

Secured drone communication based on Esalsa20 algorithm and 1D logistic map

Ibtesam Jomaa¹, Worud Mahdi Saleh², Rasha Rokan Ismail Hassan¹, Saja Huzber Hussien Wadi³

¹Department of Computer Science, Diyala University President, Diyala, Iraq

²Directorate General of Education in Diyala, Ministry of Education, Diyala, Iraq

³Department of Computer Science, College of Basic Education, Diyala University, Diyala, Iraq

Article Info

Article history:

Received Jun 20, 2022

Revised Sep 26, 2022

Accepted Oct 17, 2022

Keywords:

1D logistic function

Drone

Error sensitivity measurements

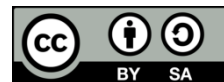
NTRIP communication protocol

Salsa20 lightweight algorithm

ABSTRACT

Over recent years, drones are increasingly being used not only for military tasks only, but also for civilian tasks too, such as environment and traffic monitoring, delivery services, and aerial surveys. Unfortunately, as they become more popular and in demand, they become more vulnerable to a variety of security threats. To combat such attacks and security threats, a proper design of a robust security and authentication system based on and stream cipher lightweight salsa20 algorithm with chaotic maps to cipher payload data to improve security network transfer of radio technical commission for maritime services (RTCM) messages over (NTRIP) communication protocol. By using a proposed key generation method which is based on a 1D logistic map to produce a flight session key for a drone with a flight plan, and then records the flight session key and the drone's flight plan in a central database that can be accessed. The proposed system is superior to other similar systems in terms of security and performance, according to the review.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ibtesam Jomaa

Department of Computer Science, Diyala University President

Diyala, Iraq

Email: Ibtesam.jomaa.h@uodiyala.edu.iq

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) or drones are expected to have numerous advantages over regular vehicles, including the ability to drive at a continuous and faster speed, the absence of physical road infrastructure, route directness, and the avoidance of traffic and congestion. They are expected to shorten delivery times and improve logistics system responsiveness. These advantages of UAV-based distribution are especially noticeable in urban areas. The ensuing time and cost savings in commercial logistics systems could benefit both companies and customers, and save lives and improve public health and safety by improving emergency services and medical supply [1]. Most autonomous drones only fly at a lower speed near hover to ensure that they can accurately sense their surroundings and have enough time to avoid obstacles. Human pilots have demonstrated that drones are capable of flying at astonishing speeds over complex terrain such as racetracks [2]. Despite the dangers and threats that manned aircraft provide to soldiers, drones were specifically created for military purposes, but they now have a wide range of additional uses. Drones are also utilized for airborne inspection and monitoring of electricity lines and oil and gas pipelines, in addition to package delivery [3]. Drones, provided with camera sensors enable improved situational awareness of several emergency responses and disaster management applications, as they can function from remote and complex accessing regions. The UAVs can be utilized for several application areas which can hold sensitive data, which necessitates secure processing using image encryption approaches [4]. Because of the various attack tactics

and targets, the outcomes vary. Some attacks attempt to steal data through communication connection security weaknesses, while others aim to spoof sensors, such as GPS spoofing.

Regarding the previous study that proposed a comprehensive assessment of drone/UAV use in various domains and for varied aims [5]. A real-world assault scenario is also demonstrated, showing how the authors recreated a hacking attack on a certain drone once the hacking cycle was finished. As a result, a variety of civilian and military anti-drone/UAV countermeasures will also be investigated.

Nguyen and Nguyen [6] the authors improved cybersecurity for people and policy suggestions for future work in this field of interest. Sensors, communication lines, and photo privacy are all used to exploit cyber security holes. As a result, a mix of solutions for many sensors, through the use of secure communication links rather than Wi-Fi, and the use of the confidentiality, integrity, and availability (CIA) trinity concepts are required to assure the security of drones. Proposed a safe authentication strategy for drones in smart cities with low latency that uses block chain technology in [7]. They use a regional architecture in a drone network, and they are using a modified decentralized consensus called Drone-based delegated proof of stake (DDPOS), which does not require re-authentication, for drones between zones in a smart city. The proposed architecture for the internet of drones aims to have a favorable impact on increased security and reduced latency (IoDs).

Aggarwal *et al.* [8], to lessen the burden of drones, they employed block chain technology to store acquired data from the drones and update information into distributed ledgers. It also ensures that the data collected by the drones in the proposed system is secure, authenticated, and authorized. In addition, compared the convolution neural network (CNN) technique with autonomous IoD to explore the security of the internet of drones (IoD) in [9]. analyze and build a better system security performance model, wireless communication technology was used. According to the results of the IoD performance investigation, the clustering technique based on signal energy has the greatest result.

This research has mostly focused on getting the power to control drones by establishing confidence between drones and ground stations, which are regarded to be trusted authorities. Furthermore, the goal of these studies is to improve the security of the communication channel between the drone and the ground station by employing classical cryptographic algorithms that utilize Drone resources like time and energy. Unlike these approaches, the goal of our research is to determine whether a drone in a fly zone has been granted permission to fly through authentication between drones and ground stations, as well as to improve the security of the communication channel between drone and ground station using the lightweight stream cipher salsa20 algorithm.

In this work, we propose the security of the drone communication network for surmounting the challenging information leakage problem due to potential eavesdropping. This work aims to design an authentication system model between the drones and ground stations and make a secure channel to exchange data using lightweight algorithms. To increase the security of information transmission through drone communications with ground control stations we use salsa20 stream cipher lightweight algorithm with chaotic map. Proposing an authentication method between the ground station and drone using proposed salsa20 lightweight algorithm key management. The main contributors of this work secure the data payload of the NTRIP based on the salsa20 algorithm and addition of an authentication method by using the proposed salsa20 lightweight key management between the grand station and drone. This new contribution will provide secure communication channels for the transmission of data between the grand station and drone.

The remaining part of the paper is laid out as follows: a related study, such as a Drone, key management, salsa20 lightweight algorithm, 1D logistic map and network transfer of RTCM messages over (NTRIP) in section 2. Meanwhile, section 3 explains the proposed design model, and section 4 analyzes the results and discussion for the finding of this study. Finally, the last section 5 will be the conclusion of the study.

2. METHOD

We introduce the techniques and methods employed in the suggested system to aid in the comprehension of the proposed system. In addition, Salsa20 lightweight algorithm has been used with 1D logistic function. We also showed the error sensitivity metrics that we used to evaluate the suggested system's performance in this work.

