RESEARCH ARTICLE OPEN ACCESS

Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography

Assist Prof. Dr. Suhad Malalla*, Msc.Farah R. Shareef **
**(Department of Computer Science, Technology University, Iraq*
*** (Department of Computer Science, Technology University, Iraq*

ABSTRACT
Steganography and cryptography are main tools for secure the information. The integration of steganography with cryptography to secure communication, is an application that integrate Steganography techniques with Cryptography techniques to get more secure communication method. This paper aim to design a system with more sturdy security, by hybrid AES cryptography and text steganography. In this paper we proposed a method that encrypt secret message and then embedding it in cover text. This done by scrambled secret message first through AES encryption algorithm then hiding it into Arabic cover text. This paper also study the efficient embedding technique that can be used for hiding the encrypted data in cover text to hide it from attackers and sent message to the receiver in a safe mode.

Keywords - Security System, Hiding Data, Steganography, Cryptography, AES

I. INTRODUCTION

Peoples have been interested to hide secret messages from the ancient times. Steganography and cryptography can be achieved this purpose through used many different strategies (we have been described it later). Steganography is the science/art of concealment the data in an unnoticed cover object so that no suspicions can be notice from eavesdropper regarding this communication. The steganography technique has many form such as pictures, texts, sound and video files. Otherwise, the cryptography technique is not interested to hiding the message, but it will convert it to incomprehensible form by a process called encryption. [1].

Cryptography is the mathematical techniques related to information security aspects like as confidentiality, entity authentication, data integrity, and data origin authentication. The cryptography secure the information by convert it into an unknown format. The original plaintext, or text is transformed to an equivalent coded known as “ciphertext” by used algorithm of encryption. Just on who has the secret key can decrypt (decipher) the ciphertext into original text. It can be classified the cryptography systems broadly to tow main types: symmetric-key and public-key systems. The first system (symmetric-key) used single key (password) which most have by both (sender and the receiver), while the second system (public-key) used two keys, a public key have by both (sender and the receiver) and a private key that only have by messages recipient [2]. In this paper, we will used only symmetric-key systems and we used AES algorithm for encryption the secret message

In other hand, steganography is the science of concealment the information in some carrier media that could be formatted text, image, video or audio. The main aim of steganography is to hide the existence of data. The process of putting hidden the information inside cover data called “data embedding”. The stego data is the data includes both the "embedded" information and the cover signal. The “cover” is the term referred to innocent message that hide original message and it may be in any form of data such as video, audio, image, text, and so on. The cover in image steganography known as “container”, and for audio signal steganography known as “host signal”. In this paper we dealing with text steganography. There are many challenges for hiding secret message within text cover, the first challenge is that the text documents have comparatively a few redundant information, the second challenges is that the text documents structure is roughly congruous to their look so any change to its content may be noticed. Though, using text steganography to hide information is more preferred than other media steganography due it more efficient, required little memory to save, cost-saving in printing and it is more easily to transfer over the network [3].

Text steganography dependents on the language used as cover media. Because there are many human languages that have different properties and characteristics, there are many algorithms have been used for this purpose. For Arabic language, a many different characters (28 characters) along with some special signs known as “Harakaat”. In addition the Arabic characters in most are joined when writing words consist of many character, in that case there is an extension character that called “Kashida” that can be placed between two Arabic characters depending on the joined characters [4]. Which has two use, one is to to justify the Arabic word within lines, like as spaces that used in English writing that been used for justifying the English words in lines, the second usage is to decorate the Arabic text format to make the looks more convenient and much better (which is very important especially in the documents titles). So for Arabic cover in text steganography, the most Arabic stego algorithms focused on the two characteristics “Harakaat” and “Kashida”. Some algorithms foucs on used some “ḥarakāt” such as (damma, kasrah, fathah, etc.) [5], and other foucs on used “Kashida” [4].

The main difference between cryptography and steganography, the cryptography will encrypted the message and to return it to original form required from receptor to have the proper key, while with steganography, the message appeared as normal message so that many people could not detect the message presence. By hybrid cryptography and steganography it can get more secure method that includes two levels of security. This hybrid method encrypted message first by using cryptography, then it using steganography to hide the encrypted message inside within a cover such as text audio, image, video, etc. and it widely used nowadays in computer for security applications such as protection of: corporate data, credit card information, e-mail messages, etc. In this work we hybrid cryptography (AES algorthim) and text steganography (focused on used some Arabic stego algorithms based on used “Kashida”.

II. RELATED WORK

To ensure a high-quality product, diagrams and lettering MUST be either computer-drafted or drawn using India ink.

Modern researches for Arabic text steganography have been focused on improved the possible applications of it. Shirali-Shaherza et al was the first one proposed a work in this field [6]. Their work is based on concealment the binary values of secret message within Persian or Arabic by used a feature coding method. This method relies on the points inherited in the Urdu, Persian, and Arabic letters. The location of points' in pointed letters concealment the information as follows: Firstly, the Secret Object (hidden information length) look to as binary with the first several bits. Then, the Cover Object (medium text), is scanned. Thus, when detect the pointed letter, their location determine if the value of hidden binary is one or zero. For hidden bit, the point location is slightly shifted up, otherwise, the point location not changed. This method has advantage that it can hide large volume of information in text because the Arabic and Persian letters have a large number of points. Also, this method has disadvantage that lost it is continent in case of retyping.

