USING SPECIAL LETTERS AND DIACRITICS IN STEGANOGRAPHY IN HOLY QURAN

Nooruldeen Subhi Shakir[1]

[1]*Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics*
ms202120666@iips.icci.edu.iq

Mohammed Salih Mahdi [2]

[2]*Business Information College, University of Information Technology and Communications, Baghdad, Iraq*
Email: mohammed.salih@uoitc.edu.iq

Abstract

Because of the great development that took place in information transfer and communication technologies, the issue of information transfer security has become a very sensitive and resonant issue, great importance must be given to protecting this confidential information. Steganography is one of the important and effective ways to protect the security of this information while it is being transmitted through the Internet, steganography is a technology to hide information inside an unnoticeable envelope object that can be an image, video, text or sound. The Arabic language has some special features that make it excellent covers to hide information from Through the diversity of the Arabic letters from dotted letters in several forms or vowels or special letters, the Holy Qur'an is considered a cover rich in movements and Arabic grammar, which makes it a wide cover for the purpose of concealing information. The Holy Qur'an is a sacred book where it is not permissible to modify, add or move any of the letters or any diacritical mark to it. The algorithm hides the two bits by uses six special letters of Arabic language. Moreover, it checks for the presence of specific Arabic linguistic features referred Arabic diacritics. The proposed system achieved a high ability to hide as in Surat Al-Baqarah (4524 bits) and also (2576 bits) in Surat Al-Imran and in Surat Al-An'am (2318 bits).

Index items: Steganography, Diacritics, Special letters, cover Text, Stego-text.

I. INTRODUCTION

Nowadays, everyone may quickly access information thanks to the advancement of computers and worldwide connection. Thus, the importance of information security has increased. Information security is a field with several sub-disciplines, and information concealing is one of them. The three mains Figure 1 Show three main technique.[1], [2].
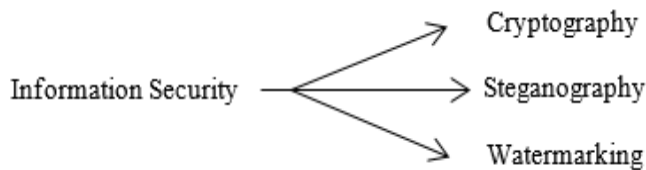

Figure 1 Information Security System

Steganography and the word "watermarking" go hand in hand. Information that is securely and silently included into the host data as a digital watermark cannot be deleted. A watermark often includes information about the source, condition, or destination of the host data in the formation [3], [4]. Steganography and watermarking vary in that the former is a technique for covert communication while the latter is a way to include watermark data. The method of sending data encoded such that only the recipient and sender are aware of a key is known as cryptography [5]–[7]. Without the data on the key, any further invader is unable to access or comprehend the data [8]. Steganography is the practice of sending confidential information that is concealed behind other data, therefore, the only types of data used in this procedure are confidential and cover data. Steganography is among the best methods for protecting information since it employs conceals data in a manner that deters intruders [9], [10]. A communication technique to lower the danger of an attack during transmission across communication medium is steganography. It is an area of study that deals with the covert transfer of information [11]. The past ten years have seen a rapid advancement in computer technology, which has renewed interest in the creation of computer steganography. Digital data now contains messages that are typically analog in nature, such as voice, audio, video, pictures, and text. Symbol text is used in text steganography to conceal sensitive information[12]. Text files may be stored with less memory use and with simpler communication than other steganographic techniques. Since texts have advantages, such as using less memory , transmitting more information, and requiring less printing [13]. Many steganographic methods have been proposed in the last decade, but most use a covering medium such as images[14], video clips [15], and sounds [16],and text[17]. text documents are currently the most common and necessary form of information and are always used as a means to cover. The most challenging type of steganography is text since it has a lower capacity compared to other cover object mediums[18].three-relation performance to procedure good steganography as follows:

Robustness: is the capability to prevent unseen data from being damaged, particularly when it is transferred via an unsafe network [19], [20]. **Security**: The level of security performance that prevents a third party with no connection to the sender and receiver from detecting the existence of a concealed message embedded in the text during the steganography process [19], [20]. **Capacity**: The amount of information in the covert message can be concealed by embedding it within the text. During text steganography, the capacity values could be classified by size bit, amount bit, and text length [19], [20].