2.1. Drone

A drone is an aircraft that can fly without a human pilot on board and are typically small aircrafts made of lightweight materials. Drones are also called as unmanned aerial vehicles (UAV), unmanned aircraft system and remotely piloted aircrafts [3]. Typically, any UAV or drone architecture consists of three main elements: unmanned aircraft (UmA), ground control station (GCS), and communication data-link. Drone is commonly used to refer to remotely (autonomously) guided aircraft. This term also describes various vehicles including

submarines or land-based autonomous vehicles. In fact, drones can be classified into three main types, according to their flying mechanisms to i) multi-rotor drones; ii) fixed-wing drones; and iii) hybrid-wing drones [5].

2.2. Security of drones communication

Flying items provide a high risk of damage; it is critical to understand the security and safety risks associated with UAVs. Attackers can "simply" take control of a UAV using ordinary "hacking" tools, prohibiting it from carrying out its duties or, even worse, especially damaging. As a result, there is a pressing need to improve UAV security. Drone manufacturers rely on frequency hopping, spectrum spreading, and key sharing as active security measures, therefore they are closely connected to protocols like IPv4 but do not employ security measures, leaving them open to known assaults [3]. Figure 1 depicts the UAV communication link [10].

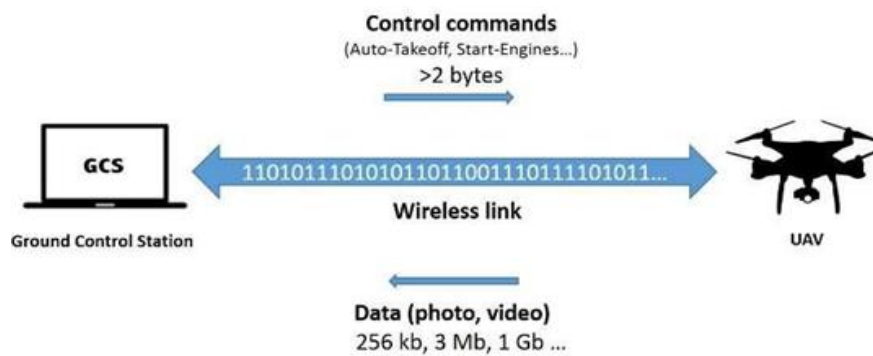


Figure 1. UAV communication link

2.3. Secure communication protocol for drones

NTRIP is becoming a more popular technique for providing real-time kinematic (RTK) service over the internet. NTRIP casters are available all over the world, and users with proper authentication can access the radio technical commission for maritime services (RTCM) [11]. NTRIP may be easily sent via the Internet utilizing several methods, including local area network (LAN), Wi-Fi, and the local mobile operator's cell network. In today's world, where more than one station is connected, the NTRIP protocol is commonly utilized since all of the data produced by the connected stations is post-processed by an NTRIP server, allowing them to act as a network rather than a single connected base station. Figure 2 shows the NTRIP network diagram. NTRIP technology is the most acceptable option for the highest level of accuracy and at least 95% time availability [12].

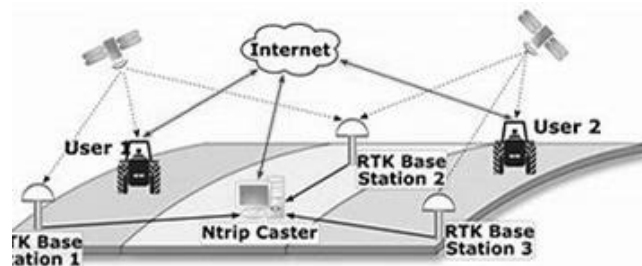


Figure 2. NTRIP network principle diagram (courtesy of AlberdingGmbH solutions)

2.4. Lightweight cryptography algorithm

Light-weight cryptography is a sector of a classical cryptographic method that is commonly defined as a cryptography for resource-constrained devices. The term "light-weight encryption" is a combination of two terms "light and weight." Platforms, as well as hardware and software, use light-weight encryption and decryption. Lightweight cryptography is divided into two categories (symmetric and asymmetric cipher). Figure 3 depicts the light-weight cryptography (LWC) block diagram [13]. The light-weight cryptography primitives can be classified as lightweight block cipher (LWBC) lightweight stream ciphers (LWSC),

lightweight hash functions (LWHF), and elliptic curve cryptography (ECC) [14]. Lightweight cryptography (LWC) expects to execute cryptographic algorithms with the use of a few computational cycles providing high robustness against security attacks meanwhile [15].

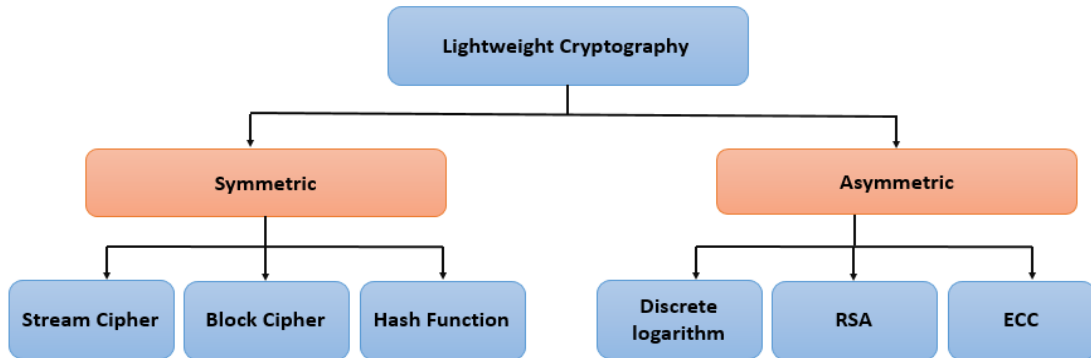


Figure 3. Light-weight cryptography diagrams

2.5. Salsa 20

Salsa20 is an original cipher function developed by Lam *et al.* [16]. As a lightweight security, technique for exchanging meter read in and other information, Salsa20 uses stream cipher as the encryption mechanism. Key stream on salsa20 methods are made up of mathematical operations that function on 32-bit words and employ a 256-bit key $K=(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ or a 128-bit key $K=(k_0, k_1, k_2, k_3)$ as input and a 64-bit nonce $N=(n_0, n_1)$ as output, resulting in a 512-bit Keystream block sequence, see [17] for more detail.

