Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.053706

ARTICLE

A Shuffling-Steganography Algorithm to Protect Data of Drone Applications

Ahamad B. Alkodre[1], Nour Mahmoud Bahbouh[2], Sandra Sendra[3], Adnan Ahmed Abi Sen[4,*], Yazed Alsaawy[1], Saad Said Alqahtany[1], Abdallah Namoun[1] and Hani Almoamari[1]

[1]Faculty of Computer and Information Systems, Islamic University, Al-Madinah, 42351, Saudi Arabia

[2]Department of Information and Communication Sciences, Granada University, Granada, 18071, Spain

[3]Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politècnica de València, Valencia, 46730, Spain

[4]Department of Graduate Studies & Scientific Research, University of Prince Mugrin, Al-Madinah, 42351, Saudi Arabia

*Corresponding Author: Adnan Ahmed Abi Sen. Email: Adnanmnm@hotmail.com

Received: 08 May 2024 Accepted: 27 September 2024 Published: 18 November 2024

ABSTRACT

In Saudi Arabia, drones are increasingly used in different sensitive domains like military, health, and agriculture to name a few. Typically, drone cameras capture aerial images of objects and convert them into crucial data, alongside collecting data from distributed sensors supplemented by location data. The interception of the data sent from the drone to the station can lead to substantial threats. To address this issue, highly confidential protection methods must be employed. This paper introduces a novel steganography approach called the Shuffling Steganography Approach (SSA). SSA encompasses five fundamental stages and three proposed algorithms, designed to enhance security through strategic encryption and data hiding techniques. Notably, this method introduces advanced resistance to brute force attacks by employing predefined patterns across a wide array of images, complicating unauthorized access. The initial stage involves encryption, dividing, and disassembling the encrypted data. A small portion of the encrypted data is concealed within the text (Algorithm 1) in the third stage. Subsequently, the parts are merged and mixed (Algorithm 2), and finally, the composed text is hidden within an image (Algorithm 3). Through meticulous investigation and comparative analysis with existing methodologies, the proposed approach demonstrates superiority across various pertinent criteria, including robustness, secret message size capacity, resistance to multiple attacks, and multilingual support.

KEYWORDS

Health of palm trees; steganography based text; steganography based image; drone; fog computing; security

1 Introduction

Date cultivation in the Kingdom of Saudi Arabia is a cornerstone of the agricultural sector, receiving considerable attention due to its significant contribution to national income. This type of cultivation is unique, covering extensive areas and involving long-living trees. To enhance sustainability and efficiency, numerous smart applications now utilize drones for various agricultural tasks. These include monitoring crop health, managing irrigation, predicting yields, and detecting diseases.

Additionally, drones are employed in other sectors such as smart transportation, crowd monitoring, disaster management, security operations, health services, and logistics [1–3].

Drones can easily reach any location and overcome geographical obstacles, which is particularly important for farms in remote areas, such as deserts. This capability underscores their importance in offering various efficient services. In agriculture, drones enhance practices by providing real-time monitoring, precise irrigation management, and early detection of plant diseases. Most of these services have emerged in recent years, driven by significant technological and communication advancements, especially after the development of the Internet of Things [4].

As drone applications become increasingly important, numerous challenges have emerged. One of the most urgent challenges is protecting the security and privacy of information transmitted by these drones to command centers or stations [5,6]. Data security and privacy are essential in all applications but they are particularly crucial in agriculture due to the sensitive nature of the services provided by drones. The security breach in drones can lead to real disasters. For instance, spreading information about a particular pest can affect date prices for an entire season or more. To address this issue, highly confidential protection methods must be employed [7]. On the other hand, traditional encryption methods are not secure against sophisticated attacks, which calls for more advanced protection strategies. This paper addresses these challenges by introducing the Shuffle Steganography (SSA) approach, a new method that incorporates strategic encryption and data hiding techniques to protect against brute force attacks and other advanced threats. The proposed approach uses predefined patterns that can be accessed from a large set of images, making unauthorized access more difficult and ensuring the integrity of the transmitted data.

Relying on traditional encryption methods is no longer effective in ensuring the security of the services provided [8]. This is particularly due to the increasing sophistication of attackers' skills and the availability of powerful resources to carry out hacking attacks or break encryption [9]. This is particularly critical in digital agriculture, where protecting sensitive crop data is essential. Hence, there is a need to rely on more effective protection methods, such as information hiding. Moreover, recent methods of image encryption (chaotic maps, pixel fusion, Feistel network, Hill, and DNA encoding) can also be broken by cryptanalysis based on chosen-plain-text or chosen-cipher-text attacks [10–14]. (Note: here, we encrypt the image itself as secret data).

Another method of data protection is information hiding. This method relies not only on strong encryption but also on not drawing the attacker's attention to the transmitted data. This can be achieved by hiding confidential data inside an envelope before sending it to its destination. The cover can be text, image, video, or maps, and will not be encrypted. Steganography essentially hides confidential agricultural information within a layer of other unimportant information (the cover). The cover is then sent to the target server without raising suspicions [15].

Furthermore, steganography methods integrate with encryption algorithms to hide confidential data by encrypting it before inserting inside the cover. Therefore, even if the attacker is aware of the presence of confidential information within the transmitted data, they will have great difficulty accessing, retrieving, decrypting, and reconstructing this information. There are many ways to employ steganography, differing in the level of protection it provides, the rate of secret data it can hide, its resistance to attacks or interference attempts, and its overall performance [16]. In the context of digital agriculture, this approach can significantly improve the security of sensitive data such as palm tree health, irrigation schedules, and pest management information. Fig. 1 shows the main steps used in steganography.

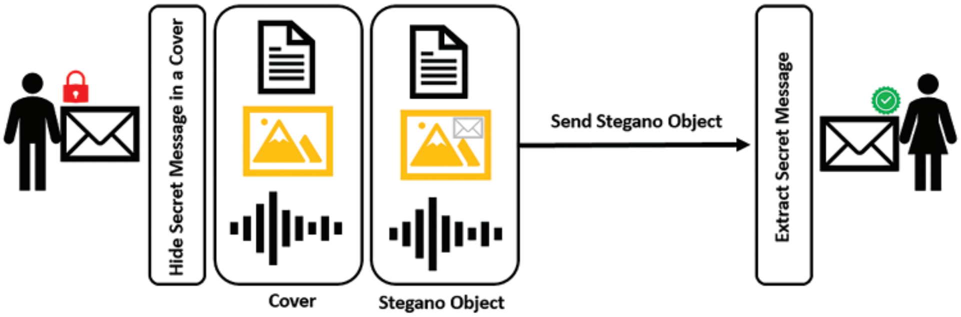


Figure 1: Main steps of steganography

The steganography approach is necessary to enhance the security of information in various communication channels, including text, images, and videos. Text-based steganography provides superior performance but limited protection, while video-based steganography is currently preferred despite affecting performance. Usually, image-based steganography achieves good security but with unacceptable performance. However, the choice of the steganography method is affected by the size of the data to be hidden. Some steganography methods are resistant to changes in the cover, providing a limited impact on the encrypted message, while in others the message can be destroyed after any change to the cover [17].

Despite numerous existing techniques for steganography, the need for new methods persists to provide more advantages and address the growing knowledge and experience of attackers [18]. This research introduces an innovative steganography method based on dividing, mixing, and merging data. In addition, the proposed method uses text-based steganography for part of the secret data and image-based steganography for other parts. In the field of digital agriculture, this research introduces a new method that can significantly enhance the protection of sensitive information, ensuring it remains secure against sophisticated attacks.

Our contributions in this research can be summarized as following:

- Proposing a new hybrid steganography method (text-based and image-based) to preserve the security and privacy of drone applications with different protection levels.
- Providing a new way to enhance the security of the proposed method by dividing the encrypted data based on a pattern.
- Proposing a new technique to hide data within a text cover, and then within an image cover.
- Implementing the proposed approach to demonstrate its superiority over other methods in terms of effectiveness, safety, protection, and reliability.

The rest of the article will be organized as follows. First, a review of important information hiding techniques based on text and images. Then we will present a table outlining the advantages and disadvantages of each approach. Then, the proposed approach and its associated algorithms will be presented in detail. In the results section, we will present the application interfaces of the proposed approach and discuss its superiority over other methods. Finally, the research will conclude with a conclusion and future perspectives.

2 Literature Review

This section provides an overview of the most significant approaches employed in steganography within text and image mediums. Previous research is categorized into three main sections: text-based hiding techniques, image-based hiding techniques, and hybrid techniques that treat text as an image. The relevance of these techniques in protecting sensitive agricultural data collected by drones is also discussed.

2.1 Text-Based Steganography Techniques

This research focused on the Arabic language, which has unique features like diacritics and morphology. These features make the Arabic language suitable to be cover for hiding data [19,20].

- KASHIDA [21]: This technique involves extending the width of a letter, and it can be applied to any letter in Arabic. It has been employed to conceal some data within the text. For example, the word "مدرسة" (school) would appear as "مـدرسـة," where two additional Kashida characters have been added, one after the letter "م" and the other after the letter "س."

This method selects specific characters and the Kashida character after one of the selected characters if the value is "1.", and does not add it if the value is "0,". Then, the data is stored as bits (a sequence of zeros and ones). It is noted that this method is easy to use, but it can be detected and hacked.

- Letter Encode [22]: This method benefits form the fact that some characters in languages like Arabic have different forms that change based on their position in a word (beginning, middle, or end). For example, the letter "م" appears as "مـ" at the start, "ـمـ" in the middle, and "ـم" or "م" at the end. This technique changes the character code based on the data to be stored.

In the decoding process, the character's position is compared to its code; if they match, it is read as "1," and if not, as "0." This method requires agreement on specific characters and positions, but some text editors may display characters incorrectly, which causes noticeable problems. In English, capitalization can be used similarly with the same character.

