Arabic text steganography using lunar and solar diacritics

Rawaa Hamza Ali[1], Ban Nadeem Dhannoon[2], Mohammed Iedan Hamel[3]
[1]Department of Biology, College of Science, University of Misan, Maysan, Iraq
[2]Department of Computer Science, College of Science, Al Nahrain University, Baghdad, Iraq
[3]Department of Artificial Intelligence, Missan Oil Company, Maysan, Iraq

Article Info

Article history:

Received Jan 5, 2023
Revised Apr 24, 2023
Accepted May 6, 2023

Keywords:

Arabic text
Diacritics
Hamzah Al-Wasl
Solar and lunar letters
Steganography

ABSTRACT

The need to hide essential information has rapidly increased as mobile devices and the internet has overgrown. Steganography is a method created to create hidden communication. Recently, methods have been developed to hide important information using text steganography. This work-study takes advantage of the possibility of concealing data in all diacritics after the two letters (ال) in the cover text. In the presented study, we propose a new algorithm in steganography in Arabic text as a cover text. After pre-processing the cover text, the algorithm hides the elements of secret messages inside the Arabic letters by adding appropriate diacritics (like Hamzah Al-Wasl) on the extracted words beginning with (ال) according to its third letter type (solar or lunar). In the proposed algorithm, the length of the secret message is determined so that the intended recipient can extract the hidden message accurately. The proposed algorithm is robust against the attack because the change in the cover text is small and imperceptible. On the other hand, since Arabic is used as a cover text, the breadth of the inclusion depends on the number of words beginning with (ال) definition.

Corresponding Author:

Rawaa Hamza Ali
Department of Biology, College of Science, University of Misan
Maysan, Iraq
Email: rawaaha@uomisan.edu.iq

1. INTRODUCTION

Communication via digital media is becoming more and more vital in human existence as social networks, the Internet, mobile platforms, and the internet of things (IoT) grow in popularity. It has yet opened up new ways for attackers to collect vital information from others with not much effort. As a result, issues related to security and vulnerability have become a vital concern [1]. Numerous approaches for protecting sensitive data were created, such as watermarking, cryptography, steganography, and secret sharing [2]. Data hiding and encryption are two basic approaches that play essential roles in information security. In addition, data encryption is a type of cryptography that converts a confidential message into a scribbled enciphered form before sending it via a private or public channel [3]. As a result, following encryption, the carrier object has no value. Information hiding is called “steganography”; in greek, this means “covered writing” [4]; it conceals the secret message during transmission through a public (untrusted) communication channel, making it invisible/unnoticed. The key distinction between information hiding and cryptography is invisibility [5]. Combining encryption with steganography allows for better private communication [6]. Secret messages are covered in unclear media with the use of steganography. Steganography is one of the methods that has been given more regard in latest years [7].

The significant point of stowing away data is to keep individuals from realizing the presence of stowed-away data. Generally, there are different kinds of cover media, like video, picture, text, sound [8], [9], and network or DNA [5]. The term steganography is gotten from two greek words: the primary word is steganó (concealed or covered), while the subsequent word is realistic (writing). Generally, there are two significant cycles to conceal data. Initially, privileged information may be hidden in cover media via embedding. Second, extractions may be used for recovering secret bits from stego text [10]. In steganography information hiding, there are three characteristics in which the systems compete with each other: security, robustness, and capacity.

In addition, security is vital when secret communication is maintained undetectable and confidential via eavesdroppers, while capacity indicates the amount of information that can be hidden in the cover medium. Finally, robustness is defined as the change a stego medium could resist before an adversary may damage its hidden data [11], [12]. This research suggests a security approach to concealing Arabic script by employing diacritics in lunar and solar characters. Our approach suggests hiding the secret message in Arabic script using diacritics on the lunar and solar letters, which is a novel aspect of the natural occurrence of diacritics as features of the Arabic language. The decision to hide confidential information in diacritics in the stego wrapper text depends on the diacritics which appear after the two letters (ال) in the word in the embedding process.

Similar efforts in text steganography utilizing the Arabic language are exploited in this section. In 2007, the authors presented a fresh steganography technique appropriate for texts in Arabic. It falls under the category of steganography feature coding techniques. The method uses the inherited points of the letters to conceal hidden information bits within them. The plan considers two attributes, the presence of focuses in the letters and the excess Arabic augmentation character, to distinguish the particular letters holding secret pieces [13]. Majumder *et al.* [9] described an enhanced approach for Arabic letters by hiding information using two diacritics (the kasra and fatha). Their suggested approach demonstrated good robustness and low-capacity quality. Kadhem and Wameedh [14] employed diacritics for differentiating between words with the same alphabet so that each one of the words is pronounced differently, and they also used them for hiding the "10" bit. In contrast, the rest of the diacritics included the 0 bit. Fatha is responsible for roughly half of all Arabic script diacritics. This method has the drawback of failing to capture the reader's attention. Nofaie *et al.* [15] proposed broadening the limit of their procedure by adding two progressive Kashida characters between connected characters for the situation when the secret piece is one and two between irrelevant characters assuming the secret piece is two. This approach is limited since it embeds whitespaces and Kashida utilizing detached and associated characters. However, because this event is viewed as rare in Arabic texts, the variety in the quantity of Kashidas starting with a single word and then onto the next may set off a per user's questions. Obeidat [16] developed a unicode-based Arabic text steganography algorithm. The method slightly modifies the related characters without changing their shape or size. The capacity regarding such a method was determined by considering just initial and isolated letters, which have a capacity of 2.90% or less.

