ISSN: 0067-2904

Improving Security of the Crypto-Stego Approach using Time Sequence Dictionary and Spacing Modification Techniques

Eman S. Harba [1*], Hind S. Harba[2], Inas Ali Abdulmunem[3], Samera Shams Hussein[4]
[1] Avicenna Unit for E-Learning, College of Arts, University of Baghdad, Baghdad, Iraq
[2] Department of Atmospheric Sciences, College of Science, University of Mustansiriyah, Baghdad, Iraq
[3] Department of Computer science, College of Science University of Baghdad, Baghdad, Iraq
[4]Department of Computer Science, College of Education for pure Science, University of Baghdad, Baghdad, Iraq

Received: 30/6/2020 Accepted: 28/11/2020

Abstract

Cryptography steganography is a practical tool for data security. Hybridization of the cryptography with steganography can provide more security by taking advantage of each technique. This work proposes a method for improving the crypto-stego method by utilizing the proposed dictionary method to modified ciphertext. After that, the modified encrypt ciphertext id was hidden in the text by using the proposed method. For cryptography, an Advanced Encryption Standard (AES) was utilized to encrypt the message. The AES employed a 128bit block size and 256bit key size. The ciphertext characters were then replaced by the characters identified by a dictionary list. The dictionary is time-dependent, where each of the equivalent words shift based on the time-shift equation. The modified ciphertext was then embedded into a cover text so that the attacker cannot separate them by applying cryptanalysis. The "Modifying Spain" method used the "Space" to build a steganography tool that hides the secret message.

The simulation results show that the proposed method achieved a high-security level when the cryptography and steganography are combined in such a way that the ciphertext is changed to another value by using a dictionary with a time sequence that makes the cryptanalysis test fails to guess and identify the algorithm that has been used for encryption. The stego test shows that the proposed method achieved good results in terms of capacity and visibility, being proved to be hard to notice. The tests also prove that the proposed method runs fast with less computational requirements.

Keywords: AES, Cryptography, Steganography, Text Stego., Time Sequence.

تحسين مستوى الحماية لتقنية التشفير والإخفاء باستخدام طريقة القاموس والتسلسل الزمني للتشفير والتباعد المعدل لتقنية إخفاء المعلومات

إيمان سليم إبراهيم حربه، هند سليم إبراهيم حربه[2]، إيناس علي عبد المنعم[3] ,سميرة شمس حسين[4]

[1]وحدة ابن سينا للتعليم الالكتروني، كلية الاداب، جامعة بغداد، بغداد، العراق

[2]قسم علم الجو، كلية العلوم، الجامعة المستنصرية، بغداد، العراق

[3]قسم علوم الحاسوب، كلية العلوم، جامعة بغداد

[4]قسم علوم الحاسبات، كلية التربية للعلوم الصرفة، جامعة بغداد

*Email: inas.ali@uobaghdad.edu.iq

الخلاصة

تعد تقنية تشفير المعلومات (Cryptography) وتقنية إخفاء المعلومات (Steganography) من الأدوات المهمة لأمن البيانات. يمكن أن يوفر التشفير الهجين الناتج من دمج تقنيتي تشفير المعلومات مع إخفاء المعلومات مزيدًا من الأمان من خلال الاستفادة من ميزات كل تقنية. هذا العمل يقترح طريقة لتحسين طريقة التشفير الهجين (crypto–stego) من خلال استخدام طريقة القاموس المقترحة لتعديل النص المشفر ومن ثم إخفاء شفرة النص المعدل في رسالة نصية باستخدام طريقة التباعد المعدلة. بالنسبة للتشفير، استخدمنا معيار تشفير متقدم (AES) لتشفير الرسالة السرية، حيث تم استخدام خوارزمية AES ذات حجم كتله Block) (Sizeمقداره 128 بت وحجم مفتاح (Key Size) مقداره 256 بت، ومن ثم تم استبدال النص المشفر بقيمة جديدة بواسطة طريقة القاموس لاختيار مرادفات للرموز. يعتمد هذا القاموس على الوقت، حيث ستتحول كل رمز من الرموز الى أخرى مكافئة بالاستناد إلى معادلة الوقت. بعد ذلك يتم تضمين النص المشفر المعدل في رسالة نصية حاملة حتى لا يتمكن المهاجم من فصله بواسطة تطبيق تحليل الشفرة. تستخدم طريقة " التباعد المعدلة" لإنشاء أداة إخفاء المعلومات التي تستخدم "الفراغات" لإخفاء الرسالة السرية.

أظهرت النتائج التجريبية أن الطريقة المقترحة قد حققت مستوى عالي من الأمان عند الجمع بين التشفير وعلم إخفاء المعلومات بحيث يتم تغيير نص التشفير إلى قيمة أخرى عن طريق القاموس المستخدم مع تسلسل زمني يجعل اختبار تحليل التشفير يفشل في تخمين وتحديد الخوارزمية التي تم أستخدمها للتشفير. يوضح اختبار كفاءة الأخفاء أن الطريقة المقترحة حققت نتائج جيدة من حيث السعة والوضوح والتي اثبتت انها من الصعب اكتشافها. واوضحت الاختبارات أيضًا أن الطريقة المقترحة تعمل بسرعة مع متطلبات حسابية قليلة

Introduction

Secure data communication is the most crucial concern in the present day. Data security has already been employed in many fields, such as education, e-commerce, and industry. Sending and receiving data securely is significant as the data is critical. Maintain the security is a hard task as the inherent data characteristics are usually numerous [1].

Cryptography is an approach associated with aspects of data security, including data integrity and confidentiality as well as origin authentication and entity authentication. Steganography is the art of hiding data. It differs from cryptography, which is used to secure data by transforming it into an alternative, unreadable format. At the same time, steganography tends to make data invisible via concealing (embedding) them within other data known as the cover (carrier). The cover message (which can be text, image, audio, or video) may be stored or transferred as a message. The secret data can be inserted into numerous cover types. In cases where the secret data is concealed in a text file, it is called stego-text. While if it is concealed in a video file, it is called stego-video; if it is concealed in an audio file, it will be a stego-audio, and if it is concealed in an image file, it would be a stego-image, etc. [2-4].