- It is considered a simple method in which empty spaces are doubled, or a single space is used, depending on the nature of the data to be stored. However, for large data sets, this method is easily noticeable. Many text engines now detect and highlight multiple consecutive spaces as errors [23].
- ZWJ and ZWNJ [24]: This method, developed from the Spacing method, adds special characters that appear as empty characters without any visible space or modification in the text. Although it cannot be detected by visual inspection alone, it increases the size of the text. Therefore, it can be detected by comparing the size of the text before and after the hiding process.
- Diacritics [25]: This method takes advantage of the features of some languages that use additional diacritics with characters, such as Arabic and Persian. Some diacritics are replaced by other diacritics based on the data to be hidden. If the data is extensive, readers familiar with the language may detect grammatical errors, leading them to suspect the presence of hidden information.
- HAMZAT [26]: This method focuses on hiding the Hamza on the Arabic letter "أ" or "إ" and replacing it with "ا." This requires an agreement on a specific hiding map between the sender and receiver. It is suitable for hiding limited secret.

Table 1 summarizes the comparison among Text-Steganography methods.

Table 1: Comparison among Text-Steganography methods and the proposed method based on Imperceptibility, Capacity, Robustness, and Security metrics

Name	Main idea	Advantages	Disadvantages
KASHIDA	Use "_" with Letters	Simple, Capacity	Easy to break and percept with large data
Letter Encode	Use on different codes for a letter	Simple, Capacity	Easy to break and suitable for private editor
Spaces	Use more than one space	Simple	Easy to break and percept
ZWJ	Use hidden character "ZWJ"	Capacity, Imperceptibility	Easy to break, can be percept
Diacritics	Change diacritic based on data	Simple, Capacity	Require a map
HAMZAT	Show or hide Hamza	Simple	Easy to break, Capacity
Hybrid Diacritics	Change the direction of diacritic	Capacity	can be percept, Performance with large data
Hybrid Letter Edge	Change the edge of some letters	Capacity, Good Security	Difficult Implementation, Performance
Proposed Method	Divide data based on a pattern, then hide a part in a Text cover, and another part in an Image one	Security, Imperceptibility, Performance, Simple	Capacity

2.2 *Image-Based Steganography Techniques*

There are two main types of hiding within the image [27]. The first type is based on the Special Domain and the second is based on the Frequency Domain [28]. The first type, Special Domain, depends on changing the least significant bits in the image (LSB). In other words, the value of the pixel is changed by one degree, knowing that the value ranges between 0 and 255. Therefore, this will affect the color degree of the pixel by one degree out of 256, which is impossible to detect by humans [29].

Fig. 2 shows the basic idea of LSB technology. This method is considered one of the good methods and easy to apply, but it is affected by changes that may occur to the image, such as compression or any modification process during transfer. As a security aspect, many developed methods have been proposed to improve the level of security. In [30], the method involved changing the starting point of the steganography process rather than beginning with the first pixel in the image. In [31], the sequence of pixels was rearranged based on a Zig-Zag pattern instead of the natural sequence for the steganography process. Reference [32] relied on inserting data into a specific color channel instead of all channels. Another method [33] worked to find the most important object in the image and then insert data into its pixels, while [34] relied oppositely on inserting data into the edges, that is, the high-frequency areas.

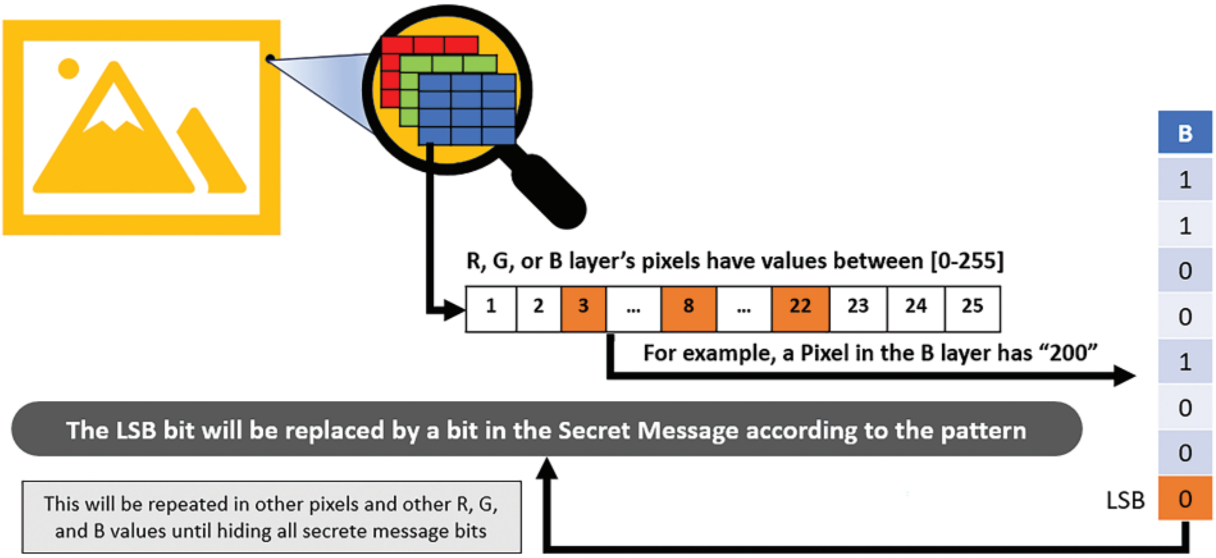

B
1
1
0
0
1
0
0
0
LSB
R, G, or B layer's pixels have values between [0-255]
1
2
3
...
8
...
22
23
24
25
For example, a Pixel in the B layer has "200"
The LSB bit will be replaced by a bit in the Secret Message according to the pattern
This will be repeated in other pixels and other R, G, and B values until hiding all secrete message bits

Figure 2: Steganography–spatial domain technique (LSB method)

The other type (frequency domain) of inserting into the image depends on converting the image into frequency form through functions such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). After the conversion process, data is either crammed into low-frequency bits or, conversely, into high-frequency bits, such as edges. The image is converted into frequency mode and then recreated. Frequency domain methods are more secure and resistant to changes, but they are more difficult and require higher performance and longer execution times [35,36]. Fig. 3 shows the basic idea of frequency domain-based methods.

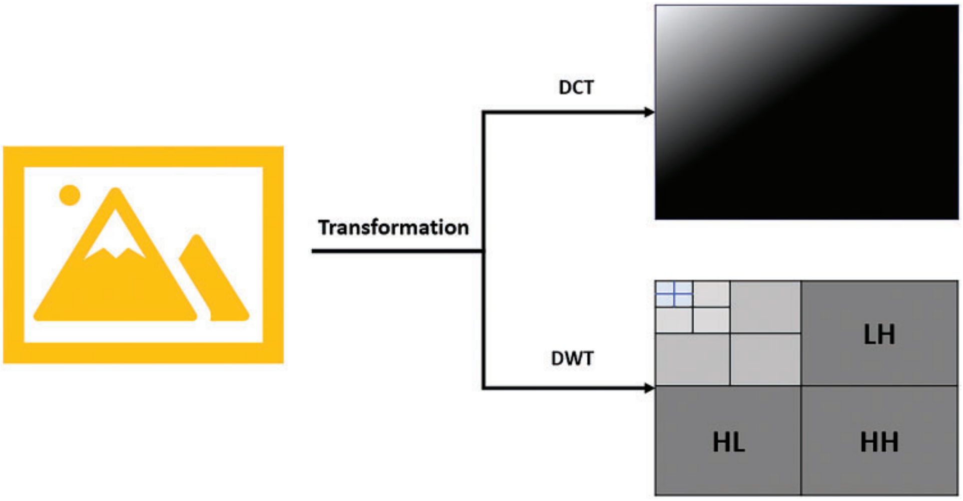


Figure 3: Steganography-frequency domain technique (DCT and DWT)

2.3 Hybrid Techniques

These techniques rely on hiding data within an image that includes text (dealing with text as the image) or combining both image-based and text-based hiding methods. In [37], the researchers modified the diacritics, as shown in Fig. 4A, which illustrates the diacritics before and after modification. In [38], they focused on altering the shape of the character endings in words, as depicted in Fig. 4B. However, it is worth noting that this method is time-consuming in the image creation and embedding processes, and it is also relatively easy to detect.

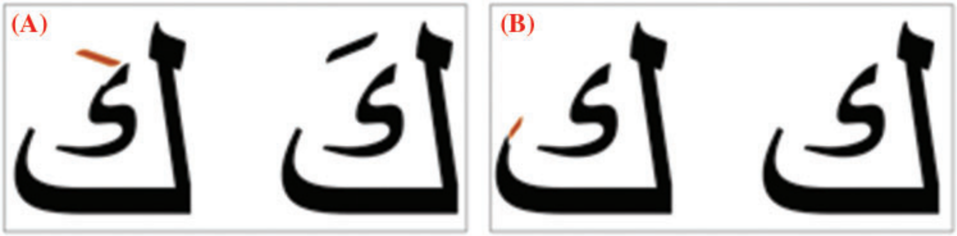


Figure 4: Change text as an image (A) diacritics modification; (B) endings modification

The previous methods did not achieve the required level of security while maintaining flexibility and ease of implementation. Even the hybrid methods have impacted performance adversely, and many fail to provide the desired level of security. In this research, we introduce a hybrid method as well, but in a completely different way. The proposed method will address the drawbacks of previous techniques and achieve a high level of protection, and imperceptibility while maintaining an acceptable capacity of data. Additionally, it is easy to implement. Furthermore, the proposed approach is suitable for applications in drone technology, as it does not require high computational resources.