II. RELATED WORK

Although being written in the traditional Arabic language and standing as the Holy Book for more than one-third of humanity, only a few text steganography methods are utilized on Arabic texts, with English texts being the most often used language for text steganography [21], The language of choice for more than 1.7 billion Muslims worldwide is Arabic. The land of the Arabs has 422 million local and native speakers. In terms of use, Arabic jumps to the fifth spot in the world. It has 28 distinct letters and is written right to left [22] . Arabic has a number of qualities that might be used to hide text. The most popular Arabic hiding techniques are diacritics, kashida, dotted letters, and the Unicode method [23]. This section will focus on some work on Arabic text steganography. the author in [24] in Arabic letters There is a letter marked as a special letter in Arabic. These special letters are 'ا' Alif, 'د' Dal, 'ذ' Thal, 'ر' Ray, 'ز' Zay, and 'و' Waw. they appear at the beginning or end of a word, these particular characters in Arabic language are private. When they appear in the middle of a word, these unusual letters cannot be related to the letter next to them. The author algorithm made use of these particular letters' efficacy. Their technique consists of two distinct situations since it is based on a combination of zero-width characters (ZWC) and zero-width joints (ZWJ) as follows:
• Inserts a ZWC combination if the letters are special letters.
• If letters are next to one another or stand-alone, an arrangement of ZWJ characters will be inserted   between the letters to conceal a pair of bits.
the author in [25] uses the same technique but with some enhancement. The method consists of three separate situations since it is based on the combinations of zero-width characters (ZWC), zero-width joints (ZWJ), and PS.
1. If the letters are unusual letters, the author adds the letters ZWC.
2. To conceal a pair of secret message bits, the author inserts a combination of ZWJ characters between letters that are joined to the following letter or that are isolated from one another.

3. When words are separated by spaces, the author inserts a PS character to conceal one bit of a hidden message. Pseudo-space (PS), on the other hand, is a character that does not display when printing it. [26]The plan is to enhance the merging approach by adding Kashida symbols in certain spots and leaving them out in others, with the goal of increasing security via ambiguity. This concept assumes Kashida locales will be used in half or less of its contents in an effort to enhance ambiguity. They proposed two adaptations, one use half of Kishida's places and the other utilizing two-thirds of those with intriguing characteristics. The half Kashida places, bi-location, assume that data is hidden in one Kashida site and not the other, i.e., one location is considered while the other is disregarded. Compared to a bilocation technique, a second upgrade using two sites, one left, aiming for a larger capacity with an appropriate degree of security will be examined.[27] The suggested approach relies on the general and contextual forms of Unicode, as well as the usage of ZWJ and Kashida extender characters. It also includes the inclusion of the ZWNJ character to increase capacity, as examined differently in study. ZWNJ inhibits the merging of Arabic letters without inserting a space between them; It is sometimes referred to as the pseudo-space and also is encoded in Unicode as U+200C. to include a hidden message The relevant letter inside the cover text gets converted from its normal Unicode format to its context form if the secret bit that is presently being processed is 1. The character doesn't change if indeed the secret is set to 0. We examine the connection between the current character and the subsequent character before processing the next secret bit. When the secret bit is set to 1, ZWNJ is put between the presently processed character and the unconnected next character; when it is set to 0, nothing is added.[28] They suggested a two-layer approach that takes use of both steganography and cryptography. They are used separately to provide the highest level of security possible, with independent, quantifiable security, capacity, and reliability measurements and improvement modifications. A very well common AES, DES, and IDEA encryption algorithms are used by the cryptography layer as generally chosen efficient algorithms, while the steganography layer makes use of the well-known Steganography will be used to conceal the diacritical marks (Fatha, Kasrah, Dammah, Fathatan, Damatan, Ksratan, Sukun, and Shadah). The secret message will first be encrypted, and then it will be inserted inside the cover text as a flow. Keep the "Diacritic Fatha" if the secret-bit is "1," but delete it if the secret is "0." and will add two "Sukun" diacritical marks to denote the conclusion of a hiding.[29]this algorithm works By selecting a word after another from the plain text and comparing it with the hidden bit, which is determined by the total of the word's litter dots; if the number of litter dots equals