In 2006, Mohammed A. et al [7], proposed a new method for text steganography that hide secret message inside Arabic text cover media. Their work utilizes Arabic language diacritics that used for vowel sounds which called “Harakaat” that founds in many literary, poetic and Islamic religious documents. These symbols “Harakaat” that used in Arabic are eight different diacritical. From their research they found that the symbol “Fatha” is used more than other seven diacritical symbols in Arabic text. The symbol “Fatha” has a value of 1 and other seven symbols to be 0. Thus, to hide a bit of value 1, the program will searching to find the first location of symbol “Fatha” and then remove it. While to hide 0 they, the program will searching to find the first location for any one of other seven symbols and remove it. This method has advantage which is the high capacity of cover due to it used all diacritical symbols inside Arabic letter, but it has disadvantage, the non-uniform in distribution (hiding some diacritics) may give attention by reader’s.

In 2008, Jibran A. [5], has been used reverse “Fatha” to concealment the secret data within cover text rather than the normal “Fatha”. He was put inverse direction “Fatha” on the Arabic cover (that includes “Fatha” inside). This inverse “Fatha” cannot easily detect by reader, which is an advantage of this method, while it has disadvantage that it needs a new font (that contain reversed Fatha” to be instill because it not a standard diacritic.

In 2010, Mohammad S. et al [8], has been proposed a new method for hiding secret information within Arabic text cover media by used an extension character “Kashida”. Their work try to maximize “Kashida” used to hide more secret information inside Arabic text cover than other methods used same method “Kashida”. To achieve this, a method known as MSCUKAT (Maximizing Steganography Capacity Using “Kashida” in Arabic Text) has been used. This improvement of this work includes: reducing the file size, increased cover media capacity to hide more information, enhanced the encoded cover media security. This tested results of this method has been compared with previous works, and it appeared that MSCUKAT saves 33% of size of cover media (ratio between the secret and the needed characters) than the best “Kashida” method in approaches[], and giving better capacity at least 53% more than other “Kashida” method in approach [].

III. THEORETICAL BACKGROUND

To ensure a high-quality product, diagrams and lettering MUST be either computer-drafted or drawn using India ink.

3.1 Cryptography

Cryptography provides a very important tool to secure message (especially for messages transmission when it transfer from one location to another). The cryptography disguise the original message by convert it to unreadable form, just intended recipients (who have encryption "key") can remove the disguise from message and read original message. The secret message may be encrypted using a "code", or a "cipher" or 'cypher'. In case of "code" each one of characters or a group of characters will be replaced by an alternative one, in case of "cipher" the whole message is converted instead of individual characters. The systems of Cryptographic commonly classified to three are three methodologies of independent dimensions [9].

1. **Text to cipher text transforming Methodology:**
   All algorithms of encryption are based on two common principles: transposition and substitution. In transposition the plaintext elements are rearranged wile in substitution each plaintext element is mapped into another element. The main requirement is not to loss any information be [10].
2. **Keys number Methodology:**
   There are many standards methods of cryptography like: hash function, public key, and secret key, and digital signature [11]:

A. ***Symmetric-key cryptography:*** In symmetric-key encryption, each one of the sender and the recipient should have the code (secret key) that been used to encrypt a packet of information in sender side before it sent to receptor over the network that should have same key to decrypt it. There is two main types of Symmetric-key cryptography AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

1. **DES:** is the an archetypal block cipher algorithm which is take a fixed-length string of plaintext bits then converts it to another cipher-text bit string with same length by a series of complicated operations. In DES the block size is 64bits. The DES uses a particular key for transformation process, so only persons that know the decryption key can view the original continent. Ostensibly the key is consists of 64 bits, but actually the algorithm are used only 56 of these bits, the remained eight bits have been used just to checking parity then it discarded. Thus, the length of effective key is 56bits [13].
2. **AES:** this encryption algorithm is based on substitution-permutation network (SPN) which is a linked mathematical operations series that have been used in block cipher algorithms as in AES. This algorithm is fast in both software and hardware. AES differs from DES (its predecessor) it's not use a Feistel network. AES is a Rijndael variant that has a 128bits fixed block size, and (128, 192, or 256 bits) key size. By contrast, Rijndael the key and block sizes is any 32 bits multiple, both with a minimum of 128bits and a maximum of 256bits [12].

B. ***Public-key cryptography:*** It also well known as "asymmetric cryptography", which is an algorithm of cryptographic that need two separated keys (public key and secret (or private) key). The "asymmetric" term come from the use of two different keys to achieve these opposite functions, as contrasted with symmetric cryptography that use a same key to achieve `both. In spite of differences, this two separated keys are mathematically linked. The public key is used to verify encrypted plaintext or the digital signature, while the private key has been used to decrypt cipher-text or generate a digital signature [14].

1. **RSA:** a crypto-system which is one of the first workable public-key crypt- systems which is vastly used to secure data transmission. For this type of crypto-system, the key of encryption is public and different from the key of decryption that is kept secret. The first publicly described RSA algorithm are Leonard Adleman, Adi Shamir and Ron Rivest in 1977. In 1973, an English mathematician (Clifford Cocks), had been developed system equivalent to RSA, but it was not declassified until 1997 [14].