2.4 Steganography and Image Encryption

Recently, significant advancements made in research on image encryption and steganography that have enhanced data security. For example, an image encryption scheme based on particle swarm optimization (PSO) using a standard exponential map has shown significant improvements in encryption, making it more resistant to attacks. In addition, a cross-channel color image encryption technique, which uses a two-dimensional hybrid randomization-based optimization map, effectively disables the correlation between colors channel, compared to traditional methods. These advancements in cryptography are particularly useful when considering potential integration with steganography, which, unlike, encryption focuses on securing data, steganography focuses on its location and presence. In our novel approach (SSA), we leverage these principles by enhancing the security of UAV communications through advanced steganography techniques. By discussing the encryption techniques and the steganography method we have proposed, we aim to illustrate how to develop a multi-layered security approach that provides robust protection for sensitive data transmitted by UAVs. This paper focuses specifically on steganography, placing it in the broader context of recent developments in data security. Table 2 compares a range of recent image encryption techniques, considering various aspects such as technique, focus, application, complexity, and robustness.

Table 2: Comparison among recent image encryption techniques

	Method							
Aspect	The Proposed Approach SSA	PSO-based Image Encryption Scheme [39]	Hyper chaotic Systems [40]	2D Hybrid Map for Image Encryption [41]	Image Encryption Using Deep Learning [42]	Hybrid Chaotic Maps for Image Encryption [43]	Lightweight Encryption for IoT Applications [44]	Quantum Chaos-Based Image Encryption [45]
Technique	Steganography (text & image)	Image encryption using PSO algorithm	Image encryption using chaotic systems	Image encryption using hybrid chaotic maps	Image encryption using deep learning and chaos	Hybrid chaotic Schaffer 2D maps	Lightweight chaotic encryption for IoT devices	Image encryption using quantum chaos
Primary Focus	Concealment of data in images	Optimization of encryption process	Enhancing security via chaos theory	Disrupting color channel correlations for security	Enhancing security through learning-based techniques	Improving security with chaotic dynamics	Lightweight and efficient encryption for IoT	High-security encryption leveraging quantum chaos
Application	Drone data security	General image security	General image security	General image security	General image security	General image security	IoT device security	High-security applications requiring advanced encryption
Complexity	Moderate	High	High	High	High	High	Moderate	High
Robustness	High (against detection and extraction attacks)	High (against cryptanalysis)	High (against differential and brute force attacks)	High (against differential and brute force attacks)	High (with learning-based resilience)	High (against various attacks)	Moderate to High (depending on application)	High (with quantum chaos providing strong unpredictability)
Advantages	Dual-layer security (text + image), suited for drone applications	Optimized encryption, efficient performance	Strong chaotic properties, high security	High level of security through complex mappings	Leverages the power of deep learning for enhanced security	Combines strengths of multiple chaotic systems	Lightweight, suitable for resource-constrained environments	Extremely high security due to quantum chaos properties
Limitations	Primarily focused on concealment, not encryption	Complexity in implementation and tuning	High computational cost	Requires careful parameter selection for effectiveness	Requires extensive training and computational resources	Complexity in ensuring stability of chaotic maps	May offer lower security in high-threat environments	High complexity and resource requirements due to quantum chaos
Potential for Integration	Can be combined with encryption for multi-layered security	Can complement steganography to enhance security	Can be integrated with steganography to boost security	Suitable for enhancing the security of steganography methods	Can be combined with steganography for advanced security solutions	Enhances steganography with chaotic properties	Can be integrated into IoT-based steganography systems	Can provide cutting-edge security when combined with steganography

3 Proposed Approach

The proposed approach depends on the main ideas to create an effective steganography method with a high level of security. The main idea is splitting the encrypted message or data into two parts (one small and another large) based on the agreed Pattern 1 (e.g., 11101011) (Algorithm 3). The smaller part will be hidden in a text cover based on algorithm1 and creating new text has the secret information. The new text will be merged with the larger part and then hidden inside an image cover based on Pattern 2 and Algorithm 2, which determine the sequence of color layers (e.g., BBRGB). This method is particularly effective in protecting data related to crop health, irrigation schedules, and pest management collected by drones in agricultural settings. All of the above will make it impossible for any attacker to detect, retrieve, reorder, and decrypt the data. In other meaning, the attacker needs to know:

- Pattern 2 is responsible for the method and sequence of hiding in the image's layers
- Key 2 of decryption data which is inserted inside the image
- Isolated the returned data to text and Part 2
- Break the method of hiding in the text and find the part
- Pattern 1 to reorder the data of Part 1 and Part 2
- Key 1 of decryption of the whole data (Part 1+Part 2)

For these reasons, it is very difficult to break the protection of the SSA. Moreover, users can use special cover text that appears as a secret message by itself, simulating the honeypot method.

The proposed method provides a new way of employing steganography in text and images, composed of multiple layers of protection. The approach hides different parts of data in each layer. Consequently, attackers can retrieve the original data only if they return all encrypted bits from both the image and text and order all bits correctly.

Note: Pattern 1, Pattern 2, Algorithm 1, Algorithm 2, and the proposed approach will be explained in detail in the next paragraphs. Fig. 5 depicts the main steps of the complete algorithm (1, 2, and 3). While Fig. 6 shows the details of the proposed approach as flowchart.

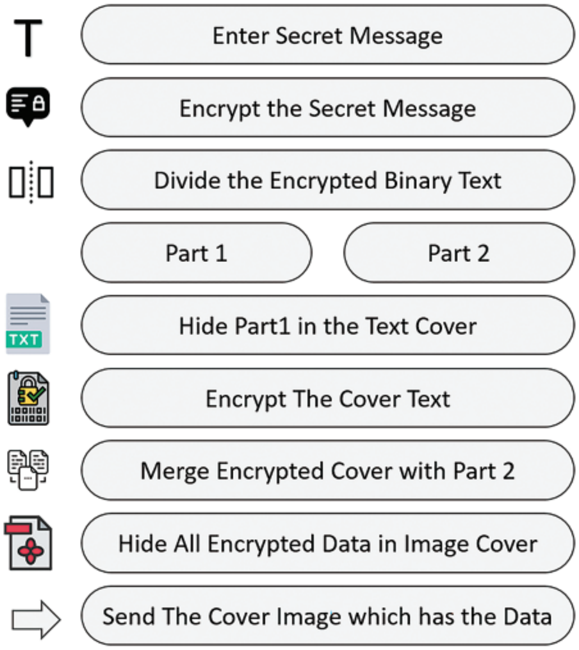

Enter Secret Message
Encrypt the Secret Message
Divide the Encrypted Binary Text
Part 1
Part 2
TXT
Hide Part1 in the Text Cover
Encrypt The Cover Text
Merge Encrypted Cover with Part 2
Hide All Encrypted Data in Image Cover
Send The Cover Image which has the Data

Figure 5: Main step of the proposed method

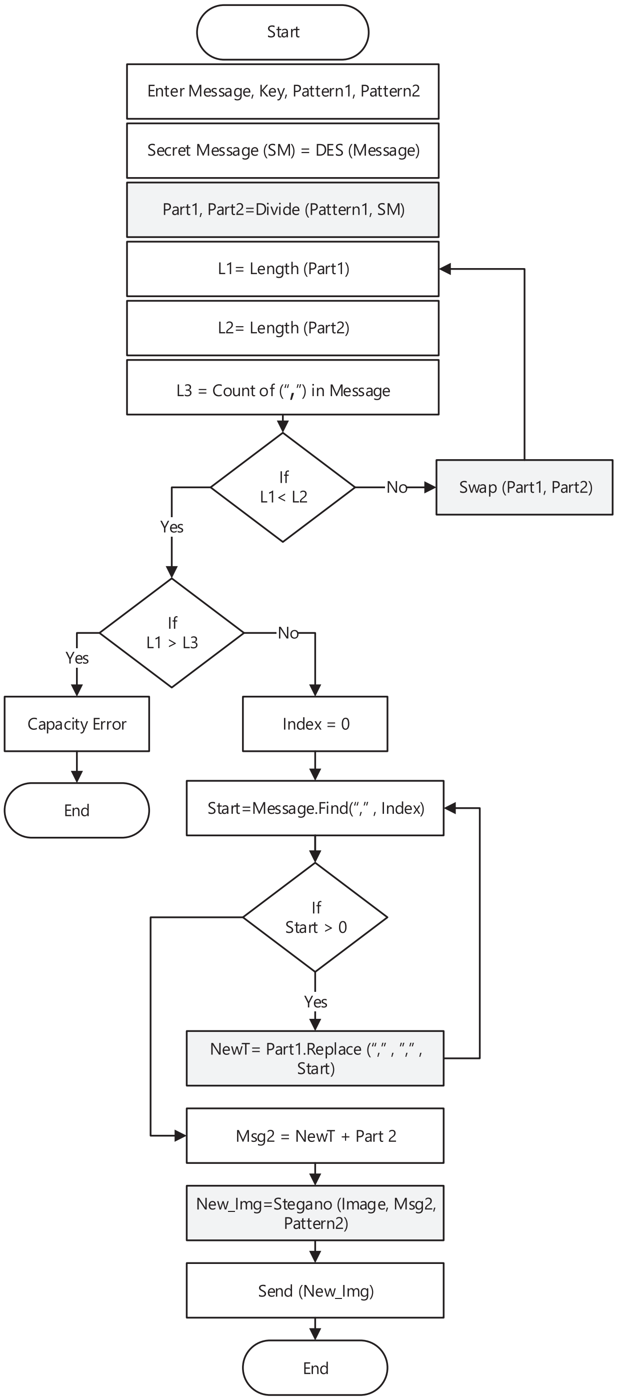

Start
Enter Message, Key, Pattern1, Pattern2
Secret Message (SM) = DES (Message)
Part1, Part2=Divide (Pattern1, SM)
L1= Length (Part1)
L2= Length (Part2)
L3 = Count of (",") in Message
If L1< L2
No
Swap (Part1, Part2)
Yes
If L1 > L3
Yes
Capacity Error
End
No
Index = 0
Start=Message.Find("," , Index)
If Start > 0
Yes
NewT= Part1.Replace ("," , "," , Start)
Msg2 = NewT + Part 2
New_Img=Stegano (Image, Msg2, Pattern2)
Send (New_Img)
End

Figure 6: Steps of the proposed approach

3.1 Algorithm 1-Steganography with Text

The proposed idea of Algorithm 1 depends on punctuation marks, especially the comma in Arabic and the comma in English. The algorithm replaces the Arabic comma “,” with the English comma “,” which are visually very similar. Users will not notice any difference in the text or size, especially since readers naturally focus more on the main content than other issues. Even if the reader has a good knowledge of syntax, they will not detect or doubt the change.