2.6. 1D logistic function

The 1D logistic map, which displays simple dynamic equations numerically with complex chaotic behavior, is among the most well-known one-dimensional chaotic maps [18]. Although using 1D logistic maps increases the efficiency of cryptography algorithms [19]. The following is a description of:

$$X_{n+1} = FL(u, X_n) = u \times X_n \times (1 - X_n) \quad (1)$$

where u is the control parameter in the range $u \in (0,4]$, x_0 denotes the chaotic map's initial value, and X_n denotes the chaotic sequence's output [20]. The logistic map's bifurcation diagram is depicted in Figure 4 the horizontal axis in the plot represents the " r " bifurcation parameter and the vertical axis shows the possible long-term population values of the logistic function. Each of these bifurcation points is a period doubling bifurcation [21].

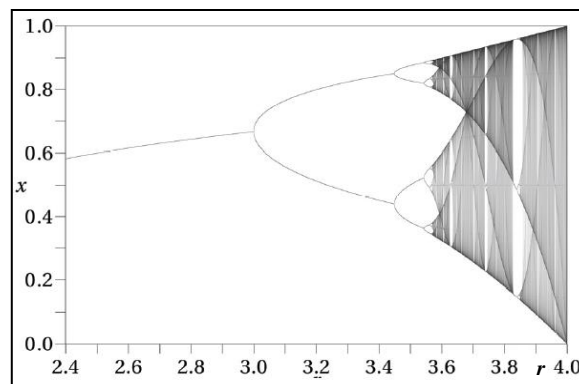


Figure 4. The logistic map's bifurcation diagram

2.7. Error sensitivity metrics

This subsection will be discussed in detail all error sensitivity measurements that using t evaluated the performance of the proposed system. The proposed method was analyzed in terms of security and speed against. This measurement are detailed in the following subsections.

2.8. Mean square error

As indicated in (2), MSE obtained by averaging the squared intensities of the original (input) and resulting (output) image pixels,

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N ((a(i,j)-b(i,j))^2)}{N \times M} \tag{2}$$

the parameters a (i, j) and b(i, j) relate to the pixels in the ith row and jth column of the original and encrypted images, respectively and M×N is the image size. The lower the MSE number, the more secure the encryption [22].

2.9. Peak signal-to-noise ratio (PSNR)

SNR is a mathematical measure of image quality depending on the pixel difference between the two images [23]. The SNR value is a comparison of the quality of the enhanced image to the original image. PSNR is given by (3) as:

$$PSNR = 10 \text{Log} \frac{s^2}{MSE} \tag{3}$$

for an 8-bit picture, s equals 255. When all pixel values are equal to the greatest possible value, the PSNR is equal to the SNR.

2.10. Normalization cross correlation

The NCC is a measurement of similarity between two wavelengths as a function of lost time applied to one of the wavelengths; the lower the value of NCC, the lower the image quality; the NCC expresses in (4) [24].

$$NCC = \frac{\sum_{m=1}^M \sum_{n=1}^N x(m,n).y(m,n)}{\sum_{m=1}^M \sum_{n=1}^N (x(m,n))^2} \tag{4}$$

Where x is the original image, y is the encryption image and the size of images is equal to m×n.

2.11. Average difference (AD)

Between the input and the recovered images, the average difference metrics of difference are calculated. If the greatest difference is high, it indicates that the image quality is weak. As shown in (5) can be used to calculate AD [25].

$$AD = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (x(i, j) - y(i, j)) \tag{5}$$

2.12. Correlation coefficient metric

The correlation coefficient is a factor that is used to determine the relationship between two variables: plaintext and encryption. This metric shows how well the suggested encryption algorithm defends against statistical attacks. As a result, cipher text must be distinct from plaintext. As shown in (6), (7), and (8) are used to get the correlation coefficient [26].

$$\text{Corr Coef}(x, y) = \frac{\sum_{i=1}^n (x_i - \mu(x))(y_i - \mu(y))}{\sigma(x)\sigma(y)} \tag{6}$$

Where $\mu(x)$ and $\mu(y)$ are the respective means of x and y.

$$\mu(x) = \frac{1}{n} \sum_{i=1}^n x_i, \text{ and } \mu(y) = \frac{1}{n} \sum_{i=1}^n y_i \tag{7}$$

The plaintext and cipher text variables are x and y. Furthermore, the terms in the denominators (also known as the x and y standard deviations) are:

$$\sigma(x) = \sqrt{\sum_{i=1}^N (x_i - \mu(x))^2}, \text{ and } \sigma(y) = \sqrt{\sum_{i=1}^N (y_i - \mu(y))^2} \tag{8}$$

The plaintext and its encryption are identical if the correlation coefficient is one. If the correlation coefficient is equal to zero, the cipher text and plaintext are completely different (i.e. good encryption). As a result, encryption success equates to lower correlation coefficient values [27].

2.13. Average security

Cipher secrecy is calculated using key equivocation (conditional entropy of key given cipher) [28]:

$$H(k/C) = \sum_{j=1}^L \sum_{i=1}^n q_i P_{ij} \log P_{ij} \tag{9}$$

where $q_i = \Pr(C=ci)$ and $P_{ij} = \Pr(K=ki/C=ci)$ L and n are the key and cipher text lengths, respectively.

3. THE PROPOSED SYSTEM

The proposed system's design goals include developing an authentication technique that creates a flight session key for such a drone and registers that key, as well as the drone's flight plan, in a centralized database for mutual authentication between both the drone and the ground control station. The registered flying session key utilized by the ground station to authenticate the drone using a chaotic function. To improve the security of proposed authentication techniques, the salsa20 lightweight algorithm used to cipher the registered flight session key in the centralized dataset in the ground station. Using lightweight cryptography salsa20 algorithms with NTRIP to protect data between ground stations and drones. Figure 5 depicts the basic block diagram for the proposed system. Three basic steps are included in the proposed system (registration, encryption and decryption, and authentication stages). The proposed system is focused on a completely ground control station (GCS) and a single drone with a large number of flying sessions.