an odd number, the word includes a secret bit with a value of (0). and if the word has an even number of litter dots, then indicates that the word has a hidden bit with the value of (1). If a word cannot be found that is near enough in meaning and has the same number of dots for its letters to equal the value of the bit to be concealed, it is neutralized. If no word can be located that is sufficiently close in meaning and has the same amount of dotted for its letter to match the value of the hidden bit, the word will be substituted with other terms that have a comparable significance but some letters dotted equivalent to the amount of the hidden bit.. The procedure is then repeated until all the last pieces of the secret text to be concealed are complete in order to find a word that does not include its letters. [21] The paper suggests two novel steganography techniques for Arabic text via the Quran as the cover text. The algorithms utilize the presence of sun characters and moon characters to conceal secret information within Arabic letters. In addition, minuscule vowel characters (Arabic Diacritics) are used to indicate the existence of certain Arabic language characteristics. Experiments utilizing the two proposed algorithms indicate that text files have a high capacity. Due to the imperceptibility of alterations to the cover text, the suggested algorithms are resistant to assault; therefore, our contribution provides a more secured algorithm with a high capacity. the first algorithm uses Arabic grammar, sun letters, and moon letters if the word starts with (ال) and flowed by sun letter then will hide one bit (1), if the word starts with (ال) and flowed by moon letter then will hide one bit (o). the second algorithm uses Arabic grammar and Arabic Diacritics; it hides two bits in each word that start with (ال) and flows by a sun or moon letter. If flowed by a sun letter and the first diacritic after (ال) is (Fatha), it will hide two bits (11), and if the first diacritic after (ال) except (fatha), it will hide two bits (10). if the word starts with (ال) and flowed by a moon letter and the first diacritic after (ال) is (Fatha), it will hide two bits (00), and if the first diacritic after (ال) except (fatha), it will hide two bits (01) .

III. PROPOSED SYSTEM

There are 28 letters in the Arabic alphabet, plus three unique characters (ا–و–ذ–د–ر–ز), whose forms change depending on wherever they display in a word. The start, finish, middle, and isolated are the four locations for Arabic characters.[30] As Shown in Table 1.

Table 1 Example of Arabic Letter Shapes Depending on Their Position and The Six Special Letters.

Original	contextual forms				Letter
	Isolate	End	Middle	Beginning	
0627 ا	65165 ا	65166 ـا	65166 ـا	65165 ا	Alef
0648 و	65261 و	65262 ـو	65262 ـو	65261 و	Waaw
1583 د	65193 د	65194 ـد	65194 ـد	65193 د	Dal
1584 ذ	65195 ذ	65196 ـذ	65196 ـذ	65195 ذ	Thal
1585 ر	65197 ر	65198 ـر	65198 ـر	65197 ر	Raa
1586 ز	65199 ز	65200 ـز	65200 ـز	65199 ز	Zae

Different diacritical marks, which are regarded as optional extra (additional) symbols in the text. Except for the preservation of Holy Quran calligraphy and Islamic religious literature, it is not frequently employed nowadays [25] , As Shown in Table 2.

Table 2 Eight Main Diacritics in The Arabic Language

Fatha	◌َ	Kasrah	◌ِ
Dhammah	◌ُ	Sukkon	◌ْ
Shaddah	◌ّ	Tanween Fath	◌ً
Tanween Kasr	◌ٍ	Tanween Dham	◌ٌ

The universal character encoding system known as Unicode supports non-ASCII characters. Unicode, which makes use of 16 bits, supports all character sets used by the world's spoken languages. Because some languages—like Arabic and Chinese—need more location bits than others, this is crucial. Kurdish, Pashto, Sindhi, Urdu, , Sindhi, and Persian characters are also present in the Unicode table for languages like Arabic. In this study's suggested algorithms, hidden binary information in Arabic language is hidden using the grammar rule [26]. In each word with any Special Arabic character (ذ – ر – ا – و – د – ز) and flowed by letter (ب, ت, ص, ج, ش, خ, س, ح, ث, ض, ط, ه, ع,) ن, ف, ق, ل, ك, م, غ, ظ, ئ, وؤ) flowed by diacritic according to the roles that we made to hide the secret message, the Arabic language as specified in article together with the Arabic (Harakat) hide a peer of bits.

IV. CONCEALMENT PROCESS

This algorithm conceals two bits in every one word containing an Arabic vowel letter (ا – و – د – ذ – ر – ز) surrounded by diacritics. Figure 2 and the Algorithm1 (Special Hiding Algorithm) illustrate the concealment procedure.

Algorithm1: Special Hiding Algorithm

Input: s.t cover-text (sura), e.s.m (encrypted secret message)
Output: stego-text