C. **Digital Signature:** Digital signature has been used due to needs the ensuring of the authentication. The digital signature is like sender signature or stamp that embedded with data together and use private key to encrypt it then send it to other side. Additionally, the signature assures that receiver will be detect any change may be made to the data that has been signed [15].

D. Hash Function: It is a one way encryption, which is a mathematical formula or well-defined procedure which is represent a small size of bits that created from a file of big sized, the function result can be called hashes or hash code. The hash code generating is faster from other methods so it much desired for integrity and authentication. Hash functions are more used for digital signature and it is highly desirable because of cheap constructions. Recently, the use of hash functions become a standard approach for message authentication in different applications, especially for internet security protocols. The integrity and the authentication considered an important issues in secure the information. It can be attached the hash code to the original file, then the users at any time be able to check the integrity and authentication after sending the secure data through put same hash function again to the received message then comparing the hash result to the sender hash code, if it's similar, it means that the received message are came from the original sender with no change in its content, because any changed in original data will changed the receiver side hash code [15].

3. **Methodology for processing plain text.**
The method of processed the plaintext. A two type of processes: stream and block cipher. In block cipher a one input block of elements are processed at a time, generating an output block for each input block, while the in stream cipher the input elements are processed continuously, generating one output element at a time, as it goes along [10].

3.2 Steganography

It is the technology of hiding data in a way that no one can be knowing there is a hidden message except the authorized one. The word "Steganography" are two words: "Stegano" that come from Greek word "steganos" that mean covered or secret, and the "graphy" mean writing or drawing. So the term "steganography" literally means the covered writing. The important purpose of steganography is to secure communicate in a fully undetectable manner and to avoid attracting doubt to hidden data transmission. Through the process, steganography methods characteristics are changes in the features and structure so it cannot be identifiable from human eye. Text, sound, videos, digital images, files, and other files of computer which contains perceptually redundant or irrelevant information can be used as carriers or "covers" to hide secret messages. When a secret message embedding into the cover it called stego (such as for cover-image we obtained stego image). The steganography basic model are consists of, Message, Carrier, Stego key and embedding algorithm. The carrier is also called "cover object" that embeds the secret message and work on to hide presence of that message [16].

1. **Text steganography:**

The concealment of information inside text is most significant method from other steganography methods. Among different types of steganography, the text steganography is more tricky because of the lack of redundant information in text files to hide a secret message as compared to other media. However, the text file have some advantage make it preferable than other types of steganographic methods such as: it needs less memory for storing, it's faster than other methods and it is easier communication. The text steganography method serve to hide a secret message in a cover text message in every nth letter of every word of it. For a large file, text stenography will not be used mostly due to the text files have a very little redundant data [17]. Figure 1 shown the Text steganography scheme.

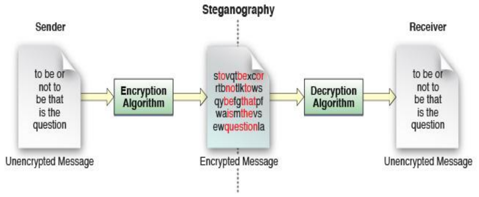

Steganography
Sender
Receiver
to be or not to be that is the question
Encryption Algorithm
stovqtbexcor rtbnotlktows qybefgthatpf waismthevs ewquestionla
Decryption Algorithm
to be or not to be that is the question
Unencrypted Message
Encrypted Message
Unencrypted Message

Figure (1): Text steganography.

2. **Audio steganography**

One of the first considerations for developing an audio steganography method is: the possible environments, the signal of sound will transfer through environments between decoding and encoding. The sound modification are in two main area: the first area is the signal digital representation or storage environment that will be used, and the second area is the pathway of transmission in which sound signal might travel [18]. Figure 2 shown the audio steganography scheme.

3. **Image/Video steganography**

The image steganography is commonly used for hiding secret files, where the images are often used as the cover objects in steganography. A secret message is embedded within the digital image through using a secret key with many embedding algorithms. The stego image that generating will be sending to the receiver. In receiver side, an extraction algorithm has been used to extract original image using the same key. During stego image transmission, the unauthenticated persons cannot guess the existence of secret message he can only noticing the transmission of an image due to steganography.

Video steganography is the technique using the video file as a cover media to hide any type of information such as (text, audio, video, and image). Video steganography are more eligible to hide large size file than other multimedia files due it is large size that can embedding hug information, in addition to memory requirements. Figure 2 illustrated Image/Video steganography technique [19].

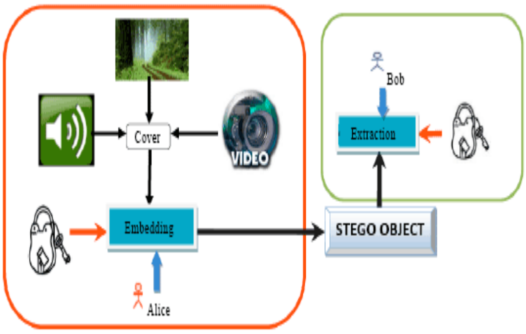


Figure (2): (Image/ Audio / Video) steganography Scheme.