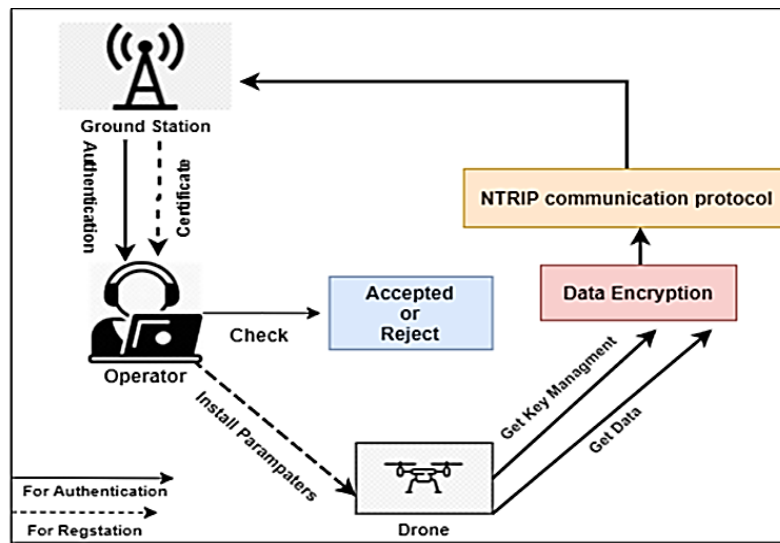


Figure 5. The proposed system's primitive block diagram

This is done on the GCS side when the drone intends to fly, firstly, ground control station (GCS) provides a session key to the drone. The GCS gives a certificate to the operator, which is represented (computer) inside GCS, GCS allows the operator permission to begin generating the secret key for each flying session using the suggested 1D chaotic maps depending on the key generation process. Also in this stage, the operator provides the drone with command and GPS coordinates for the current session. Figure 6, key management technique block diagrams.

3.1. Registration stage

This is done on the GCS side when the drone intends to fly, firstly, ground control station (GCS) provides a session key to the drone. The GCS gives a Certificate to the operator, which is represented (computer) inside GCS, GCS allows the operator permission to begin generating the secret key for each flying session using the suggested 1D chaotic maps depending on the key generation process. Also in this stage, the

operator provides the drone with command and GPS coordinates for the current session. Key management technique block diagrams has been illustrated in Figure 6.

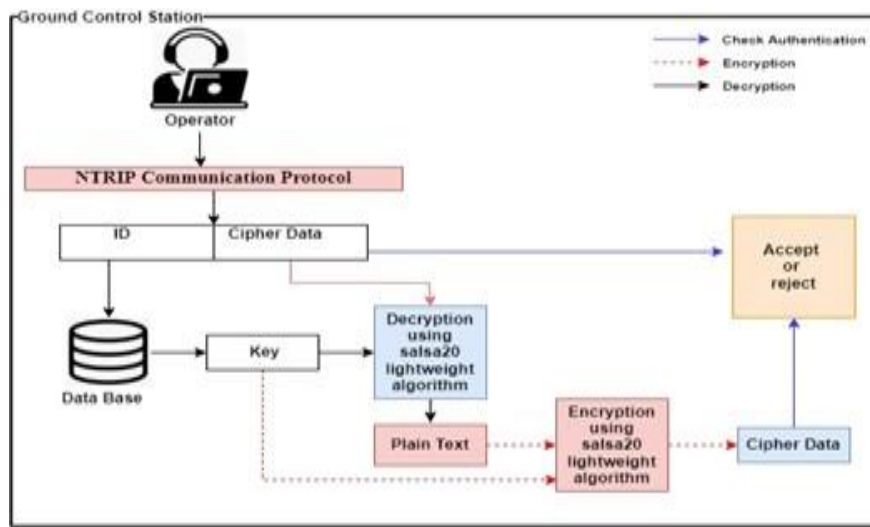


Figure 6. The key management technique is depicted as a block diagram

3.2. Key management technique

When a drone initiates a flight, it sends a request to GCS for a flight session key. The GCS obtain operator, which is a computer, wishes to manage the drone's security and authentication. GCS issues a unique certificate for each drone flight session. The certificate is the permission granted by GCS to the operator to begin the key creation procedure. To create a unique and randomized flying session key without needing to do any complicated math, the proposed system depended on one-dimension logistic chaotic function as shown in detail as shown in Algorithm 1.

Algorithm 1. Key generation

```

Input: x0, k, Key Size
Output: Key
Begin
Step 1 set key[]
Index=0
Step 2 for each byte in key size do
2.1 Calculate Logistic value by equation (1)
2.2 Data =Split (Logistic value, '.' ) and take only digits after the dot
2.3 Convert String to integer
Look up Table = "0123456789"
Key int = 0
For each char in Data
charValue = Look upTable.Index Of (char)
keyint = (keyint * 10) + charValue
End for
2.4 Key[index]= keyint mode 255
End do
End
    
```

Better reduction algorithm is used to convert integer numbers to binary byte or (32-bits) and to impairment excellent for modularity reducing of huge numbers, which is based on the basic concept of avoiding the slowness of long division by involving multiplications, subtractions, and shifts, as shown in Algorithm 2 [29].

This step will save the generated key in a central database in GCS as a pair of parameters for each fly. The operator requests the parameters for the drone from the database when he wants to install them. As indicated in the diagram below in Figure 7, the operator gives the drone two types of commands and coordinates: The operator sets up the first command and GPS coordinates for the current flight before the drone takes to the air as shown in Figure 7(a). After the drone fly, the operator sends a new command and GPS coordinates via NTRIP. When GCS wants to modification of the drone's path or if something malfunction

occurred during the flight. A heartbeat message is transmitted from the drone to the GCS before sending any new communication through the payload to ensure that the system is ready and alive as show in Figure 7(b). The salsa20 lightweight method was used to encrypt data from the GCS to the drone. In addition, the checksum computed after encryption ensures that the message is received correctly by the drone. The payload is decrypted using the salsa20 stream cipher after the checksum is verified. Manually install the parameter and command in the drone.