Alhusban and Alnihoud [17], suggested masking two secret bits. The secret bits are hidden through the presence of Kashida after a non-pointed or pointed letter in the suggested design. This approach increases the capacity of employing a single letter to hide two secret bits. One of the drawbacks of such a long calculating time is. Shaker *et al.* [18], the authors introduced an information-concealing methodology relying upon lunar and solar characters, with a couple of Kashidas remembered for the occasion of the mysterious piece. Another downside regarding such a paper is its restricted limit, as it relies on Kashida to address secret address parts. Tayyeh *et al.* [19] utilized the sun, moon and unicode letters to conceal the mysterious pieces. When the mystery bit is 1, the algorithm looks for a word that starts with (ال) and is prevailed by a sun letter to change the disengaged letter (ا) to its matching code. Also, because not all words contain moon and sun letters, the approach has a low capacity; as a result, different words in a sentence must be passed over to hide the secret bits. In 2020, the authors hid data using text characters called pseudo-spaces. They presented two types of research for this text steganography using Kashida (extension character) alone and integrated with pseudo-spaces as the traditional Arabic text steganography methods. According to experimental findings, the proposed algorithms outperformed state-of-the-art steganography techniques for Arabic regarding capacity and security. The suggested pseudo-spaces stego technique has significant advantages and can be applied to other Arabic-related languages, such as Urdu and Persian, as well as providing new avenues for text-stego study in other languages around the globe. Gutub and Alaseri [20], developed new techniques for using Arabic text steganography to conceal sensitive data. The models are set up to aid in counting-based secret-sharing techniques that require individual memory of secret shares. The Kashida augmentation character, habitually used in Arabic composing text, is the underpinning of this concentrate on steganography models. The review puts our two recommended steganographic alterations of the original Arabic text to the test involving similar text data sets for the two changes. The results were intriguing and suggested future directions for research. Alkhudaydi and Gutub [21] assessed security practicability and considered difficult conditions and scenarios. It also performed simulations on a few brief passages from the Holy Quran, treating them as established, reliable, and standard authentic texts; this produced realistic study feedback that is worth paying attention to. Our revised method outperforms the previous diacritics stego method regarding favoured capacity and security, demonstrating intriguing prospective outcomes for engagingly illuminating future research. Alanazi *et al.* [22]

offered a creative method for using a seamless unicode standard to cover up hidden bits in Arabic. Their approach conceals sensitive information using Arabic characters in their contextual versions [22]. They add additional characters like zero-width joiners (ZWJ), Kashida, medium mathematical spaces (MMSPs), and zero-width non-joiners (ZWNJ) to build the strategy's ability without compromising the respectability of the information. Their strategy shows a more prominent security proportion than different routes. It is impervious to electronic text alterations such as duplicating, glueing, and text designing. Moreover, in light of their methodology utilizing unicode characters, the encoding standard utilized in most of the world's composing frameworks, it very well may be applied to related dialects like Urdu and Farsi.

Gutub and Alaseri [23] suggested that secret share models be concealed using improved Arabic steganography inside the texts the individual has personally selected. The Kashida augmentation character, which is excess in Arabic composing text, is the groundwork of the investigation of the ongoing steganography models. They worked on new models to conceal information utilizing counting-based secret-sharing innovation joined with Arabic text steganography. Their evaluations examined the different models utilizing similar benchmarks of 40 normal text explanations. The results are significant and offer promising examination progressions. Alanazi *et al.* [24] published a comparative analysis of text-hiding approaches in 2021, particularly on methods that alter the structural elements of digital text messages and files. They discussed a variety of core standards, uses, and text-hiding-related assaults, as well as the current security issues facing the cybersecurity sector. They also outlined each category's qualities and limits to demonstrate the effectiveness of the three main categories of text-hiding strategies in various situations. Khekan *et al.* [25] used Arabic language properties to embed secret English messages where more than half of the Arabic characters contain dots. Several characters have upper dots, and others have lower dots. Some have one dot others have two dots. Few have even three dots. They utilized the secret message using 5-digit encryption (T 5BE) to make the cover text ready to incorporate more pieces of the mystery message by 37.5%. They started using the Arabic semantic dictionary to correct the hiding path and enhancement the stego-cover text to eliminate errors caused by switching words. Their extracted experimental results show that the proposed model achieves high masking accuracy in addition to the storage capacity of the cover text.

2. METHOD

The Arabic alphabet is made up of 28 letters separated into two groups: 14 letters called lunar letters (حروف قمرية), and 14 letters called solar letters (حروف شمسية), which are named based on whether they are pronounced in the reciters after the letter (ال). The lunar letters (ابغ حجك وخف عقيمه) are pronounced clearly after the (ال), while the solar letters lose their distinctive sound and are pronounced double (given shadda) at the beginning of the word, as shown in Table 1. Hamza al-Wasl is a Hamza that is pronounced at the beginning of speech and in nouns, verbs, and letters. In the proposed work, the Hamza al-Wasl was added to the letters (ال) definition of a word if its 3rd letter is solar.