Moreover, if the size of the secret data is larger than the number of commas in the text, Algorithm 1 will merge the proposed method with the KASHIDA method. This merging will enhance the capacity and mislead the attacker, making their task more difficult. The next paragraph (Algorithm 1) shows the pseudocode of this algorithm.

Algorithm 1:

```
String Encrypt1 (String message, String Key, String Pattern1, String CoverText)
Start
Int L1 = Length (Part1);
Int  L2 = Find_Count( “  „ ”, CoverText  ); // Number of all Ar  or En Comma
Index = 0;
Int  j = 0;
If (L1 < L2)
    While (Index < L1)
        Bit b= msg[Index];
        j = find ( “,”, j)
        If (b)
            CoverText  [Index] = “  , “;
        Else
            CoverText  [Index] = “  , “;
        End
        Index ++;
    End While
Else
    return “Error Length, Change Pattern or CoverText”;
End IF
Return CoverText;
End Function
```

3.2 Algoirthm 2-Split and Merge Algorithm

This is the most important phase in the proposed approach. First, the algorithm encrypts the data using the DES or AES method (Symmetric Key). The results of encryption will be binary (bits). The algorithm depends on an agreed pattern (Pattern 1 like “1110110”) between sender and receiver to split data. Bits corresponding to “0” will be in Part 1, and the bits corresponding to “1” will be in Part 2. This pattern is repeated over the entire secret message. At the end, we will have a series of bits (Part 1, Part 2). Part 1 will be inserted in Text-Cover based on Algorithm 1. The results of Algorithm 1 will be merged with Part 2 and encrypted again. Then the whole encrypted data will be inserted in an Image-Cover based on Algorithm 2. The next paragraph (Algorithm 2) shows the pseudocode of this algorithm.

Algorithm 2:

```
String Divide_Message  (String message, Key, Pattern  1, CoverText, Image img)
Start
String Sec_msg  = DES.Encrypt(message, Key);
Binary [] msg  = Convert_To_Binary(Sec_Msg);
String Part1="";
String Part2="";
Int  index = 0;
For (int  i = 0; i < Pattern1.Length; i++)
     If (Patttern1 [i] ==  "0")
          Part1+=msg[index];
     Else
          Part2+=msg[index];
If (Index<msg.Length-1)
    Index++;
Else
    Break;
If (i==Pattern1.Length)
    i=0;
End For
CoverText  = Encrypt1 (string Part1, String Key, String Pattern1, String CoverText)
Image NewImg  = Encrypt2 (string Part2, Key, Pattern2, CoverText, Image img)
End Function.
```

3.3 Algorithm 3-Steganography with Image

As the proposed method targets drone applications, it is very important to use a simple algorithm that does not consume a lot of resources (memory, power, and CPU). For this reason, the algorithm depends on a spatial domain method, not a frequency one. We enhanced the Least Significant Bit (LSB) method by agreeing on Pattern 2 between the senders and receivers. Pattern 2 dictates the sequence of hiding in the color layers (R, G, and B) of the image cover. For example, if Pattern 2 equals "GBRR," then the first bit of the secret message will be hidden in the first pixel of the "G" layer, the second bit in the "B" layer, and the third and fourth bits in the "R" layer. Algorithm 3 then repeats this process until all bits of the secret data are hidden. The next paragraph (Algorithm 3) shows the pseudocode of this algorithm.

Algorithm 3:

```
Image NewImg  Encrypt2 (String message, Key, Pattern2, CoverText, Image img)
Start
String NewMsg  = CoverText  + Part2;
String Sec_msg2 = DES.Encrypt(NewMsg, Key);
Binary [] msg2 = Convert_To_Binary(Sec_Msg);
```

(Continued)

Algorithm 3 (continued)

```
//Hiding in Image
Index = 0;
Int  L = msg2.Length;
Int  n =0;
For (int  i=0; i<img.Length; i++) // Pattern2 like “RRGBB”
        If (Pattern2[index]== “R”)
                Img[R][i].ConvertToBinary [0]=msg2[n];
        Else if (Pattern2[index]== “G”)
                Img[G][i].ConvertToBinary [0]=msg2[n];
          Else
                Img[B][i].ConvertToBinary [0]=msg2[n];
          If (n==L−1)
                Break;
          Index++;
          Index = index % index.Length;
End For
Return img;
End Function
```

3.4 Features of the Proposed Approach

The proposed approach achieves many important advantages, which can be summarized in the following points:

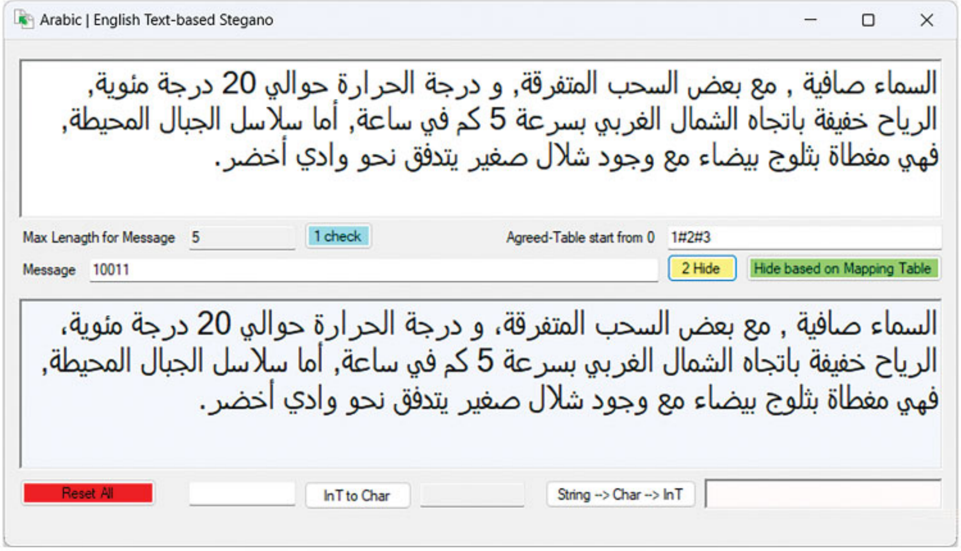
1. It is dynamic and does not require a mapping between the two parties, only requiring agreement on a shared encryption key with two patterns.
2. It is very difficult for the proposed approach to be observed with the naked eye, whether image or text.
3. It is not specific to a specific language, meaning that it is suitable for Arabic or English.
4. Difficulty in breaking and penetrating, and thus a high level of security. Even if the encryption key is discovered, it is very difficult to properly rearrange the encrypted data so that the attacker can decrypt it.
5. It uses the honeypot concept implicitly to increase the level of security.
6. It does not significantly affect performance.

4 Implementation and Results

In this section, first, the implementation and testing mechanism of the proposed approach are discussed. Then, a comparison of the proposed approach with other state-of-the-art methods [46] based on some evaluation criteria for steganography will be presented.

4.1 Implementation and Testing

The proposed algorithm was implemented using Visual Studio .NET 2019 with the C# programming language. This implementation aims to verify the applicability and effectiveness of the algorithm in information hiding and retrieval. Specifically, in digital agriculture, ensuring that sensitive information such as palm tree health and pest infestation levels remain confidential. Fig. 7 shows the application of the proposed algorithm for hiding Arabic text, and Fig. 8 shows its application with English text. Fig. 9 illustrates the application of the image steganography algorithm and displays the final results. It is worth noting that there is no significant visual difference in the image before and after hiding the data.


Arabic | English Text-based Stegano
1 check
2 Hide
Hide based on Mapping Table
Reset All
InT to Char
String --> Char --> InT

السماء صافية , مع بعض السحب المتفرقة, و درجة الحرارة حوالي 20 درجة مئوية,
الرياح خفيفة باتجاه الشمال الغربي بسرعة 5 كم في ساعة, أما سلاسل الجبال المحيطة,
فهي مغطاة بثلوج بيضاء مع وجود شلال صغير يتدفق نحو وادي أخضر.

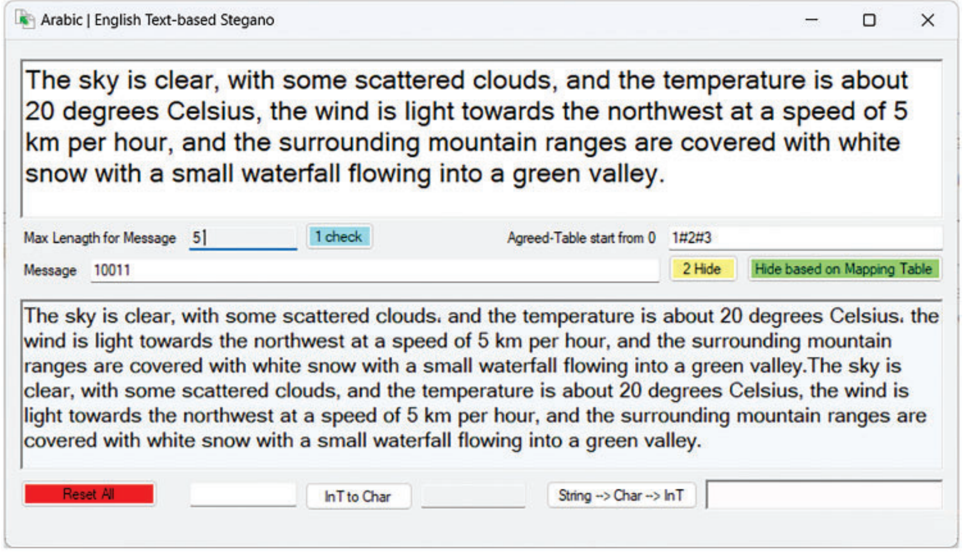
Max Lenagth for Message 5

Agreed-Table start from 0 1#2#3

Message 10011

السماء صافية , مع بعض السحب المتفرقة، و درجة الحرارة حوالي 20 درجة مئوية،
الرياح خفيفة باتجاه الشمال الغربي بسرعة 5 كم في ساعة, أما سلاسل الجبال المحيطة,
فهي مغطاة بثلوج بيضاء مع وجود شلال صغير يتدفق نحو وادي أخضر.