Cryptography achieve different purposes, where the latter hides the information of a secret message from an attacker by converting it to unreadable data. In contrast, steganography hides the existence of the message. Thus, the steganographycan provides more confidentiality and data security than cryptography as it hides the mere existence of the secret message instead of only securing the message contents. However, combining cryptography and steganography can provide more security by taking advantage of both [5,6].

Cryptography is the science of developing cryptographic algorithms to secure data or communication in the existence of an attacker. Two main types of cryptography exist that are classified depending on the type of keys used to encrypt/decrypt the data [7, 8]. Figure 1 shows the standard cryptography algorithms.

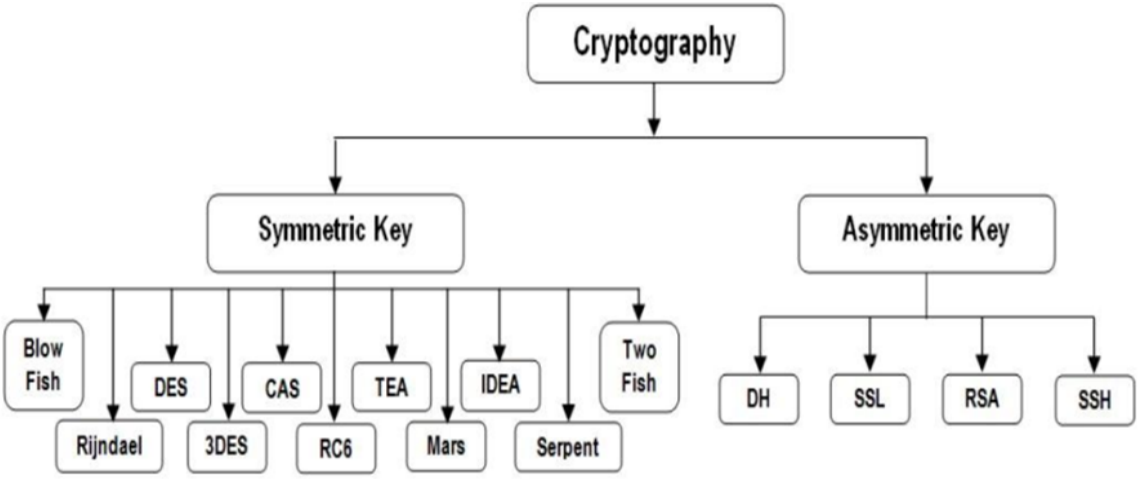


Figure 1- Different symmetric and asymmetric cryptographic algorithms [7]

In secret-key cryptography, one key is utilized for encryption/decryption. The sender makes use of the key (or any specific rules) to encrypt the data and sends the ciphertext to the recipient. The recipient uses the same key in order to decrypt the message and restore the original data. The asymmetric, i.e., public or key cryptography, rather than using one key, uses two keys, public and private, where both are needed to encrypt/decrypt data or transmission. In this work, we utilize a common standard type of secret key cryptography, which is the AES algorithm. This algorithm is a block cipher that supports three key sizes of 128, 192, and 256bits, which are usually referred to as AES128, AES192, and AES256, respectively. The length of the key is denoted by Nk, which refers to the number of 32 bit words in the key. The input and output blocks and the intermediate cipher result have the same length of 128bits. Ls and Nr denote the rounds number of AES, as determined by the key size, which is ten rounds for AES128, 12 rounds for AES192, and 14 rounds for AES256 [9].

Text steganography is one of the sensitive areas of data encoding, since the changes in the cover-media are very perceptible both in terms of syntax and semantics. That is why extra attention is paid while hiding the secret data into the covered text, which also implies that the syntax of the cover text is not awkwardly changed [10]. Based on a comparison study, Agarwal [8] presented three methods of text steganography. The first method is based on the utilization of a missing letter puzzle in which every character of the message has been hidden via removing one or more characters from the cover word. The second approach is based on hiding a message in a word list in which the ASCII values of embedded characters determine the starting letter length of a word. The last approach is to hide the secret message without degrading the cover, which is achieved by using the start and end letter of the cover words. The author also classified text steganography into three types: linguistic, statistical generation and format based random methods. The linguistic steganographyis considers the linguistic properties of the modified and generated text. In many cases it utilizes the linguistic structure to be a space in where the messages are concealed. The statistical and random generation is utilized to avoid comparing the stego cover with a known plaintext. The steganographers often, resort to generating their own cover texts. One of these methods is based on hiding data in the random-looking sequence of characters.

The other method is based on modifying the statistical properties of letter frequencies and word length to create words that appear to have identical statistical properties to those of the actual words in any given language. The third method, i.e., the format-based method, includes physically altering the text format to hide the information. This method has specific disadvantages. In the case that a stego file is opened via a word processor, misspelling, and extra white spaces may be detected. The changes in font size can give a suspicion to the observer. Also, in the case that the original plaintext is likely available, comparing the suspected steganographic text with the original plaintext will make the manipulated parts of the text visible.

