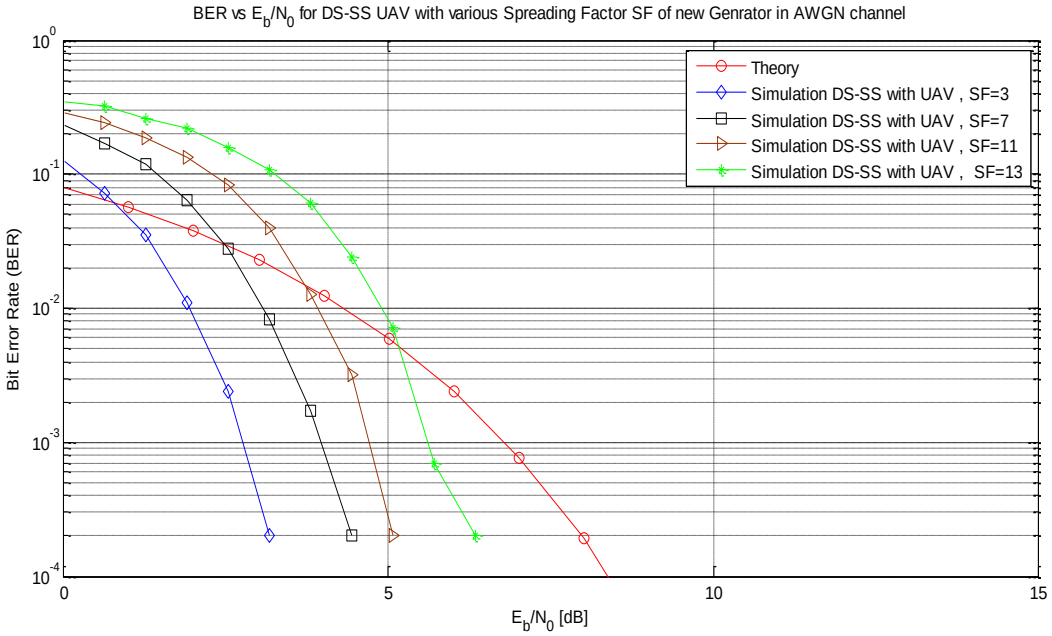


Figure 8. The Performance of data user of transmission in a UAV communication system by DS-SS in AWGN channel. With Barker code 11 chips & chaotic map parameter as K=15000, λ=4, with various Spreading Factor *SF= {3, 7, 11, 13}* of new generator

The spreading code using XOR is the data bit spread factor, with data input parameters: the chaotic input parameters: $x_0=0.1$, $K=15000$, length of chaotic map is $L_{Chaotic}$ = N bits and the Barker sequence with the following parameters: the length of the Barker sequence as $L_{Barker\ code}$ are{3, 7, 11, 13}. Figure 8 shows result the user's data transmission performance in a UAV communication system via DS-SS on a channel AWGN, in this channel with Signal-to-Noise Ratio *SNR* [0 to15] dB of the signal and add noise to this signal in order to calculate the BER, using MATLAB. Figure 8 shows the results of DS-SS data spread simulated in MATLAB and illustrates that using the new code achieves the following gains of around {4.83, 3.56, 2.93, 1.66} dB for the different spreading factors SF= {3, 7, 11, 13} respectively corresponds to BER=2.10^{-4}. Figure 8 shows the minimum error rate for each SF. Using SF 13 gives a performance closer to theory at BER =2.10^{-4}, with a gain of 1.66 db. The graphics work optimally thanks to a code that enables the information to be extended and transmitted safely in a drone communication system via DS-SS in an AWGN channel. Using DS-SS and the new spreading code (Chaos & Barker) via an AWGN channel reveals superior data transmission performance to DS-SS without chaos. Our simulation results show that data transmission in an AWGN channel using the DS-SS system, and the new spreading code outperforms the DS-SS system in Anusha & Sreedhar (2022). The proposed DS-SS system outperforms the DS-SS system with the Barker sequence alone.