Figure 7: The implemented application of Text-based Steganography (Arabic)


Arabic | English Text-based Stegano
1 check
2 Hide
Hide based on Mapping Table
Reset All
InT to Char
String --> Char --> InT

The sky is clear, with some scattered clouds, and the temperature is about 20 degrees Celsius, the wind is light towards the northwest at a speed of 5 km per hour, and the surrounding mountain ranges are covered with white snow with a small waterfall flowing into a green valley.

Max Lenagth for Message 5

Agreed-Table start from 0 1#2#3

Message 10011

The sky is clear, with some scattered clouds، and the temperature is about 20 degrees Celsius، the wind is light towards the northwest at a speed of 5 km per hour, and the surrounding mountain ranges are covered with white snow with a small waterfall flowing into a green valley.The sky is clear, with some scattered clouds, and the temperature is about 20 degrees Celsius, the wind is light towards the northwest at a speed of 5 km per hour, and the surrounding mountain ranges are covered with white snow with a small waterfall flowing into a green valley.

Figure 8: The implemented application of Text-based Steganography (English)

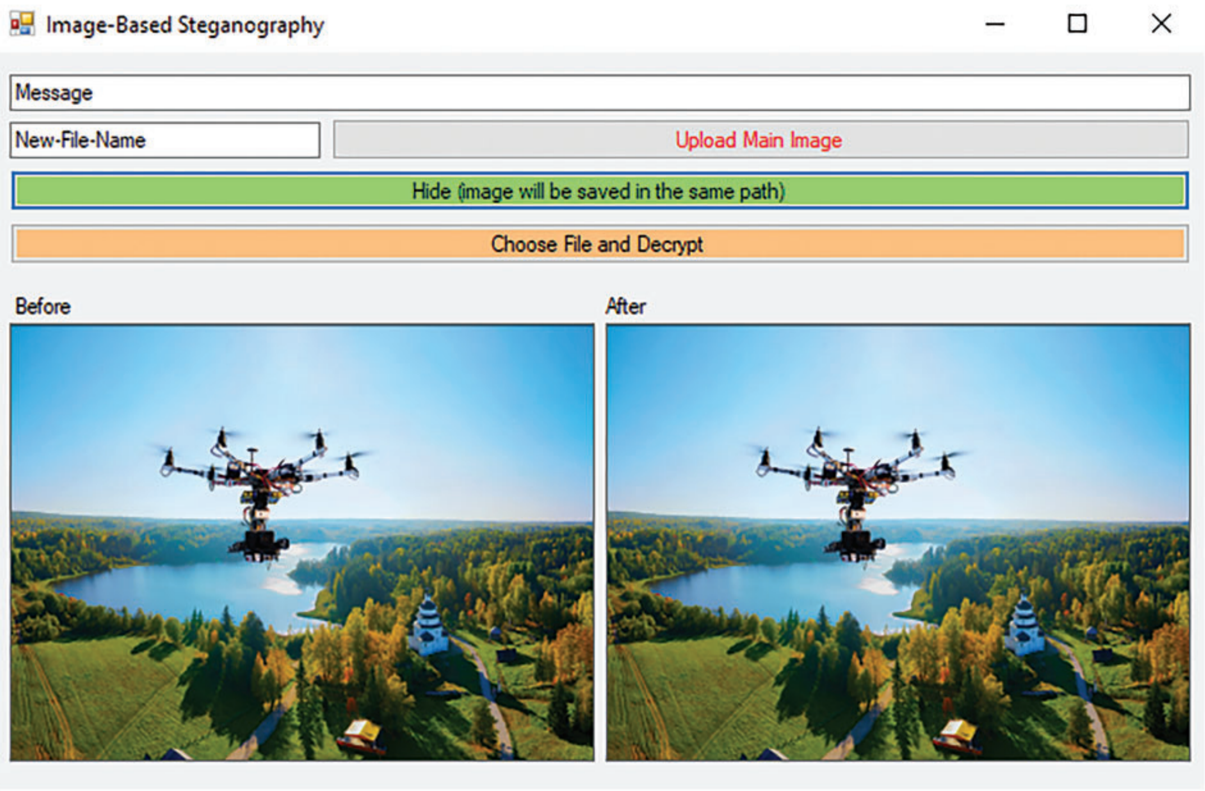


Figure 9: The implemented application of Image-based Steganography

The results demonstrate the algorithm's potential to securely transmit sensitive agricultural data collected by drones, ensuring that critical information remains protected against unauthorized access. To prove the effectiveness of the proposed approach in the criteria for evaluating steganography methods, which are [47–49]:

- Imperceptibility: According to Figs. 7 and 8, it is difficult for an ordinary person or even experts in the field to perceive the presence of hidden data within an image or text, even after decryption. This makes it superior to other methods that rely on letter shaping or changing Hamzas, which language experts can notice during text reading [47].
- Security: The proposed method achieves a very high level of protection due to the multi-stage steganography using two concealment algorithms, in addition to using data segmentation and the concept of attractor traps when selecting misleading information within the text.
- Flexibility: The proposed approach offers a high level of flexibility, which is concentrated in three basic points:
    - It can be used with more than one language, meaning that it is not linked to a specific language, for example, the Arabic language, as in the diacritics or Hamzat approach.
    - It does not require users to agree on mapping or a specific schedule for changing places before each encryption process, as in the diacritics or Hamzat approach.
    - The proposed approach can be integrated with other methods, such as the KASHIDA method, or by using the frequency domain instead of the spatial domain for hiding within the image.

- Capacity: The proposed approach solves the problem or negative present in the Multi-Layers or Double Steganography approach through the idea of segmenting the data using Pattern 1 so that a small part is hidden within the text and a large part within the image, instead of hiding the entire message within the text and then the text within the image. In this way, the proposed approach was able to achieve a higher level of security and at the same time higher capacity [48].
- Robustness: In hiding within texts, immunity is as high as possible, as even compression algorithms do not affect textual data. However, in the case of hiding within the image, the hidden data may be affected in the event of recovery when compression or modification is applied to the cover image. This applies if the LSB approach is used, but if the Frequency Domain approach is used, Robustness will become higher, but this will affect performance.
- Usability: The proposed approach achieves ease of use in that it only requires users to agree on an encryption key with two patterns. It also does not require the user to impose strict requirements on choosing the text or cover image.
- Performance: The proposed algorithm does not require much performance. It uses a simple method of hiding within the text in addition to a simple method of hiding within the image. Through testing, it appears that the time is good with LSB, however, as we mentioned, if we work on the Frequency Domain approach, performance will be negatively affected compared to the LSB approach, but this will achieve higher Robustness. Therefore, there can be parity between Robustness and Performance based on available resources [49].

4.2 Results and Discussion

To verify the strength of the proposed three-phase algorithm, a set of experiments and comparisons were conducted to prove the strength of the proposed algorithm. Here we test three algorithms in addition to our algorithm: Dynamic Bit Encoding, data hiding using Pattern-Based Techniques, and data hiding using Adaptive Filters [50–53]. Dynamic Bit Encoding adds randomness to enhance security, while Pattern-Based Techniques rely on specific hiding patterns and are easy to implement. Finally, hiding data using adaptive filters: Image analysis and adaptive filters are used to hide data intelligently and reduce the effect of noise.

First, the execution times of the four algorithms were measured, and then the robustness of the text was measured (Fig. 10).

To compare the Robustness of different algorithms, we can introduce noise into the original image after hiding the text and then measure the extent to which the hidden data is affected by this noise. Criteria such as hidden text re-extraction error ratio or mean squared error (MSE) (Eq. (1)) can be used to evaluate the effect. Storage capacity using Peak Signal-to-Noise Ratio (PSNR): It is used to measure image quality after performing operations such as compression or data masking. The following (Eq. (2)) is used to calculate PSNR [54].

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I\,(i,j) - K\,(i,j)]^2 \tag{1}$$

where m and n are the dimensions of the image.

MAX_I is the maximum possible image pixel value. In images with 8 bits, the value is 255.

$I(i,j)$ is the pixel value at location (i, j) in the original image.