4. Techniques of Hiding Data in IPv4 Header

This method used to secure data transmitting over the network. The principle of this techniques is to fragment data into different sizes rather than a fixed size (same as jigsaw puzzle) then subjoin each data fragment with a sequence number and a pre-shared MAC (message authentication code), so that the receiver can be first authenticate the received data then recombine the received fragments to one single message. In sender side, every fragment of data is suffixed and prefixed with a binary "1" and XOR (exclusive OR) operation with a Random number known as "onetime pad" then will transmitting data over the network. In authorized receiver side, exact opposite process of sender the message is performs to retrieves the original message [20]. Figure illustrated TCP/IP steganography technique

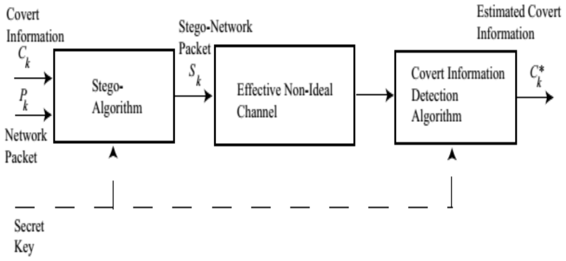


Figure (3): The general covert channel framework in TCP/IP.

IV. HYBRID TEXT STEGANOGRAPHY/ CRYPTOGRAPHY SYSTEM MODEL

Our main goal in this work is to improve steganographic by hybrid it with cryptographic. Indeed, most of the techniques that combine steganography and cryptography work on encrypted secret message first then the output encrypted data will be embedding in a cover object. As for us, we first encrypted secret message with AES algorithm then we used text steganography with different schemes to hide encrypted data. In general, a certain information has statistical characteristics. The number of 0s and 1s are different. This is the evidence of statistical attacks against security methods. In this reason, we aimed to reduce the differences of the number of 0s and 1s. We used 2 methods for this purpose including compression and cryptography. Both of these methods trend to reduce the differences. The compression has been used to reduce the bits by eliminating and identifying statistical redundancy. Algorithms of data compression usually utilize statistical redundancy to represent data more concisely. So, this provides us 2 benefits; reducing the length of secret data and revealing statistical redundancy. Cryptography reveals statistical information about the plaintext that often can be used to break them.

4.1 Algorithm for the proposed system

The architecture of hybrid system is organized with two portions: sender side which consists of Compress secret message, encrypt compressed secret message, embed to stego message, and receiver side which consists of decryption section and extraction section as shown in figure 4.

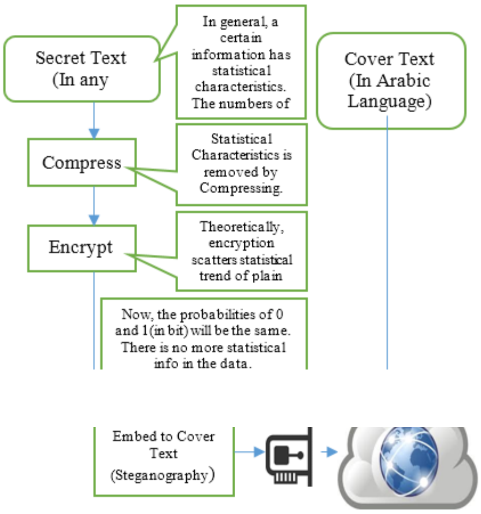

Secret Text (In any
In general, a certain information has statistical characteristics. The numbers of
Cover Text (In Arabic Language)
Compress
Statistical Characteristics is removed by Compressing.
Encrypt
Theoretically, encryption scatters statistical trend of plain
Now, the probabilities of 0 and 1(in bit) will be the same. There is no more statistical info in the data.
Embed to Cover Text (Steganography)

Figure (4): The overall architecture of Stego/AES hybrid algorithm

4.1.1 Compress secret message

The gzip algorithm has been used to compressed secret message. The gzip give a good compression ratio to secret message that encrypted with AES Algorithm. For Compressed Module basically we compressed the Input plain text using Huffman algorithm (Refer Figure 5). (Gzip depend on deflate algorithm that contains LZ77, Huffman encoding [static or dynamic], RLE [for dynamic Huffman tree], Huffman encoding for RLE compressed tree).

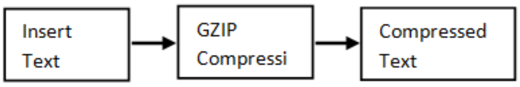


Figure (5): Compress secret message model.

4.1.2 Encrypt compressed secret message

An advanced encryption standard (AES) has been used to encrypt secret message that based on Rijndael algorithm. The symmetric block cipher can be processing (128 bits) data blocks by using cipher keys of (128, 192, and 256) bits lengths. The input and output sequences length of Rijndael can be any of the three allowed values (128, 192, and 256) bits, but for the (AES) the only length allowed is 128.

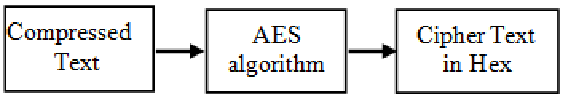


Figure (6): Encrypt the secret message model.

The common best practice for symmetric encryption is to use AEAD (Authenticated Encryption with Associated Data). In this paper, we use AES then HMAC (keyed-hash message authentication code method). A HMAC is a special structure used to calculating the MAC that including a hash function combination with a secret cryptographic key. We uses AES256 and then HMAC SHA256, a two-step Encrypt then MAC that needs more keys and more overhead. The method function takes key(s), secret message string, and an optional non-secret payload then return then authenticated encrypted string optionally prepended with the non-secret data with a 256bit key(s) randomly generated. In addition, it have a helper methods which used a string password for keys generation.

