IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. III (Sep. - Oct. 2016), PP 37-45
www.iosrjournals.org

A New Modified Fatha Method For Arabic Text Steganography Hybrid With Aes Encryption

Assist Prof. Dr. Suhad Malalla [1], PhD student Farah R. Shareef [2]
[1](Department of Computer Science / University of Technology, Iraq)
[2](Department of Computer Science / University of Technology, Iraq)

Abstract: *Growing the size of attacks that listed during the passing of data between the sending and the receiving has really demand to get high robust method for transfer information in secure manner. Both of cryptography and steganography are familiar and more utilized techniques which process data for encrypt and conceal the secret message, respectively. Two techniques are participating in the same aims and security services like: confidentiality, integrity and availability for secret message from not allowed access. In our paper we focused on the strength of combination between two techniques and this paper presents a new modified fatha in Arabic text in steganography. This method is depend on the existence of Harakt in majority of Arabic alphabets. On this basis, information was hidden in text by modified Fatha which in same direction of original Fatha but with little oriented to be like original one and not be suspicious and observed as abnormal sign. We combined this new stego method with AES encryption.*

Keywords: *modified Fatha, AES, Steganography, cryptography*

I. Introduction

In these days the communication is expanded due to the developing new technologies like Internet, mobile phones, computers etc. By using these technologies in different domains of life and work, the issue of information security has won special significance. Exchanging the hidden information is one of the important domains of information security which includes different methods e.g. cryptography and steganography.

In steganography the information is concealed in the cover media so no person observe the presence of the secret information. The working of steganography have been implemented on different Medias like text, video, images, and sounds [1].

Cryptography divided into two classes; first, the encryption by symmetric key and second, the encryption by public key. In the first encryption, the sending side and receiving side used the symmetric key for encryption and decryption the secret message. In the second encryption, two dissimilar keys are used; first for encryption and the second for decryption [2].

In Cryptography, the cipher message for example, might raises suspicion on the side of the recipient while the unseen message created with methods of steganography will not. The steganography can be helpful when the use of cryptography is not allowed: where cryptography and strong encryption are outlaw, steganography can prevent such policies to cross the message covertly. Nevertheless, steganography and cryptography differ in the way they are judged: steganography be unsuccessful when the "enemy" is able to reach the content of the cipher message, while cryptography be unsuccessful when the "enemy" discovers the existence of a secret message in the steganographic medium. The subject of study techniques for decoding cipher messages and discovering hide messages are called Cryptanalysis and Steganalysis [3].

The aim of this paper is to describe a method for integrating together cryptography and steganography through text and develop a new steganography technique for Arabic language called Modified Fatha.

II. Related Work

In 2007, Mohammed A. et al [4], proposed a new steganography method to hide secret information into Arabic text cover media. The proposed approach utilizes diacritics in Arabic language which are used for vowel sounds and found in many religious documents. There are eight different diacritical symbols used in Arabic. They found that one diacritical symbol, "Fatha", is used in Arabic text as much the other seven diacritical symbols. So, they used "Fatha" symbol to represent 1 and the other symbols to represent 0. To hide bit of value 1, they search for the first applicable location for "Fatha" and then remove it. And to hide 0 they search for the first applicable location for other diacritical 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 2011[6], A Novel Text Steganography Technique to Arabic Language Using Reverse Fatha (الفتحة) , This technique is based on the existence of Harakat in majority of Arabic alphabets. The information was hidden in the text by placing the reverse Fatha.

III. Theoretical Background

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. [7].

There are many standards methods of cryptography like: hash function, public key, secret key, and digital signature [8]:

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. **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 [9].
2. **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 [10].

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 secret message(plaintext) or the digital signature, while the private key has been used to decrypt cipher-text or generate a digital signature [11].

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 [11].

C. Digital Signature

Digital signature has been used due to needs the ensuring of the authentication. The digital signature is the same of 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 [12].

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 the file of big sized, the function output 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 in any time be able to test the integrity and authentication after sending the

secure data through put same hash function again to the received message then comparing the hash output to the sender hash code, if it's the same, 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 [12].

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 [13].

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 trickier 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 [14]. Figure 1 shown the Text steganography scheme.

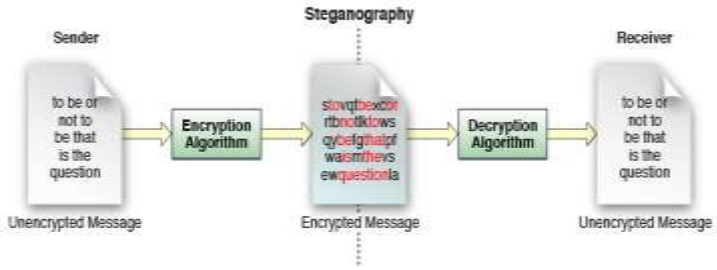

Figure (1): Text steganography

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 [15]. 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 [16].

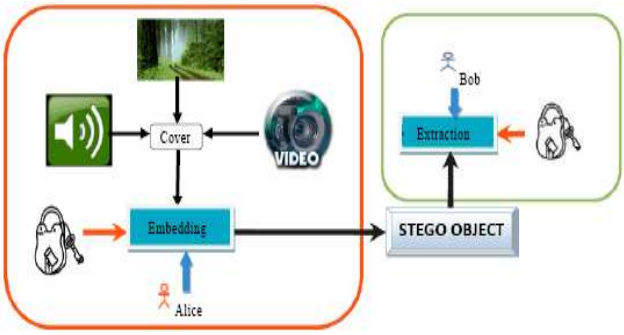

Figure (2): (Image/ Audio / Video) steganography Scheme.

IV. Proposed Mdified Fatha Technique Hybird With Aes Encryption.

In this work, we improve the steganography by hybrid it with cryptography. 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 *modified fatha* 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- Architecture of the proposed system

The architecture of hybrid system is organized with two portions: sender side which consists of Compress the encrypted secret message, embed to new stego method (Modified Fatha), and receiver side which consists of decryption section and extraction section as shown in figure 3.

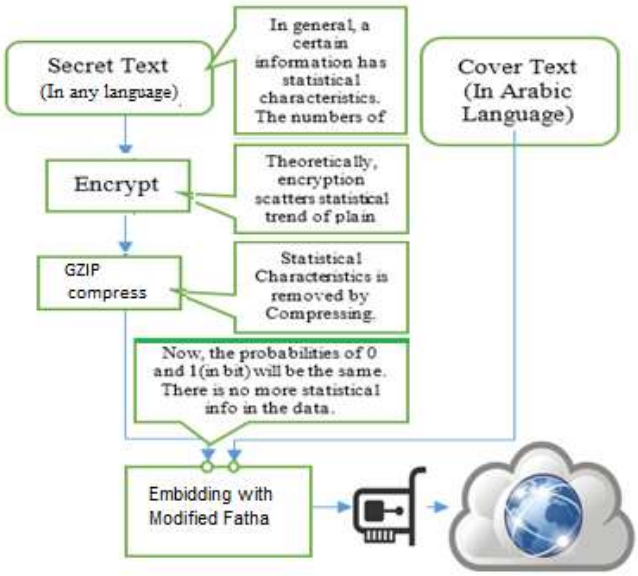

Figure (3): The overall architecture of Stego/AES hybrid

4.1.1 Encrypt 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.(see Figure 4)