Start
Step 1: Let **l.w** = []   // l.w "List of Word"
Step 2: split **s.t** to **l.w**
Step 3: set an **s** to the first word in the l.w
Step 4: While not end of **e.s.m**
     read p two bits from e.s.m
     read one word from **l.w**
  If p = (**11**) and **s** has any special letter and flowed by letter
     (ب, ت, ث, ج, ح, خ, س, ش, ص, ض, ط) and this letter
     flowed by diacritic (Fatha or shadda)
    change the Unicode of the letter
    increase **p** by 2 and increase **s** by 1
  Else increase **s** by 1
  If p = (**10**) and **s** has any special letter and flowed by letter
     (ب, ت, ث, ج, ح, خ, س, ش, ص, ض, ط) and this letter
     flowed by any diacritic except (Fatha or shadda)
    change the Unicode of the letter
    increase **p** by 2 and increase **s** by 1
  Else increase **s** by 1
  If p = (**00**) and **s** has any special letter and flowed by letter
     (ظ, ؤ , غ, ئ, ق, ل, ك, م, ن, ه, ف, ع) and this letter
     flowed by diacritic (Fatha or shadda)
    change the Unicode of the letter
    increase **p** by 2 and increase **s** by 1
  Else increase **s** by 1
  If p = (**01**) and **s** has any special letter and flowed by letter
     (ظ, ئ, ن, ف, ق, ل, ك, م, غ, ه, ع, ؤ) and this letter
     flowed by any diacritic except (Fatha or shadda)
    change the Unicode of the letter
    increase **p** by 2 and increase **s** by 1
  Else increase **s** by 1
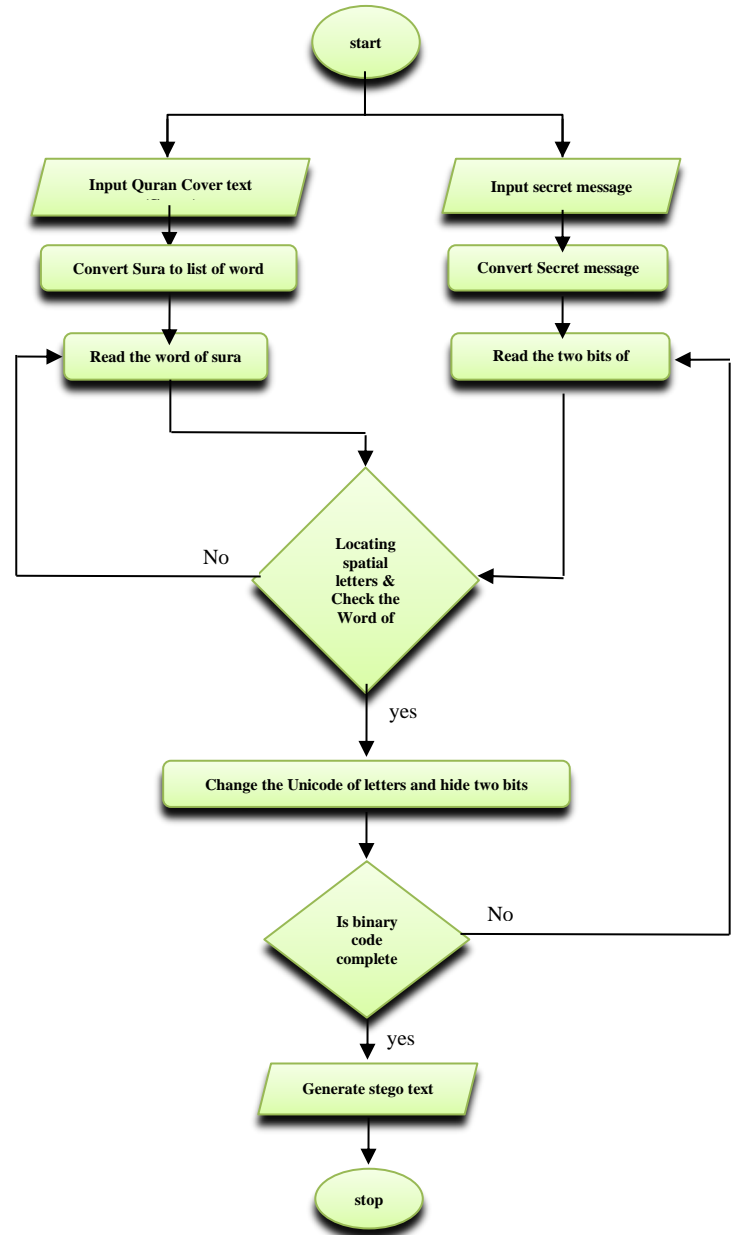 End While Loop
Step 5: generate the stego-text
End

Figure 2 Flowchart for Algorithm Special 1

V. EXTRACTION PROCESS

After the concealing algorithm is complete and a stego text has been sent to the recipient, there is a second algorithm that extracts the hide bits. The Extraction procedure is illustrated by Algorithm2 (Special Extraction Algorithm), and Figure 3.