The AES then HMAC algorithm described in follows:

Input:Secret message, cryptography keyword
Output: Cipher Text

Step 1: Start.
Step 2: Insert text for encryption.
Step 3: Use Random Salt to block pre-generated weak password attacks. The salt bit size is 64(at first salt1 is created then derived and used for crypto key in AES and also slat2 is created then derived and used for authentication key for HMAC).
Step 4: Apply AES encryption algorithm by used a 128 Block bit Size and 256 key bit size.

- Convert secret message text to UTF8.
- Convert cipher text to Hexadecimal format, based 64 string and ASCII code respectively.

Step 5: Encryption (AES) then Authentication (HMAC) of a UTF8 message

- Prepend non-secret payload
- Prepend IV
- Write Cipher text.
- Authenticate all data
- Gather encrypted message and using HMAC SHA256 to add authentication.
- Generate encrypt compressed secret message

Step 6: End.

4.1.3 Stego Module

The hiding process is used by the sender to hide the secret message into the cover text. This process involves select the input file, which represents the encrypted compressed secret message, and a group of sub processes as represented in equation 1.

Cover Text + Secret Information (encrypt compressed secret message) = Stego Text … (1)

In this paper we used a good stego model to hybrid with cryptography, which based on using “Kashida” A Four models of text steganography has been used to hiding encrypted secret message which was (Dotted Kashida (After Letters), Dotted Kashida (Before Letters), Dotted Kashida (Mixed Letters), and MSCUKAT [].

These methods used extension character in Arabic language “Kashida” to create a steganography tool to hide a secret message. The work motivation is to test the best possible method of “Kashida” that can be used to hide encrypted message. To achieve this, we have been depends on study in [] and []. In these steady, they determined the Arabic letters that can be extended and they define the rules for four “Kashida” methods (Dotted Kashida (After Letters), Dotted Kashida (Before Letters), Dotted Kashida (Mixed Letters), and MSCUKAT to embed “Kashida” in Arabic text.

As it is known, the Arabic keyboard includes a 35 different formats for 28 letters. Kashida, can come after or before certain letter formats. For both cases, “Kashida” cannot start or end the word, (i.e. it cannot be in the beginning of a word and cannot be in the end of a word), and it is not from the some letters as shown in Table 1 that shows Arabic letters and its letter formats, and shows examples when “Kashida” comes before or after letters.

Adding “Kashida” has a main rule is to put it where applicable (applicable characters has been defined in Table 1), in addition it need to test if the next letter is enter or space to excluded it because adding “Kashida” is not viable in this case.. For method “Dotted Kashida After Letters”, “Kashida” will be put after Arabic letters and when it’s not contravene to the main rules of “Kashida”; The rule, the “Kashida” will be put when have a 0 bit and there is applicable non dotted character for putting “Kashida” after. On the other hand, if we have 1 bit and we have applicable dotted character for putting “Kashida” after For method “Dotted Kashida Before Letters”, “Kashida” will be put before Arabic letters and when it’s not contravene to the main rules of “Kashida”. For Kashida-before, the “Kashida” will be put when have a 0 bit and there is applicable non-dotted character for putting “Kashida” before. For method “Dotted Kashida Mixed Letters”, “Kashida-Mixed”, the “Kashida” will be put after the applicable letter in odd lines of the cover text and put “Kashida” before the applicable letter in the even lines of the cover text. For MSCUKAT method, it used “Kashida” to hide secret bits that have 1value, while secret bits of value 0 will be skipped its applicable location and go to the next. Thus, to hide 1’s it used dotted letters and hide 0’s it used un-dotted letters whereas.

The Stego algorithm of this method are described in follows:

Input: Encrypt Compressed Secret message
Output: Stego Text

Step 1: Start.
Step 2: Insert cover text, encrypt compressed secret message.
Step 3: Remove Kashida from Cover
Step 4: Check Conditions:

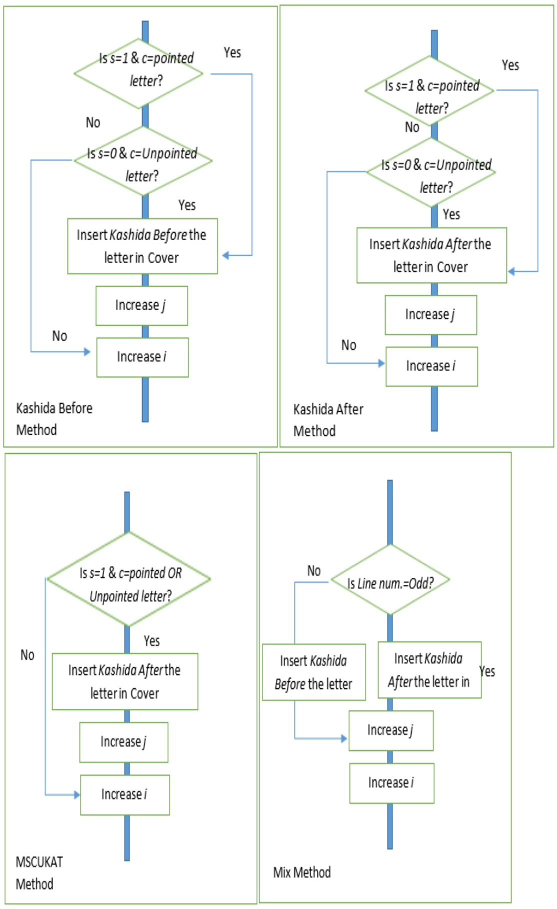
- Arabic Code Zone
- Not Start or End of a word
- Not between ل and ا
- Kashida Table

Step 5: Insert Kashida(depending on the method as: MSCKUT, After, Before, Mix) and secret bit(1 or 0) to Stego
Step 6: Output Stego
Step 7: End.