Related Works

Many approaches have been achieved for text steganography, such as the syntactic method [11] that deals with text syntax or text format to hide information, in which the punctuation is inserted within

cover text to hidden data. Some examples of this method include the use of comma (,), full stop (.), etc. that placed within cover text in suitable place. The acronym or abbreviation method [12] substitutes the word by its acronym. The word spelling method [13] is based on the fact that different countries have a different vocabulary and the words can be spelled differently. Another method [14] is based on shifting the lines vertically up to a certain extent (such as shifting to 1/400 inch down or up), while words can also be shifted [14] that based on changing the horizontal distance in-between words via inserting white spaces. In the feature coding method [15], the letters are shortened or stretched in terms of their dimension, in addition to changing many text attributes such as color. A random sequence of characters [16] that generated a random string in addition to single letters which is contains the same letters like what in the cover. The inter-sentence space method [17] utilizes spaces between sentences in order to hide the message. The curves method [18] deals with the letter shape. It consists of two groups, which are the A Group that contains letters with curves and the B group that contains letters without curves. The vertical straight-line method [19] is based on formed groups depending on the vertical straight line that appearing. The A group contains words that have a vertical line and the B Group has words that do not have a vertical straight line. Finally, the quadruple categorization method [19] is based on the formation of four groups according to the presence of a single straight vertical line, middle horizontal straight line, multiple straight vertical lines, or a curve.
Recently, many studies focused on combining steganography with cryptography. In 2011, Khalil and Hikmat [20] proposed a method that combined steganography and cryptography. In their work, they used some existing steganography techniques that allow concealing the secret message. They illustrated two different strategies. The first method dealt with combining steganography and cryptography in a way that makes it harder for a steganalyst to obtain the plaintext of a message from a stego-object. The second method employed the steganographic technique only without any cryptographic techniques. They tested both methods and described their benefits and limitations. The results showed that the combined steganography and cryptography can achieve a high-security level than the steganography or cryptography alone. In the same year, Usha *et al*. [11] proposed an encrypting system based on combined cryptography and image-steganography techniques. The conventional approaches were used for this goal, in which the data were encrypted to generate the cipher, which was then concealed within the image. They used a reference matrix for the choices of passwords according to the properties of the image. In 2017, Sharma and Batra [21] presented a hybrid crypto-stego approaches in order to decrease distortion by preserving the robustness and imperceptibility and offering high protection for the e-communication between two certified parties. In 2018, Alsaidi *et al*. [22] presented a multi-level security approach that takes the secret message (text) and compresses it by using the Lempel–Ziv–Welch (LZW) compression algorithm. After that, it is encrypted by using the Advanced Encryption Standard (AES) algorithm to be hidden within a stego message and then forwarded as an email-colored platform. Their results showed that the method of multi-level scheme confers high capacity, motivating security, and sensible performance which proved that the text crypto-stego represent an interesting method that featuring attractive contribution.

This work intended to design crypto-stego methods that utilize AES as a crypto technique and text stego as a hiding technique. The proposed method aimed to improve the security of the crypto-stego hybrid method via a strategy that includes a dictionary list to replace ciphertext vtwalues with corresponding characters or words. In this way, the receiver should have the same list in order to get the original ciphertext as well as a crypto-key to decrypt the ciphertext to get the original message. The proposed time sequence strategy is also utilized in order to increase the security of the dictionary method via rearranging the internal list with time. The time sequence strategy can give an automated dynamic list that changes its values with time and the receiver should have the time sequence algorithm and exact list used by sender in order to know the exact list values (characters or words) that are used instead of the ciphertext values of the proposed stego. The method used is called the "modified space," which is similar to the traditional method, but it differs by utilizing a used space identification number (SIN); the user should have an exact SIN value to retrieve the exact values rather than some additional characters will be evaluated and then changed the ciphertext value, and as a result, no decryption can happen. The proposed method is then compared with some recent efficient methods to determine the best method in terms of cover capacity, time complexity, compression ratio, robustness, visibility, and similarity.

The Main Methodology

In this part, the proposed approach is described in detail. The proposed approach was implemented by using visual C# net language. It essentially consists of two main parts, which are the creptography and the stegography.

The proposed approach strategy is based on misleading the attacker in two ways. The first way is by encrypting the secret message or data by using the AES algorithm. After that, the ciphertext value was replaced by changing each character with the corresponding value from the dictionary list. The list is variable daily and the values of its characters list are also changeable with time. Thus, the user needs to know the exact time of encoding in order to retrieve the original value. The process of determining the exact time is described in the elsewhere in the second stage of this method. The second way is by hiding the modified ciphertext in a cover text by utilizing a modified spacing steganography. The user needs the SIN to identify the exact spacing value, without which it is impossible to identify the exact value of the modified ciphertext. Figure 2 illustrates the proposed system structure and operation.