4.2.2. DS-SS of the binary image using the suggested method

We therefore adjusted the input signal by introducing a (M*N) image of the system with a note about the system's response to this image. The following values represent the system results with the AWGN channel, we change the SNR *(-15dB to 15dB),* Test images taken by images with (256*256) pixels;1st image taken by UAV in (Santos & Gebler, 2021) and the 2nd image peppers. Image spreading is designed using the proposed algorithmic system, in which the new pseudo-noise sequence generated by the proposed method is used to spread the RGB image of (M*N) pixels. The spreading protocol illustrated in Figure 4 is described in Krim *et al.* (2018). We choose the image size M=N=256 pixels. Color images are represented by three distinct colors: Red R, Green G and Blue B. Then, the spreading of each color outside a color blending step is used to blend data of different colors and to provide an additional aspect of confusion in the resulting accelerated image. Each pixel is represented in each color by a byte, and so we gather them one by one from one color to another using the following mechanism: the first byte is blue, the second is red and the third is green. Finally, the Signal transmission is additive via the AWGN channel.

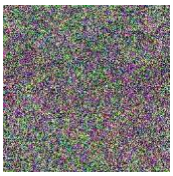
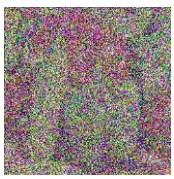
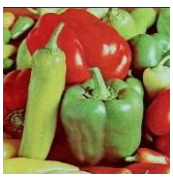
The signal obtained synchronously via PN is defined by in Formulas 2 and 19:

$$S_{RGB} = \sum \quad Spread \quad image_{RGB}\,(S_R\ ,\ \ S_G\ ,S_B), \tag{19}$$

where (S_R), (S_B) and (S_G) is the first (Red, Green, Blue respectively) byte is multiplied by the new pseudo-noise sequence, resulting in the first spread of the 8 chips.

Table 2 shows the performance compared and analysis des simulation result for first (1st) image taken by UAV and second (2nd) image peppers with method proposed, the value of the results presented in the following Tables:

Table 2. Spread of the two test images by different SNR values

Original Image	Spread Image (SNR=-15)	Spread Image (SNR=15)	Despread Image
 1st Image taken by UAV			
 2nd image Ppeppers			

Tables 3, 4, 5 and 6 show the performance compared with execution: Entropy, NPCR & UACI, Correlation Coefficient and PSNR Analysis of Images (UAV, Peppers)

Test results for correlation coefficient for two images (UAV, Peppers) Horizontally, Diagonal and Vertically, adjacent pixels are shown in Figure 9 and Table 5:

Table 3. Entropy analysis of images (UAV, Peppers)

Entropy Analysis Of Images					
Image taken by UAV			**Peppers**		
Original image	**Spread Image SNR= -15**	**Spread Image SNR=15**	**Original Image**	**Spread Image SNR= -15**	**Spread Image SNR=15**
7.1085	7.7110	7.1665	7.7300	7.6869	7.9165

Table 4. Comparison of NPCR & UACI analysis values for various spreading Algorithm proposed of Images (UAV, Peppers)

Spread image taken by UAV			**Spread Peppers**	
SNR	**SNR= -15**	**SNR=15**	**SNR= -15**	**SNR=15**
NPCR	99.3235	98.1084	99.3378	98.1084
UACI	29.3120	8.9730	30.2829	11.6978