| Algorithm 2: Special Extraction Algorithm |
|---|
| Input: s.t stego-text
Output: Secret message |
| **Start**
Step 1: set a pointer to the first word in the stego text
Step 2: While not the end of the stego text do the flowing
Step 2.1: read one word from stego text that has letter its
      Unicode was changed
Step 2.2: **If** the letter (ب, ت, ث, ج, ح, خ, س, ش, ص, ض, ط) found flowed
      by diacritic "Fatha "or diacritic "shadda " then we have
      two bits of the secret message of "11"
      Else the letter (ب, ت, ث, ج, ح, خ, س, ش, ص, ض, ط) flowed by
        any diacritic except "Fatha " or diacritic " shadda "
        then we have two bits of the secret message of "10"
      If the letter (ظ, ع, غ, ف, ق, ل, ك, م, ن, ه, ئ, ؤ) flowed by
        diacritic "Fatha " then we have two bits of the secret
        message of "00"
      Else if the letter (ظ, ع, غ, ف, ق, ل, ك, م, ن, ه, ئ, ؤ) flowed by
        any diacritic except "Fatha " then we have two bits
        of the secret message of "01"
End while loop
Step 3: convert binary secret message to the secret text
End |
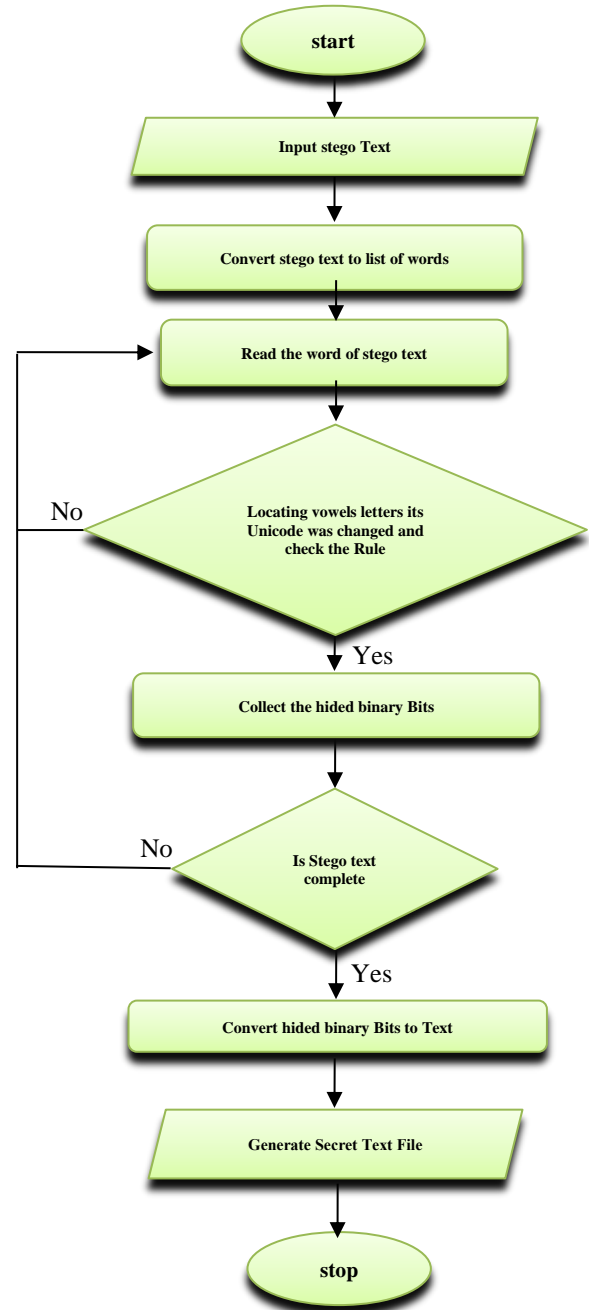
Figure 3 Flowchart for Algorithm Special 1

VI. RESULTS AND ANALYSIS

The results of the experiment are discussed in this section. The algorithms proposed utilize the Holy Quran surah to be a cover for hiding the secret message within Arabic texts. Surahs of the Holy Quran contain mandatory diacritics, which increase the file size of the cover page. This algorithm utilizes Sura Al-Fatiha cover media. As Shown in Figure 4 .