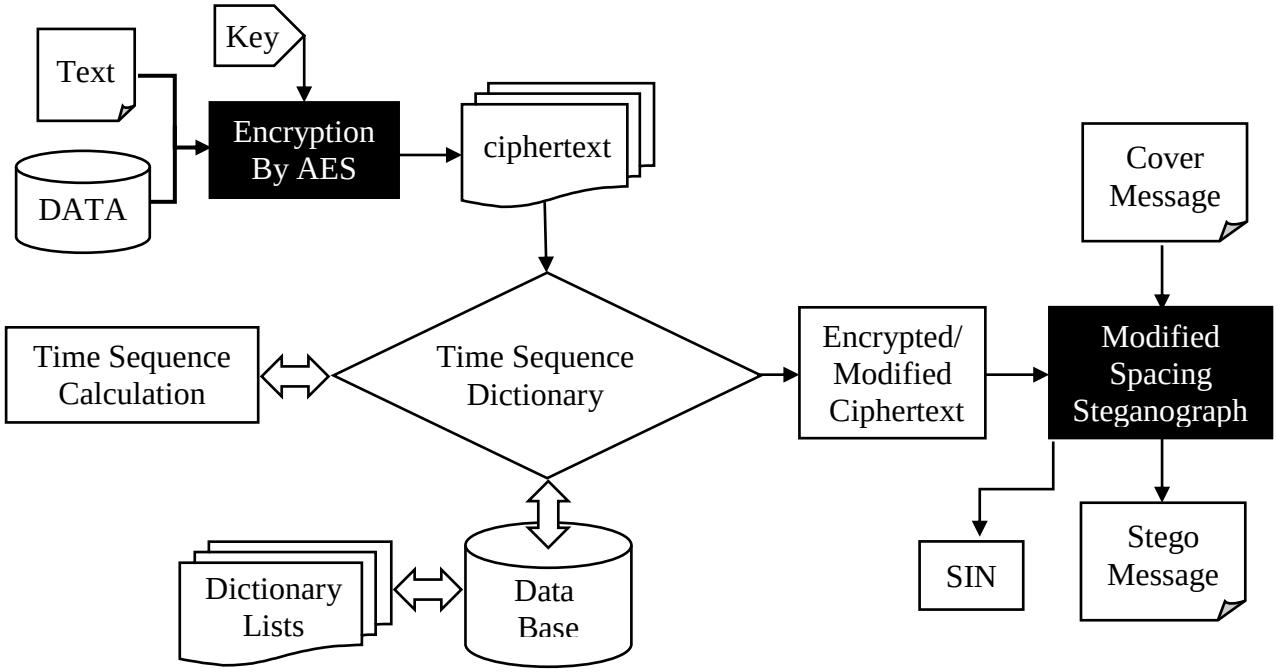


Figure 2-A proposed crypto-stego time sequence system architecture

The Cryptography Part

In this part, the message is encrypted in two stages, as described below.

First Stage: AES Encryption

An AES was used for the encryption, that is based on the Rijndael algorithm. In this work, the AES-256 bit was utilized to encrypt the secret message.

The AES algorithm is demonstrated below. [23]:

Input:	Secret Message, Crypto Key
Output:	Encrypted Message (Ciphertext)

Step 1: Start.
Step 2: Take the internal value of the key phrase used to create the crypto key.
Step 3: Set the key and the IV (Initialization Vector).
Step 4: Create an encryption key depending on the given phrase, which is then hashed to generate a unique 32 character (256bit) value, of which 24 characters (192bit) are utilized for the key and the remaining eight characters are utilized for the initialization vector (IV).
Step 5: Generate key.
Step 6: Take secret message value.
Step 7: Encrypt the provided value by using the Rijndael algorithm.

Step 8: Write the encrypted value into memory.
Step 9: Retrieve the encrypted value and return it.
Step 10: End.

Second Stage: Modifying the Ciphertext by Time Sequence Dictionary

After encrypting the secret message, we replaced each character with a corresponding character in the dictionary list. However, rather than using a stable dictionary list, we used a changeable time-dependent list in order to give more security. In this method, the characters in the dictionary are rearranged as a function of time. The dictionary includes a list of all characters, numbers, and symbols as well as the corresponding characters or words (which depend on human entry). For example, the dictionary includes English letters in upper and lower case, numbers and samples (A = B = Brother, …… a = tell, b = part, …. 1 = low, 2 = TV, ……! = wall, ….). However, as this method aims to modify the ciphertext, the dictionary list which it can be same as the original character or it distributed randomly dependent on user entry (such as A=A or A=&). Figure 3 illustrates a sample of the dictionary in which the input is the same as the output.

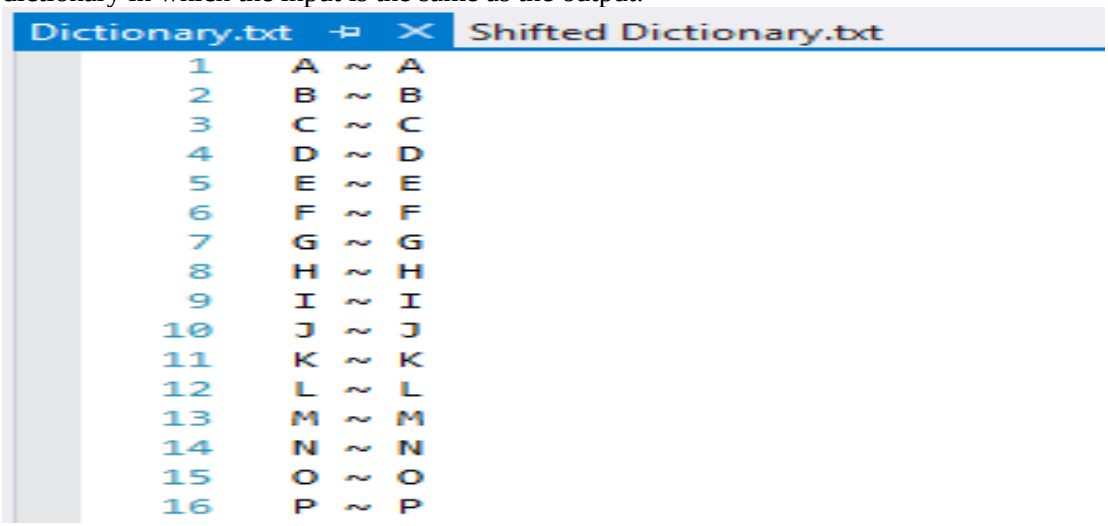


Figure 3- A sample of dictionary lists.

The words in the dictionary change as a function of time. This will give more security because the user should input the exact time at which the message was created, as described in the following procedure. The algorithm will first request a dictionary. Then it will read all lines and separate all the characters, that include letters, symbols, and numbers, from the equivalent characters. This is achieved by using the following equation:

$$X\,(i) \;=\; Y\,(i) \tag{1}$$

where X is the original character and Y is the corresponding character.
The algorithm will also request local date and time. Then, the shifting value will be calculated from the following equation:

$$S \;=\; M \;+\; D \;+\; H \;+\; I \tag{2}$$

where S is the words shifting value at the running time of month (M), day (D), hour (H), and minute (I).
Then, the algorithm will utilize a shifting value to shift the words to a new location by looping Y from equation 1 by the S value, as in the following equation

$$Y\,(i) \;=\; Y\,(i+S) \tag{3}$$

Then, the algorithm will recombine the first word, with the symbol "=", and the second word, as in the following equation:

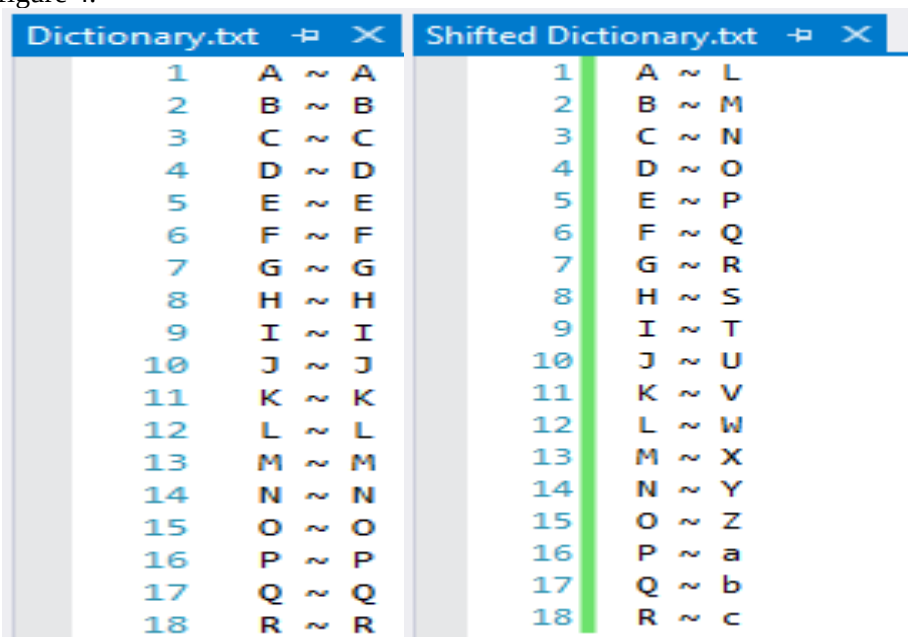
$$X\,(i) \;=\; Y\,(i+S) \tag{4}$$

The rearranged dictionary will be saved for usage in the stego process. The algorithm of Time Sequence Dictionary can be described as follows.

Input:	Ciphertext, Dictionary List (Text), Date and Time
Output:	Shifted Ciphertext (text file)

Step 1: Start.
Step 2: Upload dictionary text file.
Step 3: Get recent data and time (month, day, hour, and minute).
Step 4: Read all lines within the dictionary.
Step 5: Separator characters (X, Y) from the dictionary by using equation 1.
Step 6: Calculate the shifting value from equation 2.
Step 7: Shift the equivalent characters to a new location by applying equation 3.
Step 8: Recombine the first character with the symbol "=" and the equivalent character. Then a new list will be generated.
Step 9: Upload ciphertext.
Step 10: Read all lines within the ciphertext.
Step 11: Apply equation (1) to identify the characters corresponding to original characters.
Step 12: Replace each ciphertext character by its corresponding character.
Step 13: Save the modified ciphertext.
Step 14: End.

For example, let the original dictionary list be as that shown in figure 3 (a). Furthermore, let the time for starting the encoding be the 2nd of February at 8:00 Am. Then, the algorithm starts computing the shifting value based on equation 2, which should be equal to 30, derived from summing the values of day, month, and time (2+2+8+0) which is 12. Hence, the program will shift each character by 12 line, as shown in figure 4.



(a) **(b)**

Figure 4-Results of the rearranged dictionary process where (a) the original list, (b) the rearranged list.

As shown in figure 3, the character A in the original dictionary (figure 4 a) is replaced by the character L in the time-shifted dictionary (figure 4 b) as the time-shifting value is 12 line shifting. However, this dictionary is user-dependent, which means that the list does not need to be in series. Hence, it could be that A = j and b = #, which can give more complexity to achieve more security.

Text Stego

This method utilizes the "Space" to hide the secret message. In this method, we utilized the number of spaces as a dependent value rather than being independent as in the traditional way. The number of

spaces in this method can change the ciphertext value. The user should enter the SIN in order to decode the ciphertext value. The algorithm is constructed as follows.

Modified space Algorithm

Input: Encrypted shifted Secret Message.
Output: Stego. Cover.

Step 1: Start.
Step 2: Take the encrypted string.
Step 3: Convert each alphabet into its ASCII value.
Step 4: Convert ASCII value into an 8-bit binary value.
Step 5: Implement binary value in the form of a number of spaces between words in the cover text input by the user.

- Binary 1 = 1 space
- Binary 0 = 2 spaces continuous.

Step 6: A minimum number of words required in the cover text is calculated by the number of characters in the encrypted string * 8 + 1. This would be the SIN.
Step 7: Adding spaces between word depending on in steps 4 and 5.
Step 8: End.

For example, let the Encrypted String be “Eigrh”, thus the ASCII value and the 8bit values is shown in table 3.1.

Table 1- ASCII and 8bit values for the word "Eigrh."

Characters	E	i	g	r	h
Ascii Value	69	105	103	114	104
8-bit Binary Value	01000101	01101001	01100111	01110010	01101000

Then, the number of words required = 5 * 8 + 1 = 41.
Let the cover text be the paragraph shown in figure 5 (a). Then, the results of hiding the character E that has an Ascii value of (01000101) in the text cover will be as in figure 5 (b).

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

(a)

The0advantage1of0steganography0over0cryptography1alone0is1that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

(b)

The<space><space>advantage<space>of<space><space>steganography<space><space>over<space><space>cryptography<space>alone<space><space>is<space>that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

(c)

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

(d)

Figure 5- An illustration of adding space process by using a modified space algorithm. (a) original text file, (b) the binary value assigned text for hiding the character E that has an Ascii value of (01000101), (c) adding space process corresponding to the binary value, (d) the stego text that would be observed by users.