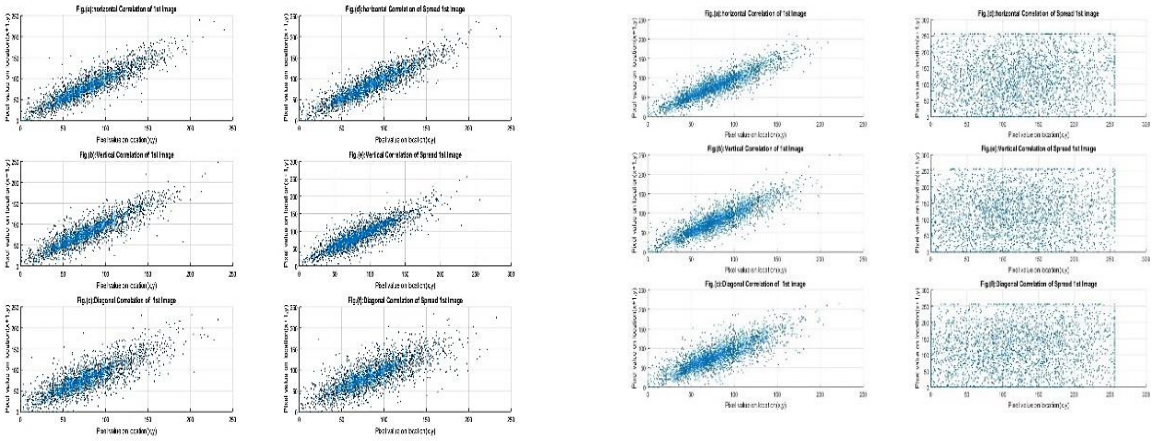


Figure 9. Results for correlation coefficient horizontally, diagonal and vertically, adjacent pixels, (a) (Left) Correlation coefficient of plain image taken by UAV, (b) (Right) Correlation coefficient of spread image taken by UAV

Table 5. Correlation coefficient for various test of images (UAV, Peppers)

Correlation Coefficient of Images						
Position	**Image taken by UAV**			**Peppers**		
	Original Image	**Spread Image SNR= -15**	**Spread Image SNR=15**	**Original Image**	**Spread Image SNR= -15**	**Spread Image SNR=15**
Horizontal	0.877060	0.019352	0.870085	0.942994	0.019352	0.931597
Vertical	0.839591	0.01527	0.833175	0.944197	0.10527	0.934507
Diagonal	0.764130	0.29702	0.754204	0.902651	0.029702	0.887566

Table 6. Comparison of PSNR analysis values for various spreading algorithm proposed test of images (UAV, Peppers)

Spread image taken by UAV			**Spread peppers**	
SNR	**SNR= -15**	**SNR=15**	**SNR= -15**	**SNR=15**
PSNR	25.26	25.58	25.41	25.42

4.3. Analysis of results

Table 2 shows the spread of two different images by our algorithm with two different SNR values. The *SNR*=-15*dB* value indicates that the signal is mixed with noise to achieve an image spread close to image cryptography, while the *SNR*=15*dB* value means that the signal is greater than the noise, resulting

in a spread close to the original image. The values in the 3rd table are within the entropy interval [0 to 8] and near the value 8, That is close to the values obtained by cryptography in Vishwas & Sanjeev Kunte (2024), which shows that our system has a cryptographic characteristic. For Table 3, the NPCR and UACI of the clear image are calculated and presented in Table.4. The aim of this analysis is to show that a small change in the image clearly introduces a major change in the spread image, and the results prove that our algorithm is resistant to attack. Figure 9 shows the correlation for a 256*256 drone image. Among them, (a) the vertical correlation, (b) the horizontal correlation, (c) the diagonal correlation of the original image and (c), (d), (e) represent the spread image correlations. Formula (15) is used to study the correlation between two vertically adjacent pixels and two horizontally adjacent pixels in an image. two horizontally adjacent pixels in an image 3000 pairs of two adjacent pixels (in horizontal, and vertical direction) from plain-image and spread-image were randomly selected. The results show that the proposed method randomizes pixels very satisfactorily. And from the last table we obtained an average PSNR value of 25, these results make our system more reliable and resistant to attack.

5. Benefits of the proposed system

The Direct Sequence Spread Spectrum (DS-SS) technique is frequently used in wireless communication technologies for UAVs. The use of pseudo-random codes gives DS-SS a protective characteristic. The system offers many advantages in terms of the information provided:

- Since only the transmitter and the receiver know the PN pseudo-noise sequence, it is difficult for unauthorized individuals to capture or compromise the signal without the right code, thus ensuring the confidentiality of data exchanges.
- Inserting a chaotic sequence into the pseudo-random sequence improves the security of the communication system.
- Signal quality optimized by wide-band broadcasting, which reduces the effects of interference from other signals in the same band thanks to unique pseudo-noise sequences, making it more difficult for unauthorized persons to detect or listen in.
- Enhanced data transfer rates.
- The DS-SS assures reliable connections between the drone and the ground control station by broadcasting the signal over a wider range. As a result, the link is safer and more reliable.