Algorithm 2. Barrett modular reduction

Input: two integer number $a=(a_{2k-1}\dots a_1x_0)$ b , $p=(p_{k-1}\dots p_1p_0)$
 (with $p_{k-1}\neq 0$), and $\mu = \lfloor \frac{b^{2k}}{p} \rfloor$

Output: $r=\text{mod } p$

Begin

$q_1 = \lfloor a/b^{k-1} \rfloor$

$q_2 = q_1\mu$

$q_3 = \lfloor q_2/b^{k-1} \rfloor$

$r_1 = a \text{ mod } b^{k+1}$

$r_2 = q_3p \text{ mod } b^{k+1}$

$r = r_1 - r_2$

if $r < 0$ then

$r = r + b^{k+1}$

whiler $\geq p$ do

$r = r - p$

return(r)

End

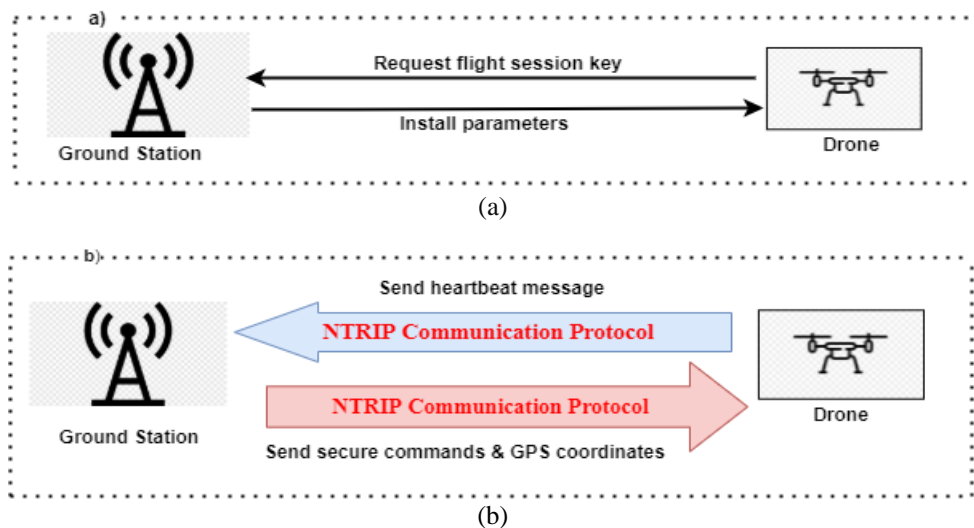


Figure 7. Mechanism of sending commands and GPS coordinates from GCS to drone; (a) before drone fly and (b) after drone fly

3.3. Encryption stage

This is an encryption/decryption stage that uses the salsa20 lightweight encryption algorithm to save time and energy for the drone. The suggested system was implemented in the following steps. As shown in Figure 8, to improve the security of the NTRIP communication protocol used by the ground control station (GCS) and the drone.

3.4. Authentication stage

To develop a secure transmission channel for data exchange in the proposed system, an authentication algorithm based on the salsa20 lightweight algorithm was proposed. The proposed authentication algorithm 3.

Algorithm 3. Authentication algorithm

Input: Cipher Data

Output: Authentication or Not Authentication

Begin


```

Step1 split Data encryption
    id session = Data encryption
    Data_En= Data encryption
    X= Data_En
Step2 get key based on id session
Step3 decryption for each block in data
    For each block in Data do
        Data_dec using the salsa20 lightweight algorithm(block, key )
    End for
Step4 encryption for each block in data
    For each block in Data do
        Data_En using the salsa20 lightweight algorithm(block, key )
    End for
Y= Data_En
Step5 check authentication or not authentication
If X=y then return authentication
Else return not authentication
End
    
```

To resist different attacks, the suggested method must meet important security requirements. The following are some of the most critical requirements:

- a. Mutual authentication: For a drone and a GCS to communicate securely, the communicating entities must mutually authenticate each other.
- b. Strong key exchange: To provide complete forward secrecy, a strong key exchange should be performed in such a way that the session keys created cannot be recovered.
- c. Confidentiality: the information sent between the drone and the GCS should be kept private so that unauthorized parties cannot access it.
- d. Integrity: It is important to ensure the authenticity of the information shared between the communicating ends (that the information has not been changed and that the source of the information is legitimate).
- e. Non-repudiation: in such scenarios, one of the most important security needs is that the action taken by one party cannot be successfully refuted without the knowledge of others.
- f. Protection against Denial of Service: Legitimate users, such as legitimate drones, should not be refused service by a service provider, such as a GCS.
- g. Protection against MITM (Man-In-The-Middle) attack: the protocol prohibits an attacker from secretly relaying messages.

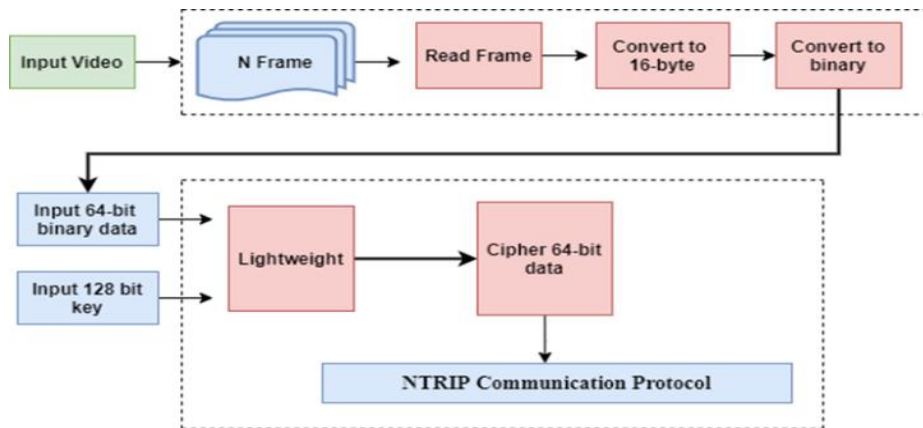


Figure 8. Block diagram of the encryption data based on lightweight algorithm

4. RESULTS AND DISCUSSION

The analysis of the proposed system security outlined in Part 3 is presented in this section. The formal security analysis is used to determine whether or not the security system meets the specified security information and requirements. Formal security analysis has been the subject of continuing for the past few years. The suggested method is explicitly proven in this study using error sensitivity-based metrics such as mean square error (MSE), peak signal to noise (PSNR), normalized cross-correlation (NCC), and average differential error (ADE), and average different (AD). Sub section 4.1 illustrates the initialization of the proposed system. The implementation and results of the proposed security and authentication of drones using salsa20 lightweight encryption algorithm are explain in sub section 4.2 and 4.3 respectively.

4.1. Initialization

The suggested system is run on a laptop computer using C#. The tests were carried out using a laptop with an Intel(R) Core (TM) i7-7700HQ processor running at 2.80 GHz (8 CPUs), a 64-bit operating system, and 16384 MB of RAM. This section contains the findings of each stage of the suggested system, as well as performance evaluations based on error sensitivity measurements, correlation coefficient metrics, and average security metrics. The suggested system consists of three main stages as illustrated in section 3 which are (registration, encryption/decryption lightweight, and authentication). Each of these stages includes sub-steps as shown in section 3, the results of all proposed system stages clarify in this section.