The <space> text is in the position of binary 1 and the <space><space> text is in the position of binary 0. In the stenograph text above, we showed the binary value of E in the cover text. The same way for other letters is also implemented. However, with modified spaces, the system will continue adding spaces (one space or two spaces) randomly until the end of the cover text. This process is implemented to put a wrong value that represent additional characters which would convert the value of the modified ciphertext, so that the user needs to put an actual value of SIN in order to determine the right ciphertext value. Figure 5 shows the spatial distribution in stego cover.

The<space><space>advantage<space>of<space><space>steganography<space><space>over<space><space>cryptography<space>alone<space><space>is<space>that<space><space>the<space><space>intended<space>secret<space>message<space>does<space><space>not<space>attract<space><space>attention<space>to<space><space>itself<space>as<space>an<space>object<space><space>of<space>scrutiny.<space>Plainly<space><space>visible<space>encrypted<space><space>messages,<space><space>no matter<space>how<space>unbreakable<space>they<space>are,<space><space>arouse<space><space>interest<space>and<space><space>may<space><space>in<space><space>themselves<space>be incriminating<space><space>in<space>countries<space>in<space><space>which<space>encryption<space><space>is illegal.

Figure 6-An illustration of space distribution in a stego text message

The decoding algorithm is written as below.

Algorithm of the Decoding Method 1

Input: Stego. Cover, SIN value
Output: Encrypted shifted Secret Message

Step 1: Start.
Step 2: Take the stenographic text and SIN as input.
Step 3: Count the number of spaces between adjacent words successively, determine the last space that should be taken, depending on the SIN value, and assign binary values to it.
Step 4: For two continuous spaces, assign binary 0, and for one space, assign binary 1.
Step 5: Form groups of 8 binary bits successively.
Step 6: Convert the 8 bits binary into a decimal number.
Step 7: Consider the converted decimal number as an Ascii value and take the character representation of it.
Step 8: In the same way, form characters.
Step 9: Pass the string to decryption.
Step 10: End.

To continue with the previous example, when the user receives a stego. text message (figure 4) that has spaces distributed as in figure 5, the user should enter the SIN value first, then the decoder will compute the spaces that are equal to the SIN number. Thus, the SIN is 8 and the spaces are 8, which represent the 8-bit binary number 01000101, and the decimal number is 69, hence the Ascii value will be 69, which represents the character E.

Results and Discussion

In this part, we tested the proposed approach in terms of computational requirements, time of sequence dictionary rearrangement, cover capacity, visibility, and robustness. In the test, a laptop with moderate computational hardware was used. Table 2 shows the laptop hardware specifications.

Table 2- Hardware and software specifications used in the test

CPU	1.6GHz Core i3
Ram	4 GB DDR2
HDD	300 GB
Operation System	Windows 10 32bit
Software	Visual Studio 2017

Operation Test

In this part, we tested the ability of the proposed method to encrypt/decrypt the secret message. The stages include the input of the secret message, the encryption of the secret message by the AES algorithm, modification of the ciphertext by time sequence dictionary algorithm, and the usage of the modified spacing to hide the modified ciphertext. Figure 7 shows the encryptor/decryptor program.

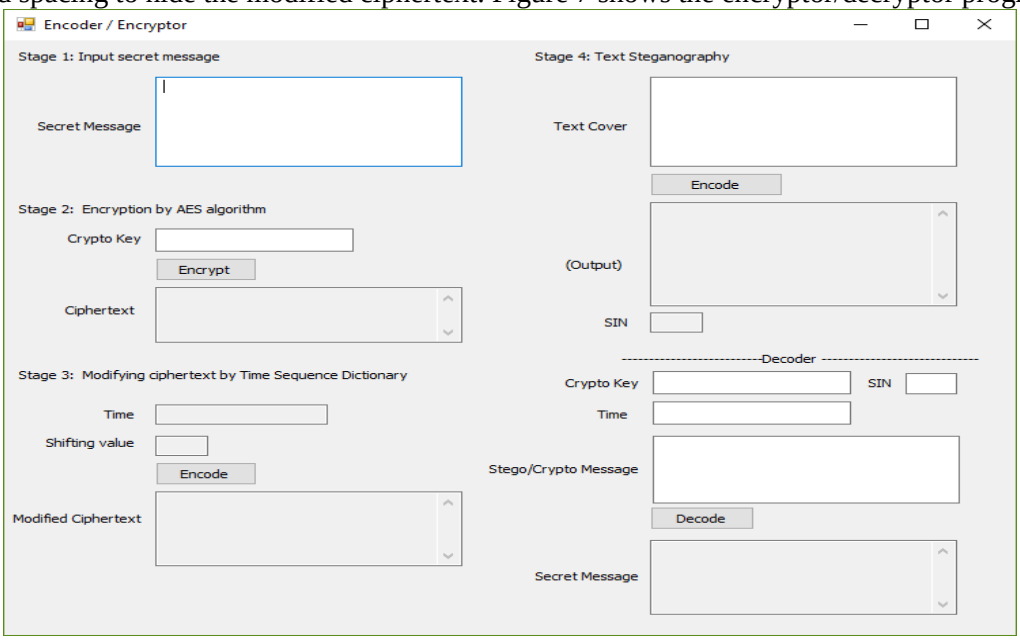


Figure 7-The graphic user interface for the proposed approach

In the test, we used a secret message, "Hello World" and the crypto key "Eman@2019". The test shows that the proposed method runs smoothly without any hang or delay. The encryption results are shown in figure 8.