Table 1: Arabic Letters, their applicability for “Kashida” and Dotted

Letter	Format	Unicode	Applicable fo “Kashida” Before Letter		Applicable fo “Kashida” After Letter		Dotted
أ	آ	1570	ـآ	Yes	آـ	No	Yes
	أ	1571	ـأ	Yes	أـ	No	Yes
	ؤ	1572	ـؤ	Yes	ؤـ	No	Yes
	إ	1573	ـإ	Yes	إـ	No	Yes
	ئ	1574	ـئ	Yes	ئـ	Yes	Yes
	ا	1575	ـا	Yes	اـ	No	No
ب	ب	1576	ـب	Yes	بـ	Yes	Yes
	ة	1577	ـة	Yes	ةـ	No	Yes
ت	ت	1578	ـت	Yes	تـ	Yes	Yes
ث	ث	1579	ـث	Yes	ثـ	Yes	Yes
ج	ج	1580	ـج	Yes	جـ	Yes	No
ح	ح	1581	ـح	Yes	حـ	Yes	No
خ	خ	1582	ـخ	Yes	خـ	Yes	Yes
د	د	1583	ـد	Yes	دـ	No	No
ذ	ذ	1584	ـذ	Yes	ذـ	No	Yes
ر	ر	1585	ـر	Yes	رـ	No	No
ز	ز	1586	ـز	Yes	زـ	No	Yes
س	س	1587	ـس	Yes	سـ	Yes	No
ش	ش	1588	ـش	Yes	شـ	Yes	Yes
ص	ص	1589	ـص	Yes	صـ	Yes	No
ض	ض	1590	ـض	Yes	ضـ	Yes	Yes
ط	ط	1591	ـط	Yes	طـ	Yes	No
ظ	ظ	1592	ـظ	Yes	ظـ	Yes	Yes
ع	ع	1593	ـع	Yes	عـ	Yes	No
غ	غ	1594	ـغ	Yes	غـ	Yes	Yes
ف	ف	1601	ـف	Yes	فـ	Yes	Yes
ق	ق	1602	ـق	Yes	قـ	Yes	Yes
ك	ك	1603	ـك	Yes	كـ	Yes	No
ل	ل	1604	ـل	Yes	لـ	Yes	No
م	م	1605	ـم	Yes	مـ	Yes	No
ن	ن	1606	ـن	Yes	نـ	Yes	Yes
ه	ه	1607	ـه	Yes	هـ	Yes	No
و	و	1608	ـو	Yes	وـ	No	No
	ى	1609	ـى	Yes	ىـ	Yes	No
ي	ي	1610	ـي	Yes	ي	Yes	Yes

(a) (b)


Is s=1 & c=pointed letter?
Yes
No
Is s=0 & c=Unpointed letter?
Yes
Insert Kashida Before the letter in Cover
Increase j
No
Increase i
Kashida Before Method
Is s=1 & c=pointed letter?
Yes
No
Is s=0 & c=Unpointed letter?
Yes
Insert Kashida After the letter in Cover
Increase j
No
Increase i
Kashida After Method
Is s=1 & c=pointed OR Unpointed letter?
Yes
No
Insert Kashida After the letter in Cover
Increase j
Increase i
MSCUKAT Method
No
Is Line num.=Odd?
Insert Kashida Before the letter
Insert Kashida After the letter in
Yes
Increase j
Increase i
Mix Method

(c) (d)

Figure (7): Stego block diagrams for: (a) Kashida Before, (b) Kashida After, (d) MSCUKAT, and Kashida Mix.

The output of this process will be a stego text which will be used from the recipient to retrieve the secret message. Figure (7) illustrated the block diagram of stego program.

V. RESULTS

This part shows the experiments results that leads to measure the performance of the proposed system and compares the different types of "Kashida" text steganographic approaches. The system has been designed by used c# language and includes. The tested has been run by used a workstation laptop (Dell) with following specifications:

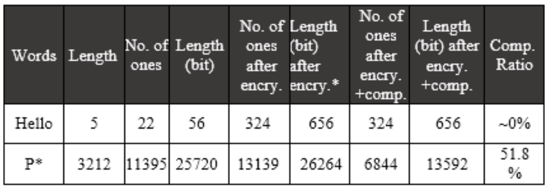
- CPU 1.8 GHz core i3
- RAM 4GB DDR3
- OS Windows 8 64bit
- Visual studio 2013

In our test we used some words to calculate their bit size, bit size after encryption, bit size after compression, size of the cover text needed, and time required for encryption and decryption.