4.2. Results of registration stage

For every session of drone flying, a unique and random secret key will be generated during the registration stage. The 1D logistic chaotic function (1) used in the suggested key generation algorithm. Table 1 shows the results of the proposed key generation algorithm in three situations, each with a different number of logistic initial parameters (x0, k) and a number of sessions (=3). The suggested key generation algorithm produces a secret key with a size of 128 bits for each drone session fly. The suggested key generation process generates a 16-byte key (16*8-128-bit) for each session, with all keys having a value between 0-255.

Table 1. Results of key generation algorithm

case #1 (x0=0.1 andk=1) and the number of sessions =3																
Session Number	Key 1	Key 2	Key 3	Key 4	Key 5	Key 6	Key 7	Key 8	Key 9	Key 10	Key 11	Key 12	Key 13	Key 14	Key 15	Key 16
0	109	206	9	166	49	233	114	236	111	4	17	253	234	186	249	236
1	171	54	76	203	55	63	81	1	171	144	142	250	140	242	81	81
2	4	171	82	171	71	148	251	21	204	235	1	49	136	49	189	19
case #2 (x0=0.2andk=2) and the number of sessions =3.																
0	247	190	1	1	9	111	14	1	71	49	33	246	76	30	186	31
1	16	193	31	115	222	24	90	17	93	106	103	64	145	235	89	30
2	35	196	1	211	189	63	19	1	171	16	16	16	81	55	41	72
case #3 (x0=0.3 andk=3) and the number of sessions =3.																
0	26	224	186	195	171	40	173	159	24	106	84	226	94	210	51	151
1	1	1	145	249	222	3	73	160	65	34	234	1	147	71	106	106
2	204	97	186	66	76	230	106	1	19	21	249	123	154	137	135	106

4.3. Results of encryption/decryption lightweight stage

The suggested system's second stage is encryption and decryption to use the lightweight algorithm. This stage is solely performed on the drone's side, where the proposed system implementation on salsa 20 is lightweight and applied to two types of data (video and text). The video that was recorded by the drone and encryption payload data and sent to GCS via NTRIP, so Table 2 illustrated samples of video (MP4 Video type and 1280×720 dimensions) with the different attributes recorded by drone through session fly.

Table 2. Sample of video

No	1	2	3	4
Video size	11.2MB	14.3MB	5.68MB	4.03MB
Video length in a second	00:00:40	00:00:49	00:00:22	00:00:30

The proposed system firstly converts video to frames image see section 3.2, where take one sample image acquired from each sample. In Figure 9 the results show the success of the salsa20 encryption algorithm in encoding the image, meaning that the cipher image is unintelligible and has no effect on the main image or the dispersed pixels of initial test images and cipher images. Where Figure 9(a) show original image and it Histogram and Figure 9(b) show Cipher image and it histogram. The results indicate that using salsa20 encryption techniques to cipher histogram images seems to improve NTRIP security, preventing unauthorized users from acquiring the original image before encoding.

Table 3 shows the results of error-sensitivity based metrics used between original and cipher images using the salsa20 algorithm. MSE using (2), PSNR using (3), normalized cross correlation (4), and AD using (5) are the error sensitivity metrics. The best MSE values are 9088.654987, the best PSNR values are 8.587654332, the best NCC values are 0.545689222, and the best AD values are 83.13457418. Figure 10 illustrates that the salsa20 cipher image of various sizes has a quick execution time. Table 4 and Figure 10 have been explained below respectively. The suggested methods are compared to three state-of-the-art methods [4],

[30], [31] which can be used to safeguard communication in a UAV network in this section. In terms of execution time, the comparison is made.