$K(i,j)$ is the pixel value at location (i, j) in the modified image.

$$PSNR = 20log_{10} \frac{MAX\_I}{\sqrt{MSE}} \tag{2}$$

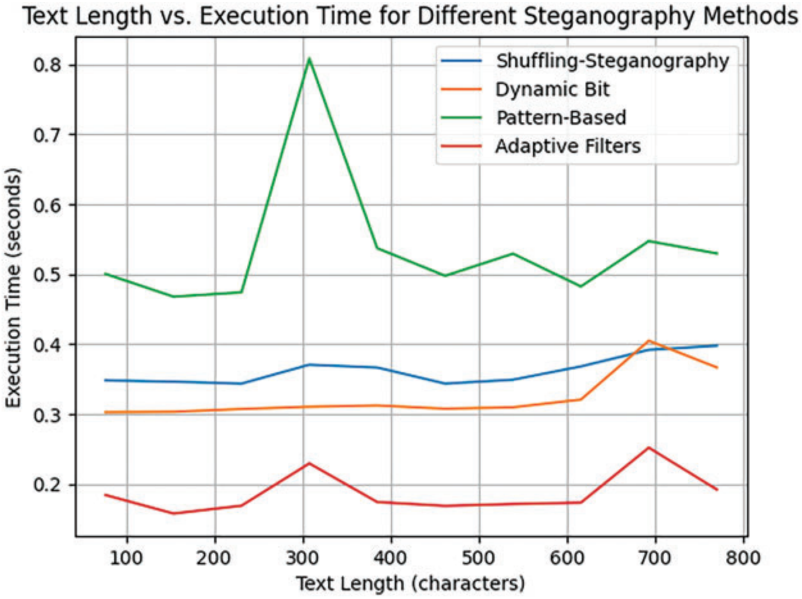


Figure 10: Secret message length *vs*. execution time

The PSNR curve is shown in Fig. 11. The higher the PSNR value the better the image quality, as it indicates that the difference between the original image and the modified image is small. In contrast, low values mean that there is a large difference between the original and the modified image. For our approach, the results normally are closed to other methods.

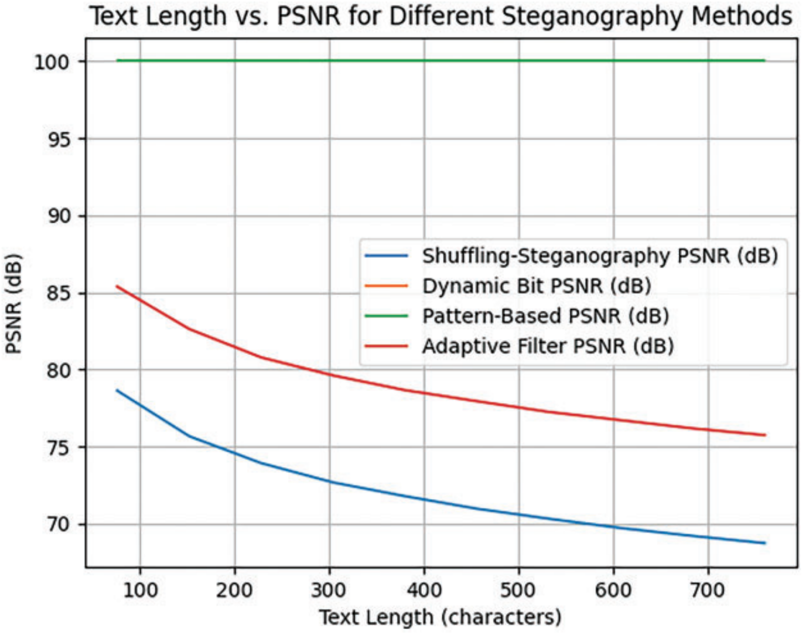


Figure 11: Secret message length *vs*. PSNR. The *X* axis represents the length of text (number of characters) hidden in the image. The *Y* axis represents the PSNR value in decibels (dB)

The same principle applies to the error extraction rate, which serves as a measure of the accuracy in extracting hidden text from a medium that has been subjected to noise or modifications (See Fig. 12). This metric quantifies the number of incorrectly extracted characters or bits relative to the total length of the hidden text. The process begins by embedding the original text within the image using a data hiding algorithm. Subsequently, noise is randomly introduced to the medium to emulate environmental effects or potential attacks. The hidden text is then retrieved from the altered image using the same algorithm [55].

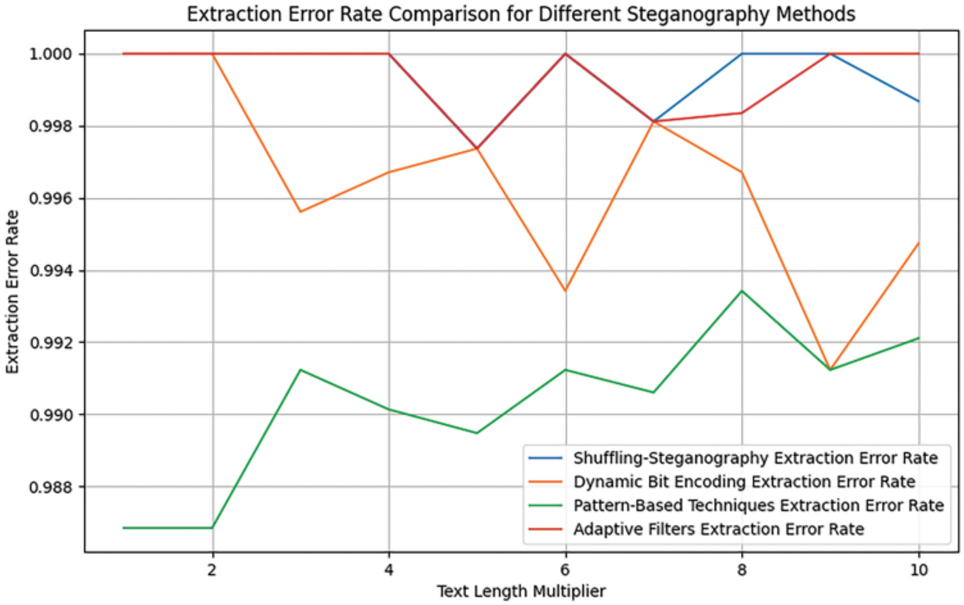


Figure 12: Comparison based extraction error rate

Calculating the error rate: The original text is compared to the extracted text on a character-by-character or bit-by-bit basis. The number of errors, defined as the characters or bits that were extracted incorrectly, is computed using the following (Eq. (3)):

Calculate the error extraction ratio:

$$\text{Error Rate} = \frac{\textit{the number of mistiken bit of letter}}{\textit{length of original message}} \tag{3}$$

To understand the computational complexity of different algorithms, we calculated the time it takes to execute each algorithm on a set of texts of increasing lengths. Fig. 13 depicts a curve showing the relationship between text length and execution time for each algorithm.

To compare the security of different data steganography algorithms, we used a common security criterion: Cipher-Text Redundancy. Although this is not a direct measure of security, it can be a good indicator of the complexity of the hidden text.

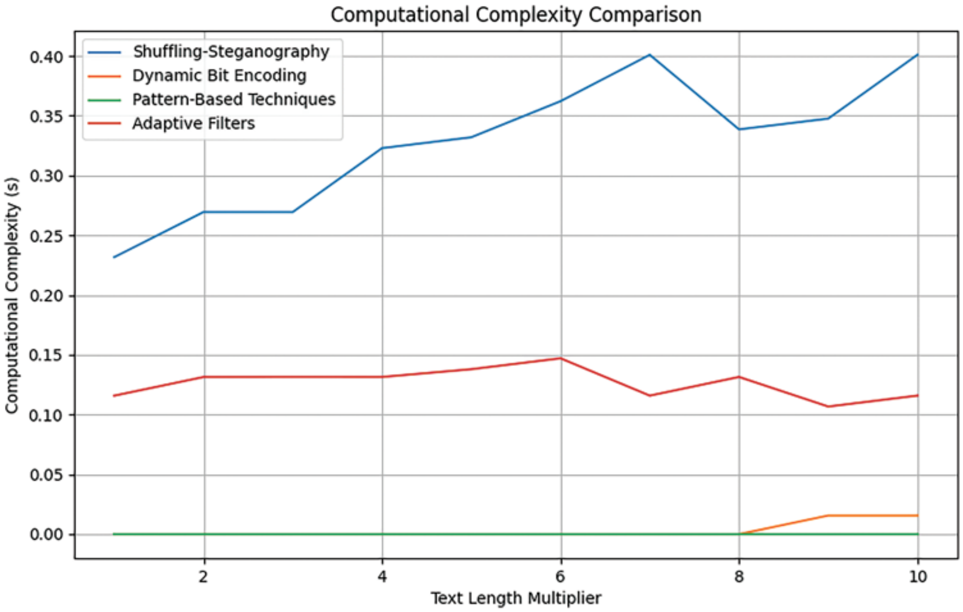


Figure 13: Comparison based computational complexity

In the context of data hiding, we used a method to determine how strong the encryption is and how complex the hidden text is. For example, the Shannon Entropy measure is used to measure the complexity of hidden text.

Shannon Entropy is a mathematical measure of the complexity and unpredictability of data. This measure is used in information theory to analyze the probability distribution of letters or symbols in a given text [56]. The mathematical principle of Shannon Entropy calculation is given by the following (Eq. (4)):

$$H\left(x\right) = -\sum\nolimits_{i=1}^{n} P\left(x_i\right) log_2 P\left(x_i\right) \tag{4}$$

X is a random variable representing the set of symbols or characters.

x_i is the symbol or letter i in the set.

$P(x_i)$ is the relative probability of the symbol.

n is the number of different symbols or letters in the text.

Considering that the Shannon Entropy of the proposed algorithm is much higher compared to other algorithms (Fig. 14), this indicates that the hidden text using this algorithm is more complex and secure.