قُلْ أَعُوذُ بِرَبِّ الْفَلَقِ ﴿١﴾ مِنْ شَرِّ مَا خَلَقَ ﴿٢﴾ وَمِنْ شَرِّ غَاسِقٍ إِذَا وَقَبَ ﴿٣﴾ وَمِنْ شَرِّ النَّفَّاثَاتِ فِي الْعُقَدِ ﴿٤﴾ وَمِنْ شَرِّ حَاسِدٍ إِذَا حَسَدَ ﴿٥﴾
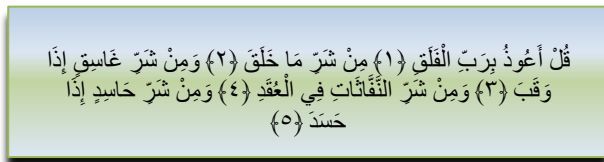
Figure 4 The Used Cover (Sura Al-Falaq)

Based on the proposed Algorithm's concealing technique, it looks for a word that has a letter (ا - و - د - ذ - ر - ز) ,flowed by any of the letters (ب, ت, ث, ج, ح, خ, س, ش, ص, ض, ط) Flowed by diacritic " Fatha " or diacritic " shadda " it hide two bits of "11" and if flowed by all diacritic except " Fatha " or diacritic " shadda " it hide two bits of "10" , if the word contains the letter (ا - و - د - ذ - ر - ز) and is followed by any letter (ظ, ع, غ, ئ) ,ف, ق) which is followed by the diacritic "Fatha," and it hide two bits of "00" , if followed by any diacritic other than "Fatha." it hide two bits of "01" ,**(Remember that these unique letters appear in various locations throughout the term.)**, Table 4 will Procedure for concealing the secret message '1101011000000110' in Surat Al-Falaq.

Table 4. Concealing Secret Message '1101011000000110' By Modifying the Unicode of Letters to Conceal 2 Bits

Stego cover	قُلْ أَعُوذُ بِرَبِّ الْفَلَقِ ﴿١﴾ مِنْ شَرِّ مَا خَلَقَ ﴿٢﴾ وَمِنْ شَرِّ غَاسِقٍ إِذَا وَقَبَ ﴿٣﴾ وَمِنْ شَرِّ النَّفَّاثَاتِ فِي الْعُقَدِ ﴿٤﴾ وَمِنْ شَرِّ حَاسِدٍ إِذَا حَسَدَ ﴿٥﴾									
Special letters	شَرِّ	وَمِنْ	خَلَقَ	مَا	شَرِّ	مِنْ	الْفَلَقِ	بِرَبِّ	أَعُوذُ	قُلْ
Word changed	☐	■	☐	☐	☐	☐	■	■	☐	☐
bits		01					01	11		
Special letters	شَرِّ	وَمِنْ	الْعُق	فِي	النَّفَّاثَاتِ	شَرِّ	وَمِنْ	وَقَبَ	إِذَا	غَاسِقٍ
Word changed	☐	■	☐	☐	■	☐	☐	■	☐	■
bits		01			00			00		10
Special letters								حَسَدَ	إِذَا	حَاسِدٍ
Word changed								☐	☐	■
bits										10
Stego Text	قُلْ أَعُوذُ بِرَبِّ الْفَلَقِ ﴿١﴾ مِنْ شَرِّ مَا خَلَقَ ﴿٢﴾ وَمِنْ شَرِّ غَاسِقٍ إِذَا وَقَبَ ﴿٣﴾ وَمِنْ شَرِّ النَّفَّاثَاتِ فِي الْعُقَدِ ﴿٤﴾ وَمِنْ شَرِّ حَاسِدٍ إِذَا حَسَدَ ﴿٥﴾									

To reveal the concealed message (secret bits) from stego text as in the previous example, The extraction Algorithm will read the stego text word by word and check if the Unicode of Arabic letters After the Special Letters are changed and by which diacritic its flowed To know which 2 bits it's hiding. As Shown in Table 5.

Table 5. Extracting A Hidden Bits in Stego Text, For the Unicode of The Letters Been Changed in The Word

Stego cover	قُلْ أَعُوذُ بِرَبِّ الْفَلَقِ ﴿١﴾ مِنْ شَرِّ مَا خَلَقَ ﴿٢﴾ وَمِنْ شَرِّ غَاسِقٍ إِذَا وَقَبَ ﴿٣﴾ وَمِنْ شَرِّ النَّفَّاثَاتِ فِي الْعُقَدِ ﴿٤﴾ وَمِنْ شَرِّ حَاسِدٍ إِذَا حَسَدَ ﴿٥﴾									
Special letters	شَرِّ	وَمِنْ	خَلَقَ	مَا	شَرَ	مِنْ	الْفَلَقِ	بِرَبِّ	أَعُوذُ	قُلْ
Word changed	☐	■	☐	☐	☐	☐	■	■	☐	☐
bits		01					01	11		
Special letters	شَرِّ	وَمِنْ	الْعُق	فِي	النَّفَّاثَاتِ	شَرَ	وَمِنْ	وَقَبَ	إِذَا	غَاسِقٍ
Word changed	☐	■	☐	☐	■	☐	☐	■	☐	■
bits		01			00			00		10
Special letters								حَسَدَ	إِذَا	حَاسِدٍ
Word changed								☐	☐	■
bits										10
Stego Text	1101011000000110									