6. Conclusion

The rapid development of drone technology requires communication information to be processed and analysed in accordance with strict safety standards to ensure reliable and safe communications, and this is our aim. Our system offers several advantages that have been demonstrated by simulation results in MATLAB. Firstly, the main advantage of Direct Sequence Spread Spectrum (DS-SS) is its ability to increase security without the need for additional hardware. This work is based on the DS-SS method with modifications to the proposed pseudo-noise PN sequence. The result is then used to spread the data and images transmitted using the DS-SS method. Simulations demonstrate the performance of this algorithm based on the use of a new pseudo-random code to optimize DS-SS against advanced attacks. From the results tables, we can say that our system is resistant to attacks and that it is close to the result of the encryption system, which concludes that our system guarantees the integrity and confidentiality of information. It also makes communication between UAVs more reliable and secure, which can increase the safety and efficiency of missions carried out by Unmanned Aerial Vehicles UAVs.

References

1. Alamgir, H., Shariful, I., Sadek, A. (2012) Performance analysis of Barker code based on their correlation property in multiuser environment. *International Journal of Information Sciences and Techniques (IJIST)*, 2(1), 27-39. https://ssrn.com/abstract=3812910.
2. Alawida, M., Teh, J.S., Alshoura, W.H. (2023) A new image encryption algorithm based on DNA state machine for UAV data encryption. *Drones*, 7(1), 38. https://doi.org/10.3390/drones7010038.
3. Anil Kumar, V., Mitra, A., Prasanna, S. R. M. (2007) Performance analysis of different PN sequences for speech encryption. In: *Proceedings of National Conference on Communications*, Kanpur, January 2007. https://www.researchgate.net/publication/327513248.
4. Anusha, T., Sreedhar, M. (2022) A new DSSS system based on multiuser time division and multiple accesses. *International Journal of Novel Research and Development*, 7(4), 2456-4184. https://ijnrd.org/papers/IJNRD2204041.pdf.