Table 1. Lunar and solar letters

Lunar letters	Solar letters
ء	ت
ب	ث
ج	د
ح	ذ
خ	ر
ع	ز
غ	س
ف	ش
ق	ص
ك	ض
م	ط
و	ظ
ي	ل
هـ	ن

2.1. Embedding algorithm

The proposed algorithm hides the binary form (0, 1) of the secret Arabic text in the form of Arabic diacritics (harakat) represented by Hamza_al Wasal ٱ(). The size of the Arabic cover text must be longer than the secret messages to ensure that it is possible to embed every bit of the secret text message inside the Arabic cover text. Before embedding the hidden message in the Arabic cover text, we reprocess the cover text by deleting every ٱ() found. After this, the secret bit will be hidden in words that start with (ال). The embedding will be started by detecting the words beginning with the (ال) definition, and then the secret bit will be tested.

If it is 1 and the 3rd letter after the (ال) definition is a solar character, the Hamza_Al Wasal ٓ() is added on (ال) and shadda (ّ) harakat is added to the solar letter. If the binary secret bit is 0 and the 3rd letter after the (ال) definition is a solar character, then there is no addition. The opposite of this procedure is applied to the lunar character, which means every word starts with (ال) definition, and its 3rd letter is a lunar character. If the binary bit of the secret message is 1, there is no addition, but if it is 0, then ٓ() will be added on (ال). The fatha, damma or kasra harakat is appended on the lunar letter if the fourth letter is the letter of the alef (ا), waw (و) or yaa (ي), respectively. A new cover text we use in the embedding process is obtained and sent to the intended recipient. After including all the letters of the secret message inside the cover text, a stego text file is received. The secret message will be hidden in the cover text without affecting the original size. Figure 1 represents the flow chart of the embedding process, while Algorithm 1 describes the embedding process. The secret message's length (the number of characters) is specified in a variable and stored in the cover letter before the secret message in the same proposed way.