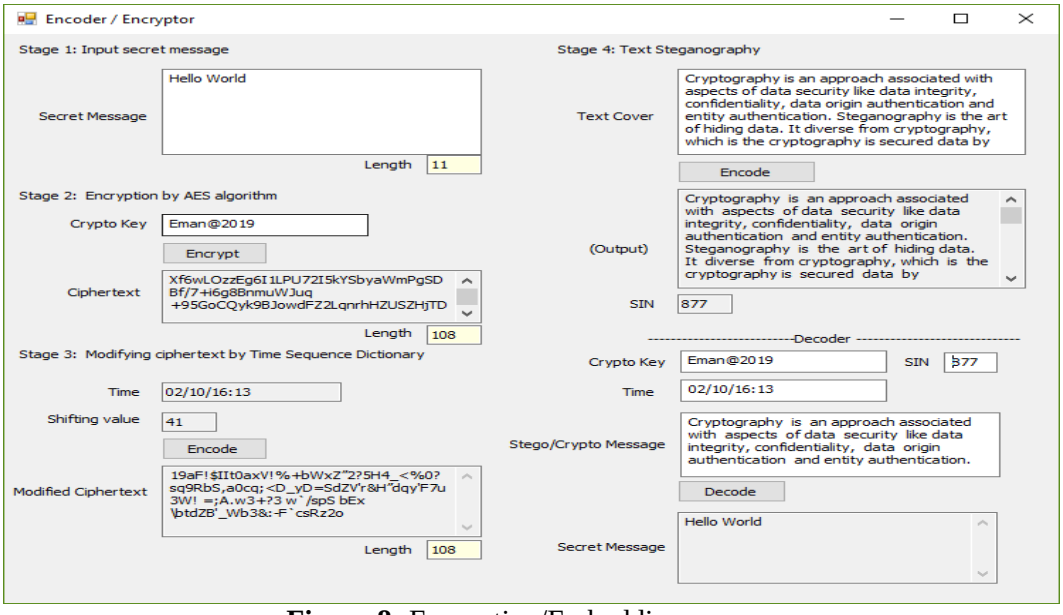


Figure 8- Encryption/Embedding process

Based on the test, we could analyze some aspects related to the security issue of both cryptography and steganography, as described below.

Cover Capacity

In this part, we tested the cover capacity needed to hide the secret message. The capacity of this

method depends on secret message characters and user entry. The secret message used in the test has 11 characters. After encrypting the message, the output ciphertext length is 108 characters, while the modified ciphertext would have the exact length. Thus, the number of words needed to form the modified ciphertext is 877. Therefore, a cover of 1000 words can be useful to embed the encrypted/modified cyphertext with extra characters for security.

Visibility

In this part, we tested the cover for visibility. For the test, we printed a stego message and showed it to a random sample of 20 students from Baghdad University. All the participants were not able to recognize any suspicion in the stegomessage. As can be observed from the message in figure 5(d), the cover message is uniform with no deformation or changes that can be noticed and, therefore, it is difficult to detect by the observer.

Similarity

In this part, we tested the cover for similarity. For the test, we used the Beyond Compare software to compare files, in order to find the similarity between the original cover and the stego message. The results of the software test showed a similarity value of 0.905, which is an excellent result.

Robustness

Robustness is the capability of the stego method to conceal data with the ability to remain undamaged even in the case that the stego cover is being subject to cropping, linear and non-linear filtering, blurring, transformation, scaling, sharpening, and other different techniques. The standard methods used for text steganography robustness are the OCR printing, font changing, copying and pasting, and retyping. Because the proposed method is not making any changes in the shape of characters or adding any extra elements to it, it can be classified as a fully robustn stego method. However, there is still an issue in determining the exact spacing when using an OCR that can retrieve wrong ciphertext values. As a result, no decryption happens.

Cryptanalysis

In this part, we employed a number of available tools that are commonly utilized to test the strength of the cryptography algorithm. As we utilized the AES algorithm to encrypt a secret message, we then selected the cracking tools that are specific to deal with AES ciphertext. These tests included the AES Crack (Brute force on passwords) from asecuritysite.com, AES Encryption and Decryption Online Tool from devglan.com, AES ECB from cryptogrium.com, in addition to the most specific software called "CrypToo", which is the desktop version that can run under the Windows operation system. The results showed that all of these tools failed to crack the ciphertext or identify the continent. However, in our point of view, the proposed method has many points of strength that make the cracking and analysis of data very difficult or even impossible without having many parameters. The first point of strength is the use of AES256, the most secure encryption algorithm that is very difficult to crack when a strong password is used. The second point of strength is that the ciphertext is modified to have new values that change the sequence of ciphertext that should be obtained by using the traditional algorithms. Even if the attacker has stolen the crypto key, it will not be useful, and no decryption will happen without knowing the algorithm. The dictionary list is user-dependent and changeable with time, so that the user needs to put the exact time that the encryption was performed to be able to retrieve the original ciphertext. The third point of strength is that the ciphertext is hidden within the text message, by using the "modified spac" stego method. This method is based on the traditional space method, however it different from traditional method that the spaces are added continuously to a text message after embedded the ciphertext within the covertex. Hence, the user needs to put the exact value of spaces that is used to hide the ciphertext, which is called the SIN. Without the SIN, the ciphertext would have some additional characters that cause failure in decryption. Table 1 shows the modified cipher generated by the tested method (figure 7).

Table 3-Sample of the modified ciphertext generated by the proposed method

Modified Ciphertext Value
19aF!$IIt0axV!%+bWxZ”2?5H4_<%0?sq9RbS,a0cq;<D_yD=SdZV'r&H”dqy'F7u3W!=;A.w3+?3 w`/spS bEx\btdZB'_Wb3&:-F`csRz2o

Conclusions

Hybrid cryptography with steganography is one of the modern security techniques that is based on encrypting the data, then hiding it in the cover medium in order to remove any existing data. The

proposed method was designed to ensure two points of strength. The first one is the use of AES to encrypt a secret message, then utilizing a dictionary with time sequence to modify the ciphertext, so that it is impossible to retrieve the original secret message even with having the encryption key. Besides having the same dictionary, the user needs to know the time at which the message has been encrypted. The second point of strength is the modified space stego method. This method differs from the traditional one that needs the SIN to determine the exact binary value to retrieve the hidden characters within the cover text. Without it, the modified ciphertext value is changed, and no decryption can be achieved. The test results showed that the proposed method runs smoothly and fastly in both processes of encryption and decryption, even with the utilized low computation system.
The results also showed relatively good capacity values when taking into consideration that the secret message is encrypted and, therefore, the length of the message is increased. The visibility test showed that the proposed method is difficult to be noticed, with no participant in the questionnaire sample could suspect changes in any element of the stegomessage. The proposed method also demonstrated full robustness, being able of performing processes such as printing, copying and pasting, and font changing without any problem in decoding. However, one issue with the OCR is that it may fail to detect spaces effectively, and thus no decryption happens. The cryptanalyses test showed that all types of attacking software used in the test failed to identify or crack the modified ciphertext. In summary, can be used as a dependable, highly secured method for securing sensitive information.