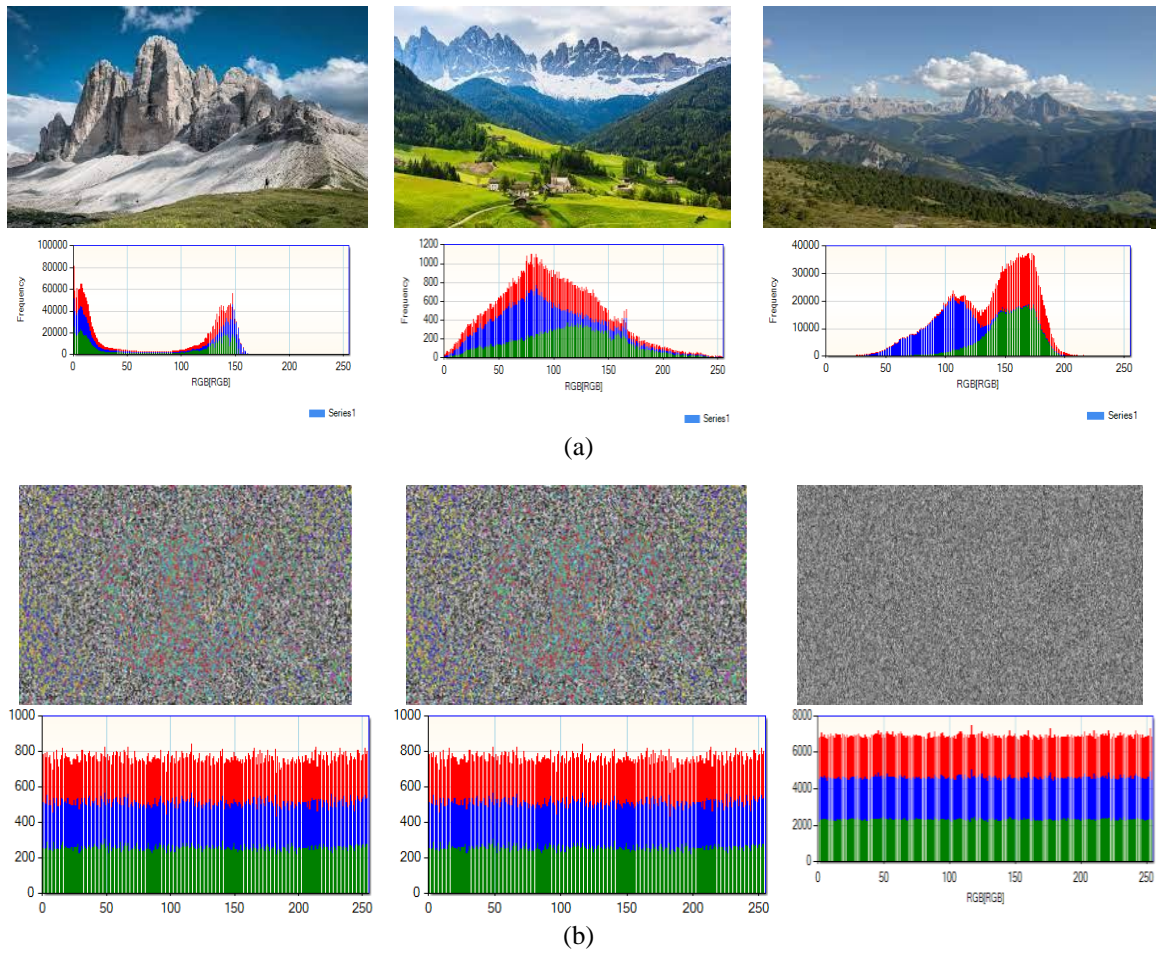


Figure 9. Salsa20 simulation results (a) original image and it histogram and (b) cipher image and it histogram

Table 3. Results of error sensitivity-based metrics

Error sensitivity based metrics		Image	Salsa20
1	MSE	Im1	4405.669205
		Im2	9088.654987
		Im3	6642.013472
		Im4	5156.547845
		Im5	5142.507929
2	PSNR	Im1	11.69068475
		Im2	8.587654332
		Im3	9.907806087
		Im4	11.00721309
		im5	11.01905391
3	NCC	Im1	0.629153028
		Im2	0.560039232
		Im3	0.545689222
		Im4	0.594587557
		im5	0.558858086
4	AD	Im1	65.42722703
		Im2	76.50540223
		Im3	83.13457418
		Im4	69.21349338
		im5	69.26755816

Table 4. Based on execution time, compare the proposed method to the previous one

No	Reference	Security methods	Execution time
1	Won <i>et al.</i> [30]	eCLSC-TKEM	9.25 s
2	Bunse and Plotz [31]	e Frequency Hopping Spread Spectrum (FHSS)	0.6 s
3	Alrayes <i>et al.</i> [4]	AISCC-DE2MS	11.13 msec
4	Our proposed method	Salsa20 algorithm	1.0 msec

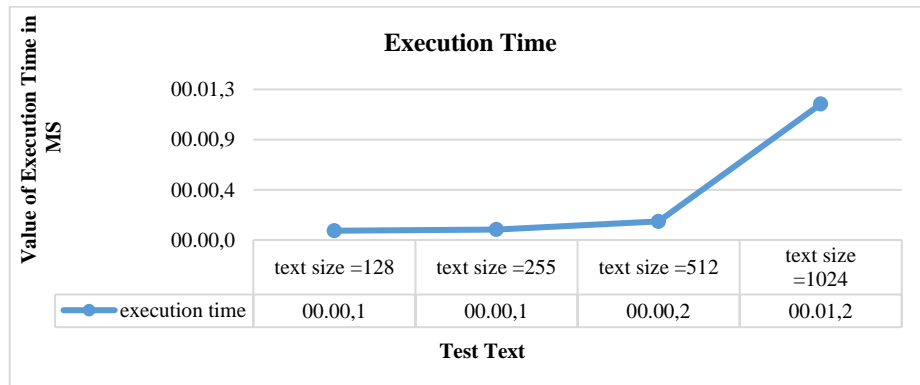


Figure 10. Cipher test execution time in MS various-sized text

5. CONCLUSION

Although unmanned aerial vehicles (UAVs) play an important role in many application areas, security issues limit their ability to supply the desired solution. The security and privacy of UAVs should be a top focus, especially in military scenarios. To solve the security issues, we proposed authentication and securing drone communications using salsa20 lightweight encryption algorithms. The proposed secured drone communications include three stages. The suggested system's initial stage is registration, while the second stage uses the salsa20 lightweight algorithm for encryption and decryption. The last stage in the suggested system is the authentication stage to check the authentication of the drone before receiving a message. Results of the proposed system done on two different types of data (colored image and text) with different sizes. Based on error sensitivity metrics the stream cipher salsa20 algorithm on ciphering-colored images achieves higher results, the most important values of MSE=9088.654987, the most important values of PSNR=8.587654332, the most important values of NCC=0.545689222, finally the best values of AD=83.13457418. In terms of speed salsa20 algorithm is faster in execution time in the case of ciphering-colored images and text, and the results demonstrate the improved performance of the processing model with an execution Time of 1.0 msec. For development of research results and application of further studies into the next, can implementing the proposed system in the real environment and using the present algorithm instead of the salsa20 algorithm with the proposed system. In addition, giving more flexibility to the proposed system by making the control process real-time and not employing pre-submitted parameters and benefit from this system not only as a security system but also as it can be employed as part of an integrated system to protect data sent by drone.




REFERENCES

- [1] M. Moshref-Javadi and M. Winkenbach, "Applications and research avenues for drone-based models in logistics: A classification and review," *Expert Systems with Applications*, vol. 177, p. 114854, Sep. 2021, doi: 10.1016/j.eswa.2021.114854.
- [2] P. Foehn *et al.*, "AlphaPilot: autonomous drone racing," *Autonomous Robots*, vol. 46, no. 1, pp. 307–320, Jan. 2022, doi: 10.1007/s10514-021-10011-y.
- [3] B. Sah, R. Gupta, and D. Bani-Hani, "Analysis of barriers to implement drone logistics," *International Journal of Logistics Research and Applications*, vol. 24, no. 6, pp. 531–550, Nov. 2021, doi: 10.1080/13675567.2020.1782862.
- [4] F. S. Alrayes *et al.*, "Artificial intelligence-based secure communication and classification for drone-enabled emergency monitoring systems," *Drones*, vol. 6, no. 9, p. 222, Aug. 2022, doi: 10.3390/drones6090222.
- [5] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things (Netherlands)*, vol. 11, p. 100218, Sep. 2020, doi: 10.1016/j.iot.2020.100218.
- [6] H. P. D. Nguyen and D. D. Nguyen, "Drone application in smart cities: the general overview of security vulnerabilities and countermeasures for data communication," in *Studies in Systems, Decision and Control*, vol. 332, 2021, pp. 185–210.
- [7] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021, doi: 10.1109/JIOT.2020.3015382.
- [8] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in internet of drones," in *IEEE International Conference on Communications*, May 2019, vol. 2019-May, pp. 1–6, doi: 10.1109/ICC.2019.8761372.