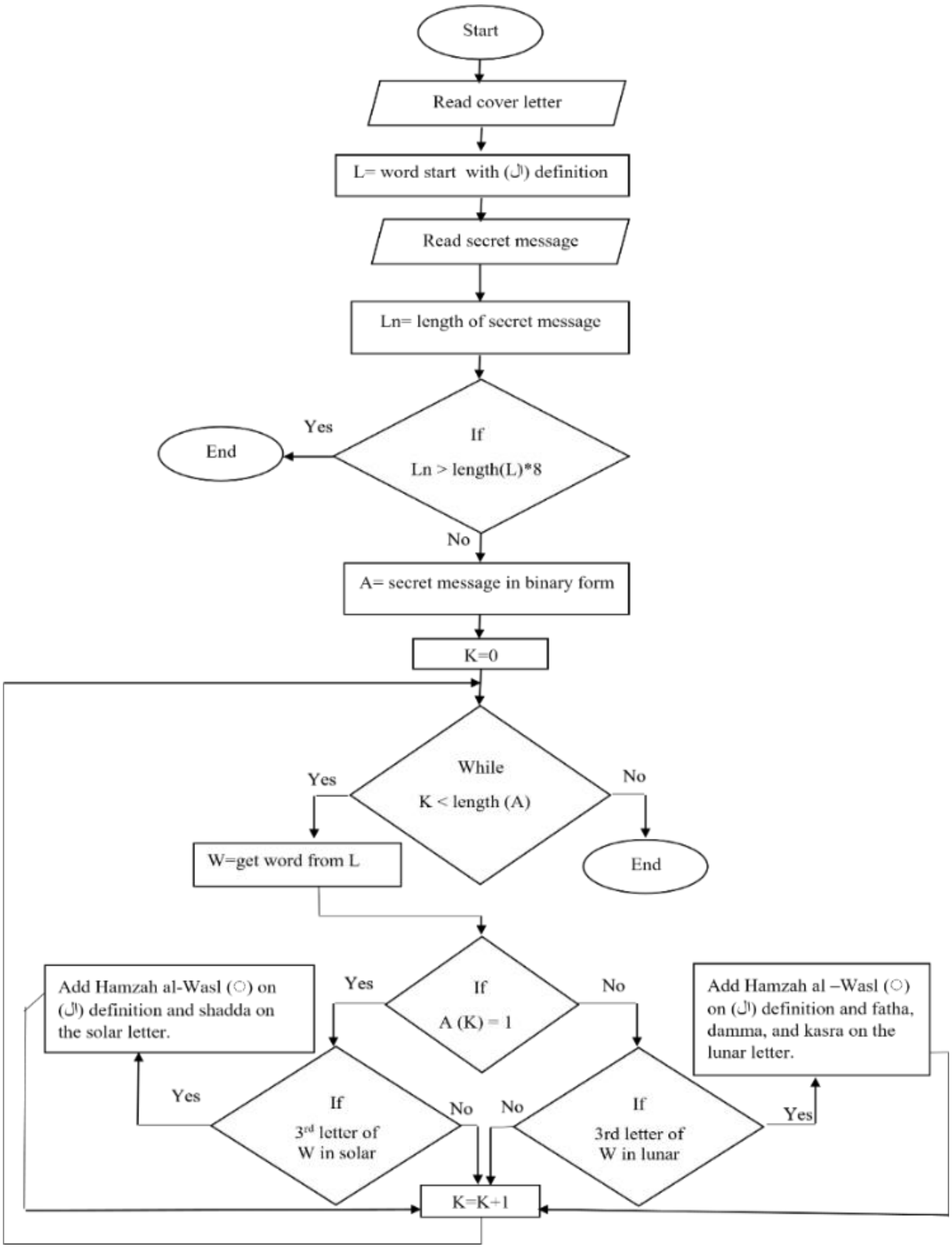

Start
Read cover letter
L= word start with (ال) definition
Read secret message
Ln= length of secret message
If
Ln > length(L)*8
Yes
End
No
A= secret message in binary form
K=0
While
K < length (A)
Yes
No
W=get word from L
End
If
A (K) = 1
Yes
No
Add Hamzah al-Wasl (○) on (ال) definition and shadda on the solar letter.
Add Hamzah al –Wasl (○) on (ال) definition and fatha, damma, and kasra on the lunar letter.
Yes
If
3rd letter of
W in solar
No
No
If
3rd letter of
W in lunar
Yes
K=K+1

Figure 1. The flow chart for the embedding process

Algorithm 1. Embedding algorithm

```
Input: Cover text, secret message
Output: Stego text
Step 1: Pre-processing the cover text
Step 2: Ln= number of words starting with (ال) letter.
Step 3: Read the secret message.
Step 4: If the length of secret message*8 > Ln, then exit.
Step 5: L = List of words that started with (ال) from the cover text.
Step 6: Assign the Length of secrete message (number of Chars) into a variable and
        put it in the header section as a binary number that consists
        of 8 bits
Step 7: Convert the secret message to binary form and save it in list L.
Step 8: Read one bit from the secret message.
Step 9: While not end of L
Step 10:
Step 10: If bit = 1 and the $3^{rd}$ letter of the word is solar then
                                 add Hamzah al -Wasl on (ال) and shadda
                                 diacritics on the solar letters
        Else
          If bit =0 and the $3^{rd}$ letter of the word is lunar Then
                      add Hamzah al -Wasl, and add fatha, damma, or kasra on the
                      lunar character if the fourth letter in the word is alef (أ),
                      Waw (و), or Yaa (ي),
                      respectively.
          Else keep the word unchanged.
        EndIf
Step 11: End while
Step 12: Return the Stego-text.
Step 13: End
```

2.2. Extracting algorithm

Extraction is the opposite of embedding. The following algorithm explains the primary concept of the stego text extraction mechanism. After reading the stego text, the words that begin with the letter (ال) were detected. If the third letter is solar and Hamzah al-Wasl is added to the (ال) definition, then the extracted binary bit is 1. If there are no diacritics in the word, the extracted binary bit is 0.

While if the third letter is lunar and Hamzah al-Wasl is added to the (ال) definition, then the removed double piece is 0. Assuming there are no diacritics in the word, the separated paired piece is 0. In this algorithm, the mystery message's length remembered for the cover is not entirely settled, and then, at that point, the twofold piece is gathered and changed over entirely to the UTF-8 mystery message. Algorithm 2 describes the extracting process, and Figure 2 (see in *Appendix*) represents the secret message's flow chart.

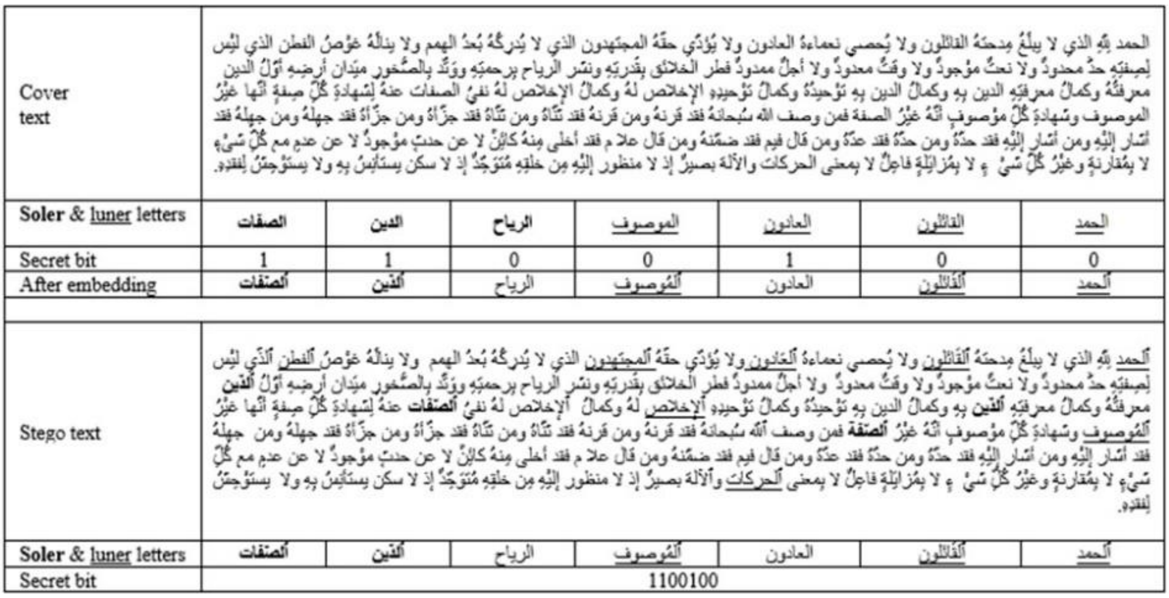
Algorithm 2. Extraction algorithm

```
Input: Stego text, length of the secret message (L)
Output: Secret message
Step 1: read words from the stego text.
Step 2: Create a List of words starting with (ال): counter =0: Smes=".
Step 3: While counter < L.
Step 4:     If the $3^{rd}$ letter is solar,
                     If Hamzah al -Wasl is found on the (ال) definition,
                     then the extracted bit = 1.
                     else bit =0
                 Else if the $3^{rd}$ letter is lunar,
                     If Hamzah al -Wasl is found on the (ال) definition,
                     then the extracted bit = 0.
                    Else bit=1.
Step 5:     Append the extracted bit to Smes: counter ++
Step 6: End while
Step 7: convert binary bit into UTF-8 as a secret message.
Step 8: Return the secret message
Step 9: End
```