References

1. Mark, R.O., **2016**. *Information Security: The Complete Reference*. McGraw-Hill Higher Education - VST E+p, ISBN: 9781259837883.
2. Wassim, AC. *Cryptography and Steganography in Digital Images*. GRIN Verlag, ISBN: 9783668599093, 2018.
3. Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., and Szczypiorski, K. **2016**. Information *Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*. IEEE Press Series on Information and Communication Networks Security, John Wiley & Sons. ISBN: 9781118861691.
4. Essa, R.J., Abdulah, N.A. and Al-Dabbagh, R.D., **2018**. Steganography Technique using Genetic Algorithm. Iraqi Journal of Science, pp.1312-1325.
5. Kumar B, M. and Sailesh C, G., **2020**. Secure Data Communication With Cryptography and Steganography. International Journal of Electrical Engineering and Technology, 11(3).
6. Harba, E.S.I., 2018. Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography. Iraqi Journal of Science, pp.600-606.
7. Keserwani, P.K. and Govil, M.C., 2020, July. A Hybrid Symmetric Key Cryptography Method to Provide Secure Data Transmission. In International Conference on Machine Learning, Image Processing, Network Security and Data Sciences (pp. 461-474). Springer, Singapore.
8. Agarwal, M. Text Steganographic Approaches: A Comparison. *International Journal of Network Security & Its Applications (IJNSA)*, 5(1), pp.91-106.
9. Pachghare, V.K., **2015**. *Cryptography and Information Security*. 2nd ed. PHI Learning. ASIN: B00TQPWHZG,
10. Douglas, M., Bailey, K., Leeney, M., and Curran, K. **2017**. *An Overview of Steganography Techniques Applied to The Protection of Biometric Data*. Springer US, Multimedia Tools, and Applications, 77(13), pp.17333–17373. Available from: https://doi.org/10.1007/s11042-017-5308-3.
11. Mohammad, H.S.S., and Mohammad, S.S., **2006**. *A new approach to Persian/Arabic text steganography*. In Proceedings of 5th IEEE/ACIS Int. Conf. on Computer and Information Science and 1st IEEE/ACIS Int. Workshop on Component-Based Software Engineering, Software Architecture and Reuse, pp.310-315. Available from: https://doi.org/10.1109/ICIS-COMSAR.2006.10.
12. Hassan, S.S., and Mohammad, S.S., **2010**. Arabic/Persian Text Steganography Utilizing Similar Letters with Different Codes. *The Arabian Journal for Science and Engineering*, 35(1B), pp.213-222.

13. Khan, F.R., **2009**. *Enhanced Text Steganography by Changing Words Spelling*. FIT '09 Proceedings of the 7th International Conference on Frontiers of Information Technology. December;7. Available from: https://doi.org/10.1145/1838002.1838082.
14. Sangita, R., and Manini, M., **2011**. *A Novel Approach to Format Based Text Steganography. ICCCS '11 Proceedings of the 2011 International Conference on Communication, Computing & Security Rourkela, Odisha, India*. DOI: 10.1145/1947940.1948046.
15. Changder, S., Das, S., and Ghosh, D. **2010**. *Text steganography through Indian languages Using Feature Coding Method*. 2010 2nd International Conference on Computer Technology and Development. Cairo, Egypt, IEEE. DOI: 10.1109/ICCTD.2010.5645849.
16. Sunita, C., Meenu, D., and Amit, S. **2016**. *Aggrandize Text Security and Hiding Data Through Text Steganography*. IEEE 7th Power India International Conference (PIICON). DOI: 10.1109/POWERI.2016.8077346.
17. Miroslav, Ć., Mladen, V., Bogdan, B., and Zoran, J. **2014**. *Application Steganography Methods of Replacement and Insertion Technique*. 2013 21st Telecommunications Forum Telfor (TELFOR). Belgrade, Serbia, IEEE. DOI:10.1109/TELFOR.2013.6716383.
18. Shraddha, D., Devesh, J., and Aroop, D., **2011**. Experimenting with The Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications (IJNSA)*, 3(6), pp.213-225.
19. Baharudin, O., Roshidi, D., and Mohd, R.I., **2015**. Capacity Performance of Steganography Method in Text-Based Domain. *ARPN Journal of Engineering and Applied Sciences. 2006-2015 Asian Research Publishing Network (ARPN)*. DOI: 10(3):1345-1351.
20. Khalil, C., and Hikmat, F. **2011**. Combining Steganography and Cryptography: New Directions. *International Journal on New Computer Architectures and Their Applications (IJNCAA), The Society of Digital Information and Wireless Communications*, 1(1), pp.199-208.
21. Sharma, N., and Batra, U., **2017**. *A Study on Integrating Crypto-Stego Techniques to Minimize the Distortion*. International Conference on Recent Developments in Science, Engineering and Technology, Springer Nature Switzerland AG., pp.608-615. Available from: https://doi.org/10.1007/978-981-10-8527-7_51.
22. Alsaidi, A., Al-lehaibi, K., Alzahrani, H., AlGhamdi, M., and Gutub, A. **2018**. Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics*, 8(3), pp.33-42.
23. Gueron, S., Feghali, W.K. and Gopal, V., Intel Corp, 2020. Architecture and instruction set for implementing advanced encryption standard (AES). U.S. Patent 10,601,583