Data concealment in text is one of the most challenging steganographic techniques since the text can change format and size while concealing data. As the holy Qur'an is a sacrosanct book, it is impossible to add a letter or alter the shape of the Arabic letters within it. Therefore, steganographic techniques such as , shifting points, Kashida, and others cannot be applied to the Arabic texts employed in the Holy Qur'an. Despite this, the Holy Qur'an is replete with diacritics and Arabic grammar, as well as a variety of Arabic letters, which gives it a broad scope. The technique proposed to conceal information in this study is a hybrid method utilizing the Unicode approach and the Arabic grammar with the benefits of diacritics on words containing special characters. The following equation1 determines the algorithm's capacity when utilized with the cover.

$$\text{Capacity ratio} = \frac{\text{number of hidden bits}}{\text{size of the cover in bytes}} \quad \ldots\ldots\ldots \text{ Equation 1}$$

The Flowing Table 6 will show the embedded ratio

Table 6 Computed Embed Ratios

cover name	Cover-size kB	Capacity of Algorithm (bit)	Ratio (b/kB)
AlFatihah	0.5	34	68
AlBaqarah	98.8	4524	41.4
Al'Imran	56.4	2576	42.5
Al-Falaq	0.3	18	60
AlMa'ida	45.7	2136	43.1
AlAn'am	48.5	2318	44.3
Yusuf	28.2	1270	42.1
Alroum	13.1	714	48
Al'Ankabot	16.1	840	46.4
Al-Dukhan	5.5	276	46.5

Total Average Capacity = 44.53

VII. CONCLUSION

By combining Arabic grammar and diacritics with the Unicode methodology and distinguishing the use of steganography based on using the special characters (ا – و – د – ذ – ر – ز) that's found in Arabic characters in Quran (Surah), a novel, and previously unexplored strategy was employed in this study to improve the ability to embed and increase the impressionability. the algorithm using diacritics does not alter them in terms of their (location, deletion, or addition) diacritical on the word with using a Unicode approach to modify the letters that will be a sign that this word is used for hiding. In the word used for concealing, it is resistant to traditional attacks and text duplication. After several uses of the proposed system on several surahs of the Holy Qur'an, it was found that the surahs with medium and many verses are more suitable for using this method, such as Surat Al-Baqarah, Al'Imran, AlAn'am, Yusuf, etc.

REFERENCES

[1] S. Shakir Baawi, M. Rosmadi Mokhtar, and R. Sulaiman, "A comparative study on the advancement of text steganography techniques in digital media," *Article in Journal of Engineering and Applied Sciences*, vol. 12, no. 1, 2018, [Online]. Available: https://www.researchgate.net/publication/323933346

[2] N. R. Zaynalov, O. N. Mavlonov, A. N. Muhamadiev, Q. Dusmurod, and I. R. Rahmatullaev, "UNICODE for Hiding Information in A Text Document," in *14th IEEE International Conference on Application of Information and Communication Technologies, AICT 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/AICT50176.2020.9368819.

[3] R. Abdulaali Azeez, M. K. Abdul-Hussein, M. Salih Mahdi, and H. T. S. Alrikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Original Research*, vol. 10, no. 1, pp. 178–187, 2022.

[4] W. Alomoush *et al.*, "Digital image watermarking using discrete cosine transformation based linear modulation," *Journal of Cloud Computing*, vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00468-w.

[5] M. S. Mahdi, N. F. Hassan, and G. H. Abdul-Majeed, "An improved chacha algorithm for securing data on IoT devices," *SN Appl Sci*, vol. 3, no. 4, Apr. 2021, doi: 10.1007/s42452-021-04425-7.

[6] R. A. Azeez, A. S. Jamil, and M. S. Mahdi, "A Partial Face Encryption in Real World Experiences Based on Features Extraction from Edge Detection," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 7, pp. 69–81, 2023, doi: 10.3991/ijim.v17i07.38753.

[7] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, vol. 47. Elsevier Ireland Ltd, Feb. 01, 2023. doi: 10.1016/j.cosrev.2022.100530.

[8] Wasit University. College of Engineering and Institute of Electrical and Electronics Engineers, *International Conference on Advances in Sustainable Engineering and Applications : 14-15 March 2018, Wasit, Iraq : ICASEA 2018 conference proceedings*.