3. RESULTS AND DISCUSSION

Increased embedding payload, extreme unawareness, security, and robustness are the fundamental aims of excellent steganography [26]. As a result, such criteria could be computed, whereas others are visualized. Approaches for text steganography to boost embedding potential. It's worth noting that stego text masking is influenced by embed ability. As a result, the text-hide technique's security is compromised, particularly when qualities like robustness and invisibility are required [19], [27].

Because of the small quantity of redundant data in the text compared to other audio, image, and video masking makes acquiring a high embedding ability rate in the text difficult [28], [29]. Furthermore, hiding parts of confidential data in a text document without causing a detectable shift in meaning is complicated. Text steganography methods can enhance embedding ability by increasing embeddable cover characters, compression methods, and merging multiple texts. For example, Figure 3 shows a practical example of embedding secret bits in a cover text. The proposed method extracts the words beginning with the (ال) definition and then determines the type of the 3rd letter (solar or lunar). According to the secret bit and the 3rd letter of the extracted word, the appropriate diacritics will be added. Then, it shows the extracting process of the secret bits from the stego text.



Cover text	الحمد لِلهِ الذي لا يبلغُ مِدحتهُ القائلون ولا يُحصي نعماءهُ العادون ولا يُؤدّي حقّهُ المجتهدون الذي لا يُدرِكُهُ بُعدُ الهمم ولا ينالهُ غوصُ الفطن الذي ليْس لِصِفتِهِ حدٌّ محدودٌ ولا نعتٌ موْجودٌ ولا وقتٌ معدودٌ ولا أجلٌ ممدودٌ فطر الخلائق بِقُدرتِهِ ونشر الرياح برحمتِهِ ووتّد بالصُّخور ميدان أرضِهِ أوّلُ الدين معرفتُهُ وكمالُ معرفتِهِ الدين بِهِ وكمالُ الدين بِهِ توْحيدُهُ وكمالُ توْحيدِهِ الإخلاص لهُ وكمالُ الإخلاص لهُ نفيُ الصفات عنهُ لِشهادةِ كُلِّ صِفةٍ أنّها غيْرُ الموصوف وشهادةِ كُلِّ موْصوفٍ أنّهُ غيْرُ الصفة فمن وصف الله سُبحانهُ فقد قرنهُ ومن قرنهُ فقد ثنّاهُ ومن ثنّاهُ فقد جزّأهُ ومن جزّأهُ فقد جهلهُ ومن جهلهُ فقد أشار إليْهِ ومن أشار إليْهِ فقد حدّهُ ومن حدّهُ فقد عدّهُ ومن قال فيم فقد ضمّنهُ ومن قال علا م فقد أخلى مِنهُ كائِنٌ لا عن حدثٍ موْجودٌ لا عن عدمٍ مع كُلِّ شيْءٍ لا بِمُقارنةٍ وغيْرُ كُلِّ شيْ ءٍ لا بِمُزايلةٍ فاعِلٌ لا بِمعنى الحركات والآلة بصيرٌ إذ لا منظور إليْهِ مِن خلقِهِ مُتوحِّدٌ إذ لا سكن يستأنِسُ بِهِ ولا يستوْحِشُ لِفقدِهِ.						
Soler & luner letters	**الصفات**	**الدين**	**الرياح**	الموصوف	العادون	القائلون	الحمد
Secret bit	1	1	0	0	1	0	0
After embedding	**ٱلصفات**	**ٱلدين**	الرياح	ٱلمُوصوف	العادون	ٱلقائلون	ٱلحمد
Stego text	ٱلحمد لِلهِ الذي لا يبلغُ مِدحتهُ ٱلقائلون ولا يُحصي نعماءهُ ٱلعادون ولا يُؤدّي حقّهُ ٱلمجتهدون الذي لا يُدرِكُهُ بُعدُ الهمم ولا ينالهُ غوصُ ٱلفطن ٱلذي ليْس لِصِفتِهِ حدٌّ محدودٌ ولا نعتٌ موْجودٌ ولا وقتٌ معدودٌ ولا أجلٌ ممدودٌ فطر الخلائق بِقُدرتِهِ ونشر الرياح برحمتِهِ ووتّد بالصُّخور ميدان أرضِهِ أوّلُ **ٱلدين** معرفتُهُ وكمالُ معرفتِهِ **ٱلدين** بِهِ وكمالُ الدين بِهِ توْحيدُهُ وكمالُ توْحيدِهِ ٱلإخلاص لهُ وكمالُ ٱلإخلاص لهُ نفيُ **ٱلصفات** عنهُ لِشهادةِ كُلِّ صِفةٍ أنّها غيْرُ ٱلمُوصوف وشهادةِ كُلِّ موْصوفٍ أنّهُ غيْرُ **ٱلصفة** فمن وصف ٱلله سُبحانهُ فقد قرنهُ ومن قرنهُ فقد ثنّاهُ ومن ثنّاهُ فقد جزّأهُ ومن جزّأهُ فقد جهلهُ ومن جهلهُ فقد أشار إليْهِ ومن أشار إليْهِ فقد حدّهُ ومن حدّهُ فقد عدّهُ ومن قال فيم فقد ضمّنهُ ومن قال علا م فقد أخلى مِنهُ كائِنٌ لا عن حدثٍ موْجودٌ لا عن عدمٍ مع كُلِّ شيْءٍ لا بِمُقارنةٍ وغيْرُ كُلِّ شيْ ءٍ لا بِمُزايلةٍ فاعِلٌ لا بِمعنى ٱلحركات وٱلآلة بصيرٌ إذ لا منظور إليْهِ مِن خلقِهِ مُتوحِّدٌ إذ لا سكن يستأنِسُ بِهِ ولا يستوْحِشُ لِفقدِهِ.						
Soler & luner letters	**ٱلصفات**	**ٱلدين**	الرياح	ٱلمُوصوف	العادون	ٱلقائلون	ٱلحمد
Secret bit	1100100						