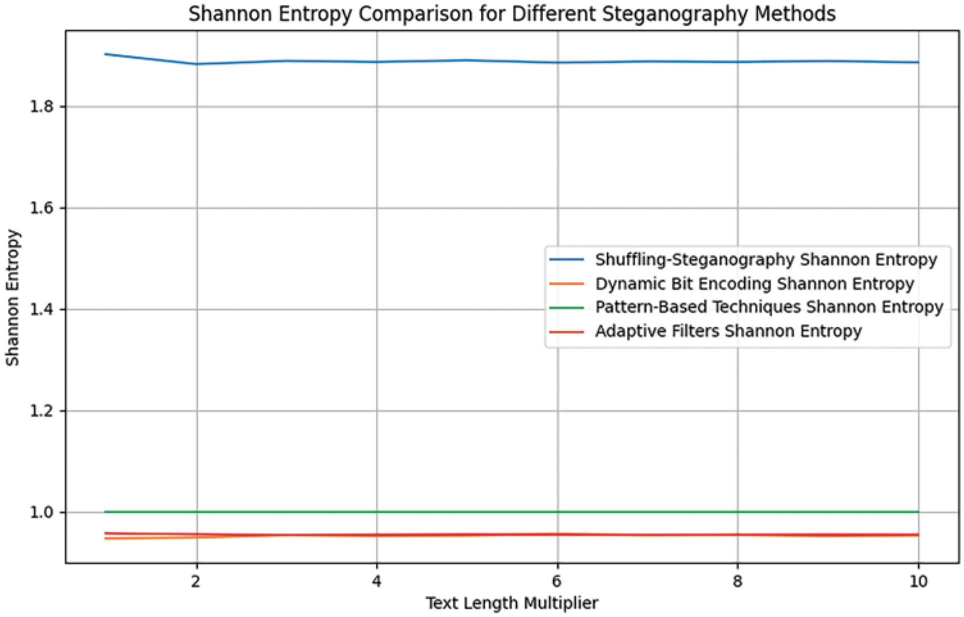


Figure 14: Comparison based shannon entropy

4.3 Advanced Security Measurement

A brute force attack involves an exhaustive search of all possible steganography keys until the correct one is identified. Due to the complexity of the described steganography techniques, this attack faces significant challenges. The proposed steganography method uses predefined patterns that can be accessed from a wide range of images across various platforms such as the web, mobile phones, and computers. This diversity results in a large number of unique steganography patterns, which complicates the brute force approach. Moreover, the attackers must guess the size of the secret message, as it is directly related to the size of the pattern. The text is inserted according to a random sequence that is affected by the color range distribution of the steganography design and the number of matching pixels, which makes it difficult to recover the steganography text because the text is hidden across different addresses in each block, which are determined by the properties of the cover and the chosen steganography pattern.

This article presents a novel approach to stealth using the LSB technique and employing AES encryption algorithms to secure the text inside the image. By randomizing the pixels and masking as the encryption key, this method enhances the inherent limitations of the LSB process. The security of this method is formally analyzed using a symmetric key-based security model. This method is secure against attacks that attempt to recover the hidden text, as security relies on the adversary's ability to distinguish between the cipher-text and random samples oracle generated by the system $O_D(.)$, making it difficult for the attacker to uncover the hidden information.

Mathematically, the security of the steganography scheme Σ_D is defined as:

$$\left|Pr\left[A_D^{Encode_D(k,.,.)}=1\right]-Pr\left[A_D^{O_D(.)}=1\right]\right|<negl\left(\lambda\right)$$

where A_D is the adversary, $Encode_D\ (k, ., .)$ is the encoding oracle with key k, and $O_D\ (.)$ is the random sampling oracle. This ensures that the encoded messages are indistinguishable from random samples, thus maintaining a high level of security.

Future developments such as encryption and data compression technologies, as well as the use of artificial intelligence, promise to increase the ability to resist decryption attempts and reveal hidden information. These techniques overcome the problems of traditional LSB steganography methods by using a secret key for each image and dividing the image into smaller parts. This increases the security of the hidden text and makes it less visible within the image. In addition, dividing the image into multiple parts and changing their order makes this method more robust to attacks and enhances overall security.

4.4 Disadvantages of the Proposed Approach and Future Work

The proposed approach suffers from some drawbacks or limitations, which can be summarized in the following points:

The amount of data that can be stored within the text is small, and therefore this must be taken into account within the chosen segmentation pattern or in choosing a very large text that contains many punctuation marks. Note that the stage of hiding within the image ensures the hiding of a large amount of data. The objective of using text is to hide part of the encrypted data, making it difficult for the attacker to reconfigure the encrypted string. As a result, they will not be able to decrypt it correctly even if they discover the encryption key. Moreover, to increase the data hidden within the text, the proposed steganography method can be easily combined with the KASHIDA method to enclose large amounts without affecting the level of protection.

Robustness: modification or compression attacks, for example, will affect hidden data. The main goal is to ensure a high level of security and performance, which was the focus of the proposed approach. However, if a higher level of robustness is desired, the LSB technology can be replaced with a frequency domain-based method, though this may slightly impact performance.

The proposed approach requires agreement on three keys: the encryption key and two patterns, one for hashing and the other for the inserting algorithm within the images. The previous requirements can be bypassed by using a specific algorithm to select the encryption key. This algorithm would include one part representing the fragmentation pattern and another part for the embedding pattern within the image layers.

5 Conclusion

This research introduced a new steganography approach that combines text and image steganography to improve security in IoT applications, especially in drone applications. This is achieved through a dividing algorithm that uses patterns between parties. The research introduced a new method for hiding textual information using punctuation. Additionally, it proposed a simple method for image-based steganography that relies on different layers of sequencing using an agreed pattern. The proposed approach achieved excellent results in steganography evaluation criteria imperceptibility, security, flexibility, capacity, robustness, usability, and performance through implementation and comparison. Moreover, the approach is adaptable to integration with other methods. This flexibility makes it particularly useful for digital agriculture, where the protection of sensitive data can lead to significant improvements in farming efficiency and productivity. Finally, the research paved the way for proposing automated algorithms to generate the patterns from the agreed encryption key itself, in addition to exploring other methods for text hiding, such as embedding dummy data or rearranging encrypted secret data. Future work could focus on implementing these automated algorithms in real-world agricultural scenarios, further validating their effectiveness in protecting sensitive data collected by drones.

Acknowledgement: This work was fully funded by the Research Deanship of the Islamic University of Madinah. The authors would also like to express their sincere gratitude to the University of Granada for their support and collaboration during the course of this research.

Funding Statement: This work was fully funded by the Research Deanship of the Islamic University of Madinah under grant number 966.

Author Contributions: Ahmad B. Alkhodre, Nour Mahmoud Bahbouh: Conceptualization, Methodology, Writing—Original draft, Writing—Reviewing and Editing, Investigation. Sandra Sendra, Adnan Ahmed Abi Sen: Conceptualization, Methodology, Writing—Reviewing and Editing, Supervision, Funding Acquisition, Conceptualization, Investigation. Yazed Alsaawy, Hani Almoamari, Abdallah Namoun, Saad Said Alqahtany: Conceptualization, Investigation, and Writing—Reviewing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: The authors have read and followed the ethical requirements for publication in CMC and confirm that the current work does not involve human subjects, animal experiments, or any data collected from social media platforms.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. M. S. M. Daud *et al.*, "Applications of drone in disaster management: A scoping review," *Sci. Justice*, vol. 62, no. 1, pp. 30–42, 2022. doi: 10.1016/j.scijus.2021.11.002.

[2] S. Ahirwar, R. Swarnkar, S. Bhukya, and G. Namwade, "Application of drone in agriculture," *Int. J. Curr. Microbiol. Appl. Sci.*, vol. 8, no. 1, pp. 2500–2505, 2019. doi: 10.20546/ijcmas.2019.801.264.

[3] Á. Restás, "Drone applications fighting COVID-19 pandemic—Towards good practices," *Drones*, vol. 6, no. 1, 2022, Art. no. 15. doi: 10.3390/drones6010015.

[4] M. A. Hoque, M. Hossain, S. Noor, S. R. Islam, and R. Hasan, "IoTaaS: Drone-based Internet of Things as a service framework for smart cities," *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12425–12439, 2021. doi: 10.1109/JIOT.2021.3137362.

[5] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Prog. Aerosp. Sci.*, vol. 91, no. 4, pp. 99–131, 2017. doi: 10.1016/j.paerosci.2017.04.003.

[6] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, 2020, Art. no. 100218. doi: 10.1016/j.iot.2020.100218.

[7] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: A survey," *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, 2018. doi: 10.1007/s41870-018-0113-4.

[8] A. A. Abi Sen and A. M. Basahel, "A comparative study between security and privacy," in *2019 6th Int. Conf. Comput. Sustain. Global Dev. (INDIACom)*, New Delhi, India, IEEE, 2019, pp. 1282–1286.

[9] N. Arora, “Types and tools of steganography,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 2049–2053, 2022. doi: 10.22214/ijraset.2022.44279.

[10] H. Wen, Y. Lin, L. Yang, and R. Chen, “Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos,” *Expert. Syst. Appl.*, vol. 250, no. 1, 2024, Art. no. 123748. doi: 10.1016/j.eswa.2024.123748.

[11] H. Wen and Y. Lin, “Cryptanalyzing an image cipher using multiple chaos and DNA operations,” *J. King Saud Univ.—Comput. Inf. Sci.*, vol. 35, no. 7, 2023, Art. no. 101612. doi: 10.1016/j.jksuci.2023.101612.

[12] H. Wen, Y. Lin, and Z. Feng, “Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps,” *Eng. Sci. Technol., Int. J.*, vol. 51, no. 14, 2024, Art. no. 101634. doi: 10.1016/j.jestch.2024.101634.

[13] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, “Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding,” *IEEE Access*, vol. 9, pp. 145459–145470, 2021. doi: 10.1109/ACCESS.2021.3123571.

[14] W. Feng *et al.*, “Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption,” *Expert. Syst. Appl.*, vol. 246, no. 3, 2024, Art. no. 123190. doi: 10.1016/j.eswa.2024.123190.

[15] R. Adee and H. Mouratidis, “A dynamic four-step data security model for data in cloud computing based on cryptography and steganography,” *Sensors*, vol. 22, no. 3, 2022, Art. no. 1109. doi: 10.3390/s22031109.

[16] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, “A review on text steganography techniques,” *Mathematics*, vol. 9, no. 21, 2021, Art. no. 2829. doi: 10.3390/math9212829.