5. Atoev, S., Kwon, O., Lee, S., Kwon, K. (2018) An efficient SC-FDM modulation technique for a UAV communication link. *Electronics*, 7, 1-18. https://doi.org/10.3390/electronics7120352.
6. Balaji, D., Durga Rao, J., Srikanth, P. and Srinivasu, CH. (2012) Performance evaluation of barker codes by using nonsinusoidal waveforms in radar signal processing. *International Journal of Engineering Science and Technology (IJEST),* 4(03), 1071-1079. https://www.idc-online.com/technical_references/pdfs/electronic_engineering/PERFORMANCE%20EVALUATION%20OF.pdf.
7. Cai, G., Chen, B. M. and Lee, T. H. (2011) *Unmanned rotorcraft systems*. Springer London. doi:10.1007/978-0-85729-635-1.
8. DMS. (2010) *AR. Drone de Parrot. Technical Data*. DMS Company - ITS Department. https://cpge-grasshopper.fr/systemes/ar-drone/dossier_technique/dossier-technique-ar-drone.pdf (in French).
9. El-Iskandarani, M. A., Darwish, S. and Abuguba, S. M. (2008) A robust and secure scheme for image transmission over wireless channels. In: *Proceedings of the 42nd Annual IEEE International Carnahan Conference on Security Technology*, Prague, October 2008. IEEE: 51–55. doi:10.1109/CCST.2008.4751276.
10. Faraji-Biregani, M., Fotohi, R. (2021) Secure communication between UAVs using a method based on smart agents in Unmanned Aerial Vehicles. *The Journal of Supercomputing*, 77(6), 5076–5103. doi:10.1007/s11227-020-03462-0.
11. Glaviaux, A. (1990) *Information theory and codage*. UK: ENST Bretagne National High School of Telecommunications of Brittany, VII, 2-10.
12. Golomb, S. W. and Scholtz, R. A. (1965) Generalized Barker sequences. *IEEE Transactions on Information Theory*, 11(4), 533-537. doi: 10.1109/TIT.1965. 1053828.
13. Ismael, H.M., Al-Ta'i, Z.T.M. (2021) Authentication and encryption drone communication by using HIGHT lightweight algorithm. *Turkish Journal of Computer and Mathematics Education.* 12(11), 5891-5908. https://www.proquest.com/docview/2639740375?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals.
14. Jain, S., Ogale, J. V. (2018) Contribution of Barker and nested Barker code in CDMA technology. *International Journal of Management, Technology and Engineering*, 8(XI), 1633-1644. https://www.ijamtes.org/gallery/203-nov.pdf
15. Kiranmai, B., Rajesh Kumar, P. (2014) Performance Evaluation of Barker Codes using New Pulse Compression Technique. *International Journal of Computer Applications*, 107(20), 975–8887. doi:10.5120/18869-0417.
16. Krim, M., Ali-Pacha, A., Hadj-Said, N. (2017) New binary code combined with new chaotic map and gold code to ameliorate the quality of the transmission. *Indonesian Journal of Electrical Engineering and Computer Science*, 5(1), 166-180. http://doi.org/10.11591/ijeecs.v5.i1.pp166-180.
17. Krim, M., Ali-Pacha, A., Hadj-Said, N. (2018) The quality of the new generator sequence improvent to spread the color system's image transmission. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 16(1), 402-414. doi:10.12928/telkomnika.v16i1.6583.
18. Kristanto, A., Indriyanto, T. (2023) Development of communication system for UAV ground control station with ATC based on controller pilot data link communication. *Warta Penelitian Perhubungan*, 35(2), 243-256. doi:10.25104/warlit.v35i2.2308.
19. Li, W. K. (1991) Some Lagrange multiplier tests for seasonal differencing. *Biometrika*, 78(2), 381-384. https://doi.org/10.1093/biomet/78.2.381.
20. Lynch, S. (2014) *Dynamical systems with applications using MATLAB*. Birkhauser: 2nd edition. https://doi.org/10.1007/978-3-319-06820-6.
21. Mitra, A. (2007) On pseudo-random and orthogonal binary spreading sequences. *International Journal of Information Technology*, 4(2), 137-144.
22. Qin, X. Qu, F. and Zheng, Y. R. (2019) Circular superposition spread-spectrum transmission for multiple-input multiple-output underwater acoustic communications. *IEEE Communications Letters*, 23(8), 1385-1388. doi:10.1109/LCOMM.2019.2917192.
23. Sajid, A. Habib, A. Ali, S. Ejaz, S. (2019) Development of multi-user TDMA-based DSSS system. In: *Proceedings of the 2nd International Conference on Communication, Computing and Digital Systems (C-CODE)*, Islamabad, March 2019, 1-5. doi: 10.1109/C-CODE.2019.8681019.
24. Santos, Th. T., Gebler, L. (2021) A methodology for detection and localization of fruits in apples orchards from aerial images. In: *Proceedings of the 13th Brazilian Congress of Agroinformatics*, November 2021. https://doi.org/10.5753/sbiagro.2021.18369.
25. Scholtz, R. (1982) The origins of spread-spectrum communications. *IEEE Transactions on Communications*, 30(5), 822-854. doi: 10.1109/TCOM.1982.1095547.

26. Scholtz, R. (1997) The spread spectrum concept. *IEEE Transactions on Communications*, 25(8), 748-755. doi: 10.1109/TCOM.1977.1093907.
27. Stojanovic, N., Todorovic, B.M., Ristić, V.B, Vukanic Stojanovic, I. (2024) Direct sequence spread spectrum: History, principles and modern applications. *Vojnotehnicki glasnik*, 72(2), 790-813. DOI:10.5937/vojtehg72-49325.
28. Vishwas, C. G. M., Sanjeev Kunte, R. (2024) Chaotic map based random binary key sequence generation. *International Journal of Computer Network and Information Security (IJCNIS)*, 16(4), 102-117. doi:10.5815/ijcnis.2024.04.07.
29. Viterbi, A. J. (2002) Spread spectrum communications myths and realities. *IEEE Communications Magazine*, 40(5), 34-41. https://doi.org/10.1109/MCOM.2002.1006970.
30. Xue, H., Wang, Sh., Meng, X. (2013) Study on one modified chaotic system based on logistic map. *Research Journal of Applied Sciences*, 5(3), 898-904. doi:10.19026/rjaset.5.5037.
31. Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J. & Sajjad, A. (2022) Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 21, 917-935. https://doi.org/10.1007/s10207-022-00588-5.