Figure 3. The embedding and extracting process

The suggested approach should prevent the attacker from visualizing the hidden information, altering it, or extracting it via cracking (understanding) the embedding process. Invisibility and durability standards have an impact on the safety standard. Because of its invisibility, an eavesdropper cannot figure out what's going on in a stego script. Durability, on the other hand, prohibits the attacker from altering the hidden message. Table 2 shows a comparison in terms of capacity and security, as well as invisibility, between several algorithms used to hide inside an Arabic text.

Table 2. Comparison with other algorithms

Algorithm	Capacity	Security	Invisibility	Complexity	Running speed
Tayyeh [19]	Low	High	Medium	Medium	High
Shaker [18]	Low	Low	Low	Low	Medium
Malalla [30]	Low	High	Low	Medium	High
Ahmadoh [11]	Medium	High	Medium	High	Medium
Alanazi [31]	Medium	Medium	Low	High	Medium
Proposed method	Low	High	High	Low	Low

4. CONCLUSION

In this paper, we describe a new algorithm for hiding a secret message inside an Arabic text by adding Hamzat al-Wasl to the word, which starts with (ال) definition depending on its third letter (the Arabic lunar or solar letter). At first, the length of the secret message is hidden within the Arabic cover text before hiding the secret message itself. Experimental results related to the proposed algorithm indicate that the information is hidden with almost no change in the cover text, resulting in high transparency. The proposed algorithm is also robust against the attack because the secret message is hidden in the Arabic text with little change and the proposed algorithm does not change the size of the cover text. The breadth of the embedding depends on the number of words that start with the letter (ال) the more words that begin with (ال), the greater the embedding capacity. In future work, embedding capacity can be increased by using more features for Arabic embedding and combining high-security algorithms with the proposed method to improve security. It is used because it won't change the content of the writing. Due to its superior capacity performance, the proposed method beats out the other three methods. We can conclude that a steganography method's capacity performance depends on selecting the appropriate features to conceal secret text. The benefit of using the moon and sun letters concept is that it can increase the likelihood of hiding secret information in any letter. Maintaining the imperceptibility aspect while increasing capacity is crucial, though the imperceptibility of this method will be assessed in the future.

5. CONTRIBUTION TO THE STUDY

Although some researchers have considered Arabic characters, most have not applied their suggested techniques to social media. In the meantime, since social networks are constantly flooded with texts, these platforms provide fertile grounds for information concealment. Because there are so many texts, it is challenging for the eavesdropper to choose any that might include secret information specifically. Researchers can thus apply some of these techniques to support Arabic characters in social media. Adding text steganography techniques expands the potential and makes it more difficult for eavesdroppers to identify the embedding algorithm. These methods, however, carry over the drawbacks of the constituent methods. This is particularly clear in the Kashida approach, which lengthens the stego file while raising suspicion in particular situations. The integration should be thoroughly studied to determine which methods achieve the desired goals while minimizing the drawbacks of the constituent methods.