[17] B. Sharma, “A comparative overview & analysis of text and image steganography,” *Think India J.*, vol. 22, no. 12, pp. 297–305, 2019.

[18] M. Kumar, S. Kumar, and H. Nagar, “Comparative analysis of different steganography technique for image or data security,” *Int. J. Adv. Sci. Technol. (IJAST)*, vol. 29, no. 4, pp. 11246–11253, 2020.

[19] A. A. Idres and H. I. Yaseen, “Text steganography techniques: A review,” *Int. Res. J. Innov. Eng. Technol.*, vol. 7, no. 11, 2023, Art. no. 648.

[20] R. Kumar and H. Singh, “Recent trends in text steganography with experimental study,” in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Springer: Cham, 2020, pp. 849–872.

[21] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi, N. A. Roslan and R. Din, “A comparative analysis of Arabic text steganography,” *Appl. Sci.*, vol. 11, no. 15, 2021, Art. no. 6851. doi: 10.3390/app11156851.

[22] R. H. Ali and J. M. Kadhim, “Text-based steganography using Huffman compression and AES encryption algorithm,” *Iraqi J. Sci.*, pp. 4110–4120, 2021. doi: 10.24996/ijs.2021.62.11.31.

[23] S. Zhang, Z. Yang, J. Yang, and Y. Huang, “Linguistic steganography: From symbolic space to semantic space,” *IEEE Signal Process. Lett.*, vol. 28, pp. 11–15, 2020. doi: 10.1109/LSP.2020.3042413.

[24] N. Alanazi, E. Khan, and A. Gutub, “Functionality-improved Arabic text steganography based on unicode features,” *Arab. J. Sci. Eng.*, vol. 45, no. 12, pp. 11037–11050, 2020. doi: 10.1007/s13369-020-04917-5.

[25] S. S. Alqahtany, A. B. Alkhodre, A. Al Abdulwahid, and M. Alohaly, “A dynamic multi-layer steganography approach based on arabic letters,” *Diacritics Image Layers. Appl. Sci.*, vol. 13, no. 12, 2023, Art. no. 7294. doi: 10.3390/app13127294.

[26] R. H. Ali, B. N. Dhannoon, and M. I. Hamel, “Arabic text steganography using lunar and solar diacritics,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 3, pp. 1559–1567, 2023. doi: 10.11591/ijeecs.v31.i3.pp1559-1567.

[27] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “Image steganography: A review of the recent advances,” *IEEE Access*, vol. 9, pp. 23409–23423, 2021. doi: 10.1109/ACCESS.2021.3053998.

[28] R. Din, “Comparison of steganographic techniques of spatial domain and frequency domain in digital images,” *Borneo Int. J.*, vol. 6, no. 3, pp. 109–118, 2023.

[29] A. M. Alhomoud, “Image steganography in spatial domain: Current status, techniques, and trends,” *Intell. Autom. Soft Comput.*, vol. 27, no. 1, pp. 69–88, 2021. doi: 10.32604/iasc.2021.014773.

[30] G. Maji, S. Mandal, and S. Sen, “Cover independent image steganography in spatial domain using higher order pixel bits,” *Multimed. Tools Appl.*, vol. 80, no. 10, pp. 15977–16006, 2021. doi: 10.1007/s11042-020-10298-6.

[31] S. T. Alam, N. Jahan, and M. M. Hassan, “A new 8-directional pixel selection technique of LSB based image steganography,” in *Cyber Secur. Comput. Sci.: Second EAI Int. Conf., ICONCS 2020,* Dhaka, Bangladesh, 2020, vol. 2, 101–115.

[32] S. S. Ahmed and S. A. Mehdi, “Multi-layer security for color image based on five-dimension chaotic system and image steganography algorithm,” in *2022 Int. Conf. Data Sci. Intell. Comput. (ICDSIC),* Karbala, Iraq, IEEE, 2022, pp. 170–174.

[33] Y. Luo, J. Qin, X. Xiang, and Y. Tan, “Coverless image steganography based on multi-object recognition,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2779–2791, 2020. doi: 10.1109/TCSVT.2020.3033945.

[34] S. Mukherjee and G. Sanyal, “Edge based image steganography with variable threshold,” *Multimed. Tools Appl.*, vol. 78, no. 12, pp. 16363–16388, 2019. doi: 10.1007/s11042-018-6975-4.

[35] S. N. Ahmed, S. Chandra, and V. Todwal, “Image steganography using time and frequency domain,” *Int. J. Res. Eng., Sci. Manag.*, vol. 2, no. 8, pp. 278–280, 2019.

[36] S. K. Yadav and R. K. Bhogal, “A video steganography in spatial, discrete wavelet transform and integer wavelet domain,” in *2018 Int. Conf. Intell. Circuits Syst. (ICICS)*, IEEE, Apr. 2018, pp. 258–264.

[37] M. S. Memon and A. Shah, “A novel text steganography technique to Arabic language using reverse Fat5Th5Ta,” *Pak. J. Eng., Technol. Sci.*, vol. 1, no. 2, 2015. doi: 10.22555/pjets.v1i2.167.

[38] N. A. Roslan, R. Mahmod, and N. I. Udzir, “Sharp-edges method in Arabic text steganography,” *J. Theor. Appl. Inf. Technol.*, vol. 33, no. 1, pp. 32–141, 2011.

[39] O. Kocak, U. Erkan, A. Toktas, and S. Gao, “PSO-based image encryption scheme using modular integrated logistic exponential map,” *Expert Syst. Appl.*, vol. 237, 2024, Art. no. 121452.

[40] Y. Gao, J. Liu, and S. Chen, “Image encryption algorithms based on two-dimensional discrete hyperchaotic systems and parallel compressive sensing,” *Multimed. Tools Appl.*, vol. 83, no. 19, pp. 57139–57161, 2024. doi: 10.1007/s11042-023-17745-0.

[41] F. Toktas, U. Erkan, and Z. Yetgin, “Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions,” *Expert. Syst. Appl.*, vol. 249, no. 8, 2024, Art. no. 123583. doi: 10.1016/j.eswa.2024.123583.

[42] N. Baranwal, K. N. Singh, and A. K. Singh, “Using chaos to encrypt images with reconstruction through deep learning model for smart healthcare,” *Comput. Electr. Eng.*, vol. 114, no. 3, 2024, Art. no. 109089. doi: 10.1016/j.compeleceng.2024.109089.

[43] U. Erkan, A. Toktas, and Q. Lai, “2D hyperchaotic system based on Schaffer function for image encryption,” *Expert. Syst. Appl.*, vol. 213, no. 17, 2023, Art. no. 119076. doi: 10.1016/j.eswa.2022.119076.

[44] A. M. N. Gilmolk and M. R. Aref, “Lightweight image encryption using a novel chaotic technique for the safe internet of things,” *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, 2024, Art. no. 146. doi: 10.1007/s44196-024-00535-3.

[45] S. O. Hwang, H. M. Waseem, and N. Munir, “Billiard quantum chaos: A pioneering image encryption scheme in the post-quantum era,” *IEEE Access*, vol. 12, pp. 85150–85164, 2024.

[46] Y. Alsaawy, A. A. Abi Sen, A. Alkhodre, N. M. Bahbouh, N. A. Baghanim and H. B. Alharbi, “Double steganography-new algorithm for more security,” in *2021 8th Int. Conf. Comput. Sustain. Global Dev. (INDIACom)*, IEEE, Mar. 2021, pp. 370–374.

[47] A. Al-Mohammad, “Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility,” Doctoral dissertation, Brunel Univ., School of Inf. Syst., 2010.

[48] T. Rabie, M. Baziyad, T. Bonny, and R. Fareh, “Toward a unified performance metric for benchmarking steganography systems,” *J. Circuits, Syst. Comput.*, vol. 29, no. 3, 2020, Art. no. 2050042. doi: 10.1142/S0218126620500425.

[49] R. Sharma, R. Ganotra, S. Dhall, and S. Gupta, “Performance comparison of steganography techniques,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 9, pp. 37–46, 2018. doi: 10.5815/ijcnis.2018.09.04.

[50] K. Juneja and S. Bansal, “Frame selective and dynamic pattern based model for effective and secure video watermarking,” *Int. J. Comput.*, vol. 18, no. 2, pp. 207–219, 2019. doi: 10.47839/ijc.18.2.1419.

[51] R. Roselinkiruba, T. S. Sharmila, and J. J. Julina, "A novel pattern-based reversible data hiding technique for video steganography," 2022. Accessed: Jun. 22, 2024. Available: https://www.researchsquare.com/article/rs-1619375/v1

[52] Priyanka, N. Baranwal, K. N. Singh, O. P. Singh, and A. K. Singh, "HIDDEn: Robust data hiding for medical images with encryption and local binary pattern," *Circuits, Syst., Signal Process.*, vol. 43, pp. 1–21, 2024.

[53] P. K. Singh, B. Jana, and K. Datta, "Robust data hiding scheme through distinct keypoint selection exploiting modified Bilateral-Laplacian SIFT with encoding pipeline," *Displays*, vol. 74, no. 1, 2022, Art. no. 102268. doi: 10.1016/j.displa.2022.102268.

[54] Y. L. Pan and J. L. Wu, "Rate-distortion-based stego: A large-capacity secure steganography scheme for hiding digital images," *Entropy*, vol. 24, no. 7, 2022, Art. no. 982. doi: 10.3390/e24070982.

[55] R. Agrawal and K. Ahuja, "CSIS: Compressed sensing-based enhanced-embedding capacity image steganography scheme," *IET Image Process.*, vol. 15, no. 9, pp. 1909–1925, 2021. doi: 10.1049/ipr2.12161.

[56] K. H. Ng, S. C. Liew, and F. Ernawan, "An improved RDWT-based image steganography scheme with qr decomposition and double entropy," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 3, 2020. doi: 10.14569/issn.2156-5570.