- [9] Z. Lv, "The security of Internet of drones," *Computer Communications*, vol. 148, pp. 208–214, Dec. 2019, doi: 10.1016/j.comcom.2019.09.018.
- [10] J. Shahmoradi, E. Talebi, P. Roghanchi, and M. Hassanalani, "A comprehensive review of applications of drone technology in the mining industry," *Drones*, vol. 4, no. 3, pp. 1–25, Jul. 2020, doi: 10.3390/drones4030034.
- [11] P. Zhu, L. Wen, X. Bian, H. Ling, and Q. Hu, "Vision meets drones: a challenge," *arxiv preprints*, Apr. 2018, doi: 10.48550/arXiv.1804.07437.
- [12] P. Getsov, S. Nachev, W. Bo, and D. Zafirov, "Precision drones-today and tomorrow," *Issledovanie Zemli iz Kosmosa*, no. 1, pp. S1–S8, Mar. 2019, doi: 10.31857/S0205-96142019184-91.
- [13] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," in *International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, Mar. 2018, pp. 105–108, doi: 10.1109/ICASEA.2018.8370965.
- [14] S.-L. Peng, S. Pal, and L. Huang, *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, vol. 174. Cham: Springer International Publishing, 2020, doi: 10.1007/978-3-030-33596-0.
- [15] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next generation lightweight cryptography for smart IoT devices: : implementation, challenges and applications," in *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, Apr. 2019, pp. 707–710, doi: 10.1109/WF-IoT.2019.8767250.
- [16] D. K. Lam, V. T. D. Le, and T. H. Tran, "Efficient architectures for full hardware script-based block hashing system," *Electronics (Switzerland)*, vol. 11, no. 7, p. 1068, Mar. 2022, doi: 10.3390/electronics11071068.
- [17] A. H. Fadel, R. S. Hameed, J. N. Hasoon, S. A. Mostafa, and B. A. Khalaf, "A light-weight ESalsa20 Ciphering based on 1D logistic and chebyshev chaotic maps," *Solid State Technology*, vol. 63, no. 1, pp. 1078–1093, 2020.
- [18] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5455–5472, May 2016, doi: 10.1007/s11042-015-2515-7.
- [19] Z. A. Abduljabbar *et al.*, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.
- [20] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, Sep. 2017, doi: 10.1016/j.sigpro.2017.03.011.
- [21] M. Almazrooie, A. Samsudin, and M. M. Singh, "Improving the diffusion of the stream cipher salsa20 by employing a chaotic logistic map," *Journal of Information Processing Systems*, vol. 11, no. 2, pp. 310–324, Jun. 2015, doi: 10.3745/JIPS.02.0024.
- [22] Y. Y. Al-najjar and D. C. Soong, "Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI," *International Journal of Scientific & Engineering Research*, vol. 3, no. 8, pp. 1–5, 2012.
- [23] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Optics and Laser Technology*, vol. 60, pp. 111–115, 2014, doi: 10.1016/j.optlastec.2014.01.015.
- [24] K. Domin, E. Marin, and I. Symeonidis, "Security analysis of the drone communication protocol: fuzzing the MAVLink protocol," in *Proceedings of the 37th Symposium on Information Theory in the Benelux*, 2016, [Online]. Available: <https://www.esat.kuleuven.be/cosic/publications/article-2667.pdf>.
- [25] S. A. Thomas and S. Gharge, "Half-tone visual cryptography for grayscale images using error diffusion and direct binary search," in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 2018, pp. 1091–1096, doi: 10.1109/ICOEI.2018.8553863.
- [26] K. Aoki *et al.*, "Camellia: A 128-Bit block cipher suitable for multiple platforms – Design and analysis," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2012, 2001, pp. 39–56, doi: 10.1007/3-540-44983-3_4.
- [27] M. Yahuza *et al.*, "Internet of drones security and privacy issues: taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021, doi: 10.1109/ACCESS.2021.3072030.
- [28] N. M. Sahib, A. H. Fadel, and N. S. Ahmed, "Improved RC4 algorithm based on multi-chaotic maps," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 15, no. 1, pp. 1–6, Jan. 2018, doi: 10.19026/rjaset.15.5285.
- [29] S. Ji and K. Wan, "Adaptive modular exponentiation methods v.s. python's power function," *arxiv preprints*, Jul. 2017, [Online]. Available: <http://arxiv.org/abs/1707.01898>.
- [30] J. Won, S. H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," in *ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, Apr. 2015, pp. 249–260, doi: 10.1145/2714576.2714616.
- [31] C. Bunse and S. Plotz, "Security analysis of drone communication protocols," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10953 LNCS, 2018, pp. 96–107, doi: 10.1007/978-3-319-94496-8_7.

BIOGRAPHIES OF AUTHORS






Ibtesam Jomaa    is a Master at Department of Computer Science, College of Science, Diyala University, Iraq. She holds a Master degree in Computer Science from Diyala University and the Bachelor degree in software engineering from the University Al-Rafidain College, Baghdad. She can be contacted at email: Ibtesam.jomaa.h@uodiyala.edu.iq.






Worud Mahdi Saleh    holder of a technical diploma from the Institute of Management/Rusafa and a bachelor's degree from Al-Mustansiriya University in computer science, as well as a master's degree from Diyala University in the same specialty. An employee in the Diyala Education Directorate for eight years. She can be contacted at email: hawhral1888@gmail.com.



Rasha Rokan Ismail Hassan    she is studied Bachelor's degree in the Department of Computer Science/College of Science/University of Diyala in the year 2006/2007 and master's degree in the Department of Computers/College of science/Diyala University in 2019. I have participated in many training courses, scientific seminars, conferences and scientific lectures in various fields. She can be contacted at email: rasharokan85@gmail.com, rasha_rokan@uodiyala.edu.iq.



Saja Huzber Hussien Wadi    she is studied Bachelor's degree in Computer Science from the University of Diyala/College of Basic Education for the academic year 2013-2014, with the sequence of the first on the department and the second on the college on the graduation batch. I was appointed to the permanent staff on 22/12/2016 as an employee in the presidency of the University of Diyala/Department of Administrative and Financial Affairs, titled (Programmer). She can be contacted at email: sajahussien109@gmail.com.