APPENDIX

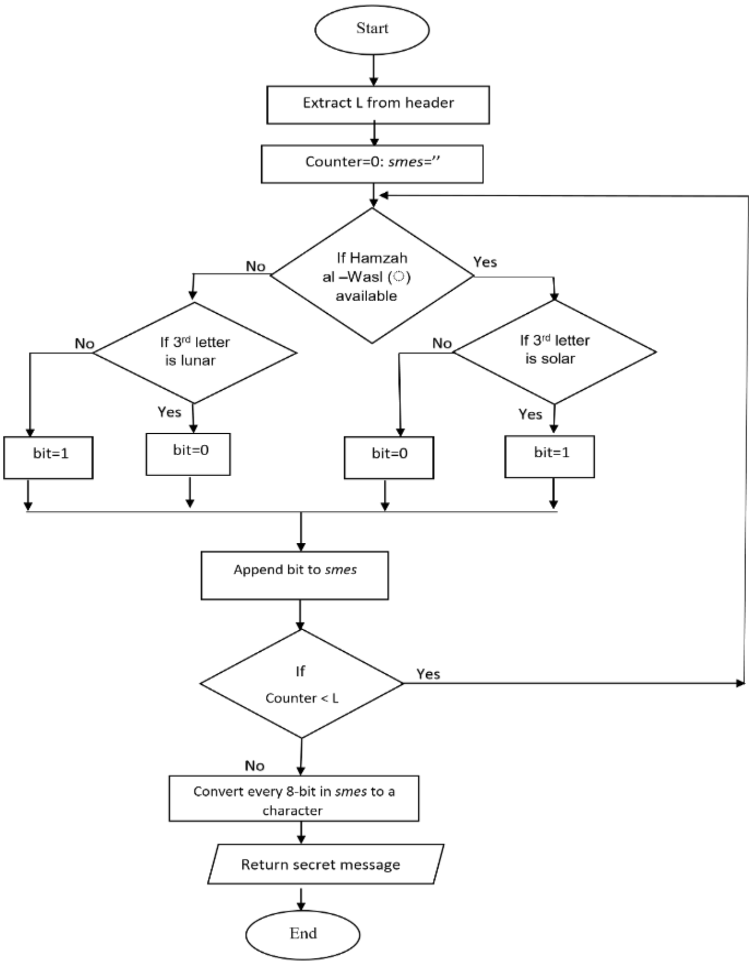


Figure 2. Flow chart for extracting process

REFERENCES

[1] Z. N. Sultani and B. N. Dhannoon, "Image and audio steganography based on indirect LSB," *Kuwait Journal of Science*, vol. 48, no. 4, 2021, doi: 10.48129/KJS.V48I4.8992.

[2] S. M. A. Al-Nofaie and A. A. A. Gutub, "Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications," *Multimedia Tools and Applications*, vol. 79, no. 1–2, pp. 19–67, 2020, doi: 10.1007/s11042-019-08025-x.

[3] A. H. Ibrahim and A. S. Alturki, "Computational analysis of arabic cursive steganography using complex edge detection techniques," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, pp. 496–500, 2020, doi: 10.14569/IJACSA.2020.0110959.

[4] M. B. Mahmood and B. N. Dhannoon, "Information hiding by using developed M8PAM technique," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 6, no. 8, 2017, doi: 10.17148/IJARCCE.2017.6802.

[5] R. Thabit, N. I. Udzir, S. M.Yasin, A. Asmawi, N. A. Roslan, and R. Din, "A comparative analysis of arabic text steganography," *Applied Sciences (Switzerland)*, vol. 11, no. 15, p. 6851, 2021, doi: 10.3390/app11156851.

[6] B. N. Dhannoon, "An indirect MSB data hiding technique," *Life Science Journal*, vol. 10, no. SPL.ISSUE11, pp. 263–266, 2013.

[7] S. Jusoh, A. Mustapha, A. Ismail, and R. Din, "A review of Arabic text steganography: Past and present," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 17, no. 2, pp. 1040–1046, 2020, doi: 10.11591/ijeecs.v17.i2.pp1040-1046.

[8] R. Din, S. Utama, and A. Mustapha, "Evaluation Review on Effectiveness and Security Performances of Text Steganography Technique," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 11, no. 2, pp. 747-754, 2018, doi: 10.11591/ijeecs.v11.i2.pp747-754.

[9] A. Majumder, S. Changder, and N. C. Debnath, "A new text steganography method based on sudoku puzzle generation," *Lecture Notes in Electrical Engineering*, vol. 605, pp. 961–972, 2020, doi: 10.1007/978-3-030-30577-2_85.

[10] R. H. Ali and J. M. Kadhim, "Text-based steganography using huffman compression and AES encryption algorithm," *Iraqi Journal of Science*, vol. 62, no. 11, pp. 4110–4120, 2021, doi: 10.24996/ijs.2021.62.11.31.

[11] E. M. Ahmadoh and A. A.-A. Gutub, "Utilization of two diacritics for Arabic text steganography to enhance performance," *Lecture Notes on Information Theory*, vol. 3, no. 1, 2015, doi: 10.18178/lnit.3.1.42-47.

[12] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in *2015 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2015*, 2015, doi: 10.1109/LISAT.2015.7160192.

[13] A. A. Gutub and M. M. Fattani, "A novel arabic text steganography method using letter points and extensions," in *Engineering and Technology*, 2007, pp. 28–31.

[14] S. M. Kadhem and D. Wameedh, "Proposed Arabic text steganography method based on new coding technique," *International Journal of Engineering Research and Applications*, vol. 6, no. 9, pp. 38–46, 2016.

[15] S. M. Al-Nofaie, M. M. Fattani, and A. A. Gutub, "Merging two steganography techniques adjusted to improve Arabic text data security," *Journal of Computer Science & Computational Mathematics*, pp. 59–65, 2016, doi: 10.20967/jcscm.2016.03.004.

[16] A. A. Obeidat, "Arabic text steganography using unicode of non-joined to right side letters," *Journal of Computer Science*, vol. 13, no. 6, pp. 184–191, 2017, doi: 10.3844/jcssp.2017.184.191.

[17] A. M. Alhusban and J. Q. O. Alnihoud, "A meliorated kashida based approach for Arabic text steganography," *International Journal of Computer Science and Information Technology*, vol. 9, no. 2, pp. 99–112, 2017, doi: 10.5121/ijcsit.2017.9209.