5.1 Capacity

For our test we calculated the secret message bit size before encryption and after encryption and with and without compression for one words and for a large paragraph to calculate the compression ratio.

Table **2:** the secret message capacity with or without encryption and compression.



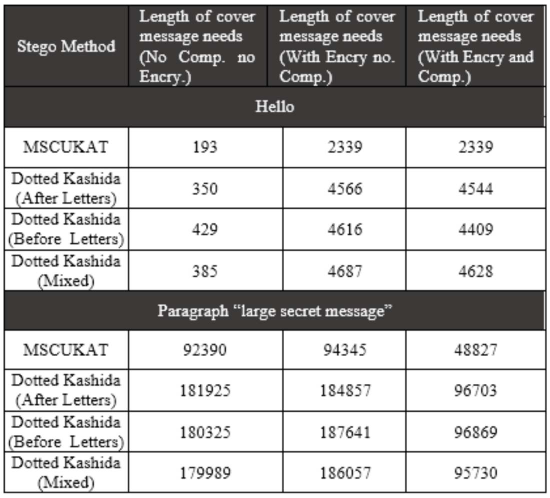
Words	Length	No. of ones	Length (bit)	No. of ones after encry.	Length (bit) after encry.*	No. of ones after encry. +comp.	Length (bit) after encry. +comp.	Comp. Ratio
Hello	5	22	56	324	656	324	656	~0%
P*	3212	11395	25720	13139	26264	6844	13592	51.8 %

* The P is an English paragraph (3212 byte).
** The encryption Key that been used is "Farah123456".

From table 2, the results shows that compression with (gzip) is very useful with large secret message that is be practically efficient.

In second part, we calculate the cover capacity need to hide secret information. The cover capacity needs for each stego method has been shown in table 3.

Table 3: cover capacity of stego methods with or without compression and encryption

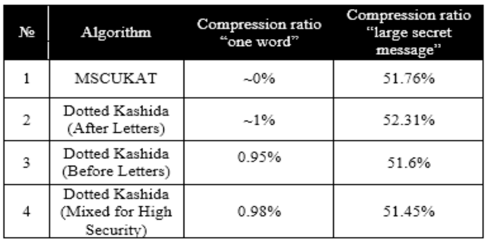


Stego Method	Length of cover message needs (No Comp. no Encry.)	Length of cover message needs (With Encry no. Comp.)	Length of cover message needs (With Encry and Comp.)
Hello			
MSCUKAT	193	2339	2339
Dotted Kashida (After Letters)	350	4566	4544
Dotted Kashida (Before Letters)	429	4616	4409
Dotted Kashida (Mixed)	385	4687	4628
Paragraph "large secret message"			
MSCUKAT	92390	94345	48827
Dotted Kashida (After Letters)	181925	184857	96703
Dotted Kashida (Before Letters)	180325	187641	96869
Dotted Kashida (Mixed)	179989	186057	95730

5.2 Compression Ratio

For our test we calculated the compression ratio of each stego method, which calculated depends on table 3.

Table 4: compression ratio of stego methods (with Encrypt no Comp.) and (with Encrypt and Comp.).

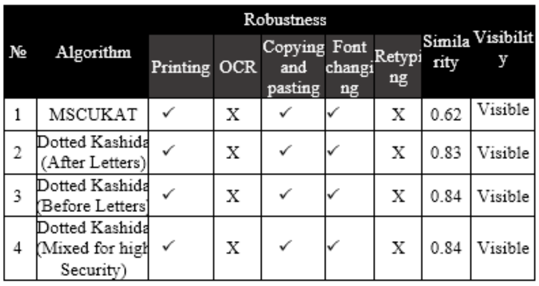


№	Algorithm	Compression ratio "one word"	Compression ratio "large secret message"
1	MSCUKAT	~0%	51.76%
2	Dotted Kashida (After Letters)	~1%	52.31%
3	Dotted Kashida (Before Letters)	0.95%	51.6%
4	Dotted Kashida (Mixed for High Security)	0.98%	51.45%

5.3 Robustness, Visibility, & Similarity

Robustness is the resistance of the steganography technique against modifying or destroying the secret message. Table 5.

Table 5: Robustness, similarity and visibility for five methods.



№	Algorithm	Robustness					Similarity	Visibility
		Printing	OCR	Copying and pasting	Font changing	Retyping		
1	MSCUKAT	✓	X	✓	✓	X	0.62	Visible
2	Dotted Kashida (After Letters)	✓	X	✓	✓	X	0.83	Visible
3	Dotted Kashida (Before Letters)	✓	X	✓	✓	X	0.84	Visible
4	Dotted Kashida (Mixed for high Security)	✓	X	✓	✓	X	0.84	Visible

VI. CONCLUSION

The emphasis of this paper is to develop a hybrid method that combine cryptography and steganography. In this paper, an AES algorithm has been used to encrypt the secret message. Text steganography technique has been used to hiding the encrypted secret message which will give an improvement in security. A Four models of text steganography has been used to hiding encrypted secret message which was (Dotted Kashida (After Letters), Dotted Kashida (Before Letters), Dotted Kashida (Mixed Letters), and MSCUKAT. The experimental results showed that it need more cover capacity when used cryptography method for short message which will be increased to 10-12 times more than cover capacity without encryption, so that usage a compression model which be efficient to compress large amount of data will be useful to reduce the cover size needs to hide message and gzip is a good choice for this purpose. From results it appeared that MSCUKAT are the best stego model that can be used to hybrid with encrypted secret message because it give a lower cover size needs to hide secret message than other methods. The proposed technique can be further improved to have more security, robustness and reduced cover capacity through used new stego method or compression techniques.