[9] A. Alshamsi, S. Albaloushi, M. Alkhoori, H. Almheiri, and N. Ababneh, "Enhancing Arabic Text Steganography Based on Unicode Features," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 685–693, 2022, doi: 10.12785/ijcds/110155.

[10] M. Salih Mahdi and N. Flaih Hassan, "A SUGGESTED SUPER SALSA STREAM CIPHER," *Iraqi Journal for Computers and Informatics*, vol. 44, no. 2, Dec. 2018, doi: 10.25195/2017/4422.

[11] M. Salih Mahdi, R. Abdulaali Azeez, and N. Falih Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," vol. 8, no. 4, pp. 2138–2145, 2020.

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

[13] D. Lavanya *et al.*, "Quantum Text Steganography By Using BB84 Protocol."

[14] 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.

[15] M. Fuad and F. Ernawan, "Video steganography based on DCT psychovisual and object motion," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1015–1023, Jun. 2020, doi: 10.11591/eei.v9i3.1859.

[16] E. Abdullah, "AUDIO STEGANOGRAPHY METHOD USING LEAST SIGNIFICANT BIT (LSB) ENCODING TECHNIQUE," *J Theor Appl Inf Technol*, vol. 30, no. 12, 2022, [Online]. Available: www.jatit.org

[17] B. Osman, N. I. Yahya, K. Mohd Zaini, and A. Abdullah, "TEXT STEGANOGRAPHY USING THE SECOND QUOTIENT REMAINDER THEOREM AND DARK COLOUR SCHEMES," *Journal of Computational Innovation and Analytics (JCIA)*, vol. 2, no. 1, pp. 21–40, Jan. 2023, doi: 10.32890/jcia2023.2.1.2.

[18] A. Alshamsi, S. Albaloushi, M. Alkhoori, H. Almheiri, and N. Ababneh, "Enhancing Arabic Text Steganography Based on Unicode Features," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 685–693, 2022, doi: 10.12785/ijcds/110155.

[19] M. A. Ali Khodher and T. W. Aldeen Khairi, "Review: A comparison Steganography between Texts and Images," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Aug. 2020. doi: 10.1088/1742-6596/1591/1/012024.

[20] S. S. Alqahtany, A. B. Alkhodre, A. Al Abdulwahid, and M. Alohaly, "A Dynamic Multi-Layer Steganography Approach Based on Arabic Letters' Diacritics and Image Layers," *Applied Sciences*, vol. 13, no. 12, p. 7294, Jun. 2023, doi: 10.3390/app13127294.

[21] 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, Jun. 2019, doi: 10.11591/ijece.v9i3.pp1910-1918.

[22] A. Taha, A. S. Hammad, and M. M. Selim, "A high capacity algorithm for information hiding in Arabic text," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 6, pp. 658–665, Jul. 2020, doi: 10.1016/j.jksuci.2018.07.007.

[23] A. I. Alaqeel and M. S. Saleh, "Developing a Performance-based Tool for Arabic Text Steganography," in *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021. doi: 10.1109/NCCC49330.2021.9428837.

[24] A. Ditta, C. Yongquan, M. Azeem, K. Gulzar Rana, H. Yu, and M. Qasim Memon, "Information hiding: Arabic text steganography by using Unicode characters to hide secret data A. Ditta et al," 2018.

[25] A. S. Al-Dini, N. M. Al-Aidroos, and K. Q. Sha'afal, "Data Hiding Enhancement in Arabic Text," 2021. [Online]. Available: http://wwwijeair.com

[26] A. Gutub and K. Alaseri, "Hiding Shares of Counting-Based Secret Sharing via Arabic Text Steganography for Personal Usage," *Arab J Sci Eng*, vol. 45, no. 4, pp. 2433–2458, Apr. 2020, doi: 10.1007/s13369-019-04010-6.

[27] 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, Dec. 2020, doi: 10.1007/s13369-020-04917-5.

[28] M. Alkhudaydi and A. Gutub, "Securing Data via Cryptography and Arabic Text Steganography," *SN Comput Sci*, vol. 2, no. 1, Feb. 2021, doi: 10.1007/s42979-020-00438-y.

[29] A. Boulesnane, A. Beggag, and M. Zedadik, "A New Steganography Technique Based on Dotted Arabic Letters Features," in *5th International Conference on Networking and Advanced Systems, ICNAS 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICNAS53565.2021.9628914.

[30] 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, Dec. 2020, doi: 10.1007/s13369-020-04917-5.