[18] A. A. Shaker, F. Ridzuan, and S. A. Pitchay, "Text steganography using extensions kashida based on the moon and sun letters concept," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 8, 2017, doi: 10.14569/ijacsa.2017.080838.

[19] H. K. Tayyeh, M. S. Mahdi, and A. S. A. AL-Jumaili, "Novel steganography scheme using Arabic text features in Holy Quran," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1910–1918, 2019, doi: 10.11591/ijece.v9i3.pp1910-1918.

[20] A. Gutub and K. Alaseri, "Hiding shares of counting-based secret sharing via Arabic text steganography for personal usage," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2433–2458, 2020, doi: 10.1007/s13369-019-04010-6.

[21] M. G. Alkhudaydi and A. A. Gutub, "Integrating light-weight cryptography with diacritics Arabic text steganography improved for practical security applications," *Journal of Information Security and Cybercrimes Research*, vol. 3, no. 1, pp. 13–30, 2020, doi: 10.26735/fmit1649.

[22] N. Alanazi, E. Khan, and A. Gutub, "Inclusion of unicode standard seamless characters to expand Arabic text steganography for secure individual uses," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 4, pp. 1343–1356, 2022, doi: 10.1016/j.jksuci.2020.04.011.

[23] A. A. A. Gutub and K. A. Alaseri, "Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 9, pp. 1108–1120, 2021, doi: 10.1016/j.jksuci.2019.06.014.

[24] N. Alanazi, E. Khan, and A. Gutub, "Efficient security and capacity techniques for Arabic text steganography via engaging unicode standard encoding," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 1403–1431, 2021, doi: 10.1007/s11042-020-09667-y.

[25] A. R. Khekan, H. M. W. Majeed, and O. F. A. Adeeb, "New text steganography method using the arabic letters dots," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, no. 3, pp. 1784–1793, 2021, doi: 10.11591/ijeecs.v21.i3.pp1784-1793.

[26] M. T. Ahvanooey, Q. Li, J. Hou, A. R. Rajput, and Y. Chen, "Modern text hiding, text steganalysis, and applications: A comparative analysis," *Entropy*, vol. 21, no. 4, p. 355, Apr. 2019, doi: 10.3390/e21040355.

[27] M. Aman, A. Khan, B. Ahmad, and S. Kouser, "A hybrid text steganography approach utilizing unicode space characters and zero-width character," *International Journal on Information Technologies & Security*, vol. 1, no. 1, p. 2017, 2017.

[28] M. Shirali-Shahreza and M. H. Shirali-Shahreza, "Text steganography in SMS," in *2007 International Conference on Convergence Information Technology, ICCIT 2007*, 2007, pp. 2260–2265, doi: 10.1109/ICCIT.2007.4420590.

[29] S. M. Kadhem, "Text Steganography Method Based On Modified Run Length Encoding," *Iraqi Journal of Science*, vol. 57, no. 3, pp. 2338–2347, 2016.

[30] A. S. Malalla and M. R. Shareef, "Improving hiding security of Arabic text steganography by hybrid AES cryptography and text steganography," *Journal of Engineering Research and Application*, vol. 6, no. 65, pp. 2248–962260, 2016.

[31] N. Alanazi, E. Khan, and A. Gutub, "Functionality-improved Arabic text steganography based on unicode features," *Arabian Journal for Science and Engineering*, vol. 45, no. 12, pp. 11037–11050, 2020, doi: 10.1007/s13369-020-04917-5.

BIOGRAPHIES OF AUTHORS

Rawaa Hamza Ali holds a B.Sc. degree. in computer science from the University of Babylon, Iraq, in 2003, and has an M.Sc. degree. in computer science from Al-Nahrain University, Baghdad, Iraq, in 2021. She worked as an assistant lecturer at the college of science, Missan University, Missan, Iraq. Her research interests include computer science in general and cryptography, data hiding and computer networks in particular. She can be contacted by email: rawaaha@uomisan.edu.iq.

Ban Nadeem Dhannoon received a B.Sc. in computer science from Baghdad University, an M.Sc. in computer science from Al-Nahrain University, and a Ph.D. in artificial intelligence from the University of technology. She held several administrative posts with the college of science/Al-Nahrain University since 2007, including the assistant dean of scientific affairs from (2007-2014), and the head of the computer science department (2016-2020). She is a professor at the department of computer science. She has supervised and co-supervised more than 40 masters and 5 Ph.D. students. She has authored or co-authored over 50 publications. Her research interests include machine and deep learning, Image processing, and natural language processing. She can be contacted by email: ban.n.dhannoon@nahrainuniv.edu.iq.

Mohammed Iedan Hamel is an engineer at Missan Oil Company (Iraq) and a master's student at the Islamic Azad University, artificial intelligence department (Iran). He has experience in many programming languages like python, C++, Java and JS, and database (SQL and NoSQL), data engineering and system administration. Mr. Hamel has introduced a lot of training courses in algorithms, programming, information security and other ICT fields. He is the cofounder of ICT taskforce initiation for training a student in ICT fields, and he got a lot of certifications like Microsoft certified trainer (MCT), Microsoft certified association solution (MCSA), Microsoft certified professional (MCP) and information technology infrastructure library (ITIL). He can be contacted by email: mohammedhamel@moc.oil.gov.iq.