REFERENCE

[1]. Manish M. and Navdeep K., *"Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques"*, I. J. Computer Network and Information Security, DOI: 10.5815/ijcnis,, 2012, pp. 76-92.

[2]. Siddharth T., Prashant K. K., *"A Novel Information Security Scheme by Creptic Video Stegnography"*, International Journal of Computer Technology and Electronics Engineering (IJCTEE), *Vol. 2, Issue 1,* ISSN: 2249-6343, (2012), pp.65-69.

[3]. Jain V. K., *"Information Technology Issues & Challenges"*, Excel Books India, ISBN: 978-8174467065, 2009.

[4]. Ahmed A. N. and Adnan G., *"Exploit Kashida Adding to Arabic e-Text for High Capacity Steganography"*, In Proceedings of the International Workshop on Frontiers of Information Assurance & Security (FIAS'09) in conjunction with the IEEE 3rd International Conference on Network & System Security (NSS'09), Gold Coast, Queensland, AUSTRALIA, 2009.

[5]. Jibran A. M., Kamran K., and Hameedullah K., *"Evaluation of Steganography for Urdu /Arabic Text."*, Journal of Theoretical and Applied Information Technology (JATIT), *Vol.4, No.3*, 2008, pp.232–237.

[6]. Shirali-Shahreza H., Shirali-Shahreza M., *"A New Approach to Persian/Arabic Text Steganography"*, 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 06), 2006, pp. 310- 315

[7]. Mohammed A., Sameh A., AbdulRahman E., and Adnan G., *"Arabic Diacritics Based Steganography"*, In Proceedings of the IEEE International Conference on Signal Processing and Communications (ICSPC'07), Dubai, UAE, 2007, pp.756–759.

[8]. Adnan G., and Ahmed A. N., *"High Capacity Steganography Tool for Arabic Text Using 'Kashida"*, The ISC Int'l Journal of Information Security (ISeCure), *Vol.2, No.2,* pp.107–118, (July 2010).

[9]. S. D. Joshi, Anil G., and Sunita B. *"Information security using encrypted Steganography"*, National Conference on Advanced Computing and Communication network, 9- 10 March 2007.

[10]. Gurtaptish K., *"An Efficient Text Storage Security Algorithm Research fellow"*, International Journal of Application or Innovation in Engineering & Management (IJAIEM), *Vol.2, Issue 6,* ISSN: 2319 – 4847, 2013.

[11]. A. J. Raphael and V. Sundaram, *"Cryptography and Steganography-A Survey"*, 2010.

[12]. Himanshu G., *"Twin Key Implementation in AES"*, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, *Vol.16, Issue 5*, pp.01-05, (2014).

[13]. Vibha V., Avinash D., *"Analysis of comparison between Single Encryption(Advance Encryption Scheme (AES)) and Multicrypt Encryption Scheme"*, International Journal of Scientific and Research Publications, *Vol.2, Issue 4,* ISSN: 2250-3153, (April 2012) .

[14]. Sadkhan A. M., Sattar B., *"Multidisciplinary Perspectives in Cryptology and Information Security: Advances in Information Security, Privacy, and Ethics"*, Book, IGI Global, ISBN: 978-1466658097, 2014.

[15]. Shailendra M. P., Sandip R. S., Vipul D. P., and Puja S., *"A Survey on compound use of Cryptography and Steganoghaphy for Secure Data Hiding"*, International Journal of Emerging Technology and Advanced Engineering (IJETAE), *Vol.3, Issue 10,* ISSN: 2250-2459, (October 2013).

[16]. Ali K. H., Zaidan B. B., Zaidan A. A. and Hamid A. J., *"An Overview on Hiding Information Technique in Images"*, Journal of Applied Sciences, 10: 2094-2100, DOI: 10.3923/jas.2010.2094.2100, 2010.

[17]. May H., Su W. P. *"A New Embedding Algorithm for Data Security"*, International Conference on Data Mining, Electronics and Information Technology (DMEIT'15), Pattaya, Thailand, 2015.

[18]. Swati M., Manish S., Dr. Anubhuti K., *"Audio Steganography by Different Methods"*, International Journal of Emerging Technology and Advanced Engineering (IJETAE), *Vol.2*, *Issue 7*, ISSN 2250-2459, (2012).

[19]. Chandra P. S., Ramneet S. C., and Abhishek K., *"Enhance Security in Steganography with cryptography"*, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) *Vol.3*, *Issue 3*, ISSN (Online): 2278-1021, March 2014, pp.5696- 5699

[20]. Suresh. A, Devendra K., Malathi P., *"A Survey on Various Form of Data Hiding Techniques"*, International Journal for Scientific Research & Development (IJSRD), *Vol.3*, *Issue 09*, ISSN (online): 2321-0613, (2015).

[21]. Mujtaba S., M., Asadullah S., *"A Novel Text Steganography Technique to Arabic Language Using Reverse Fatha"*, Vol.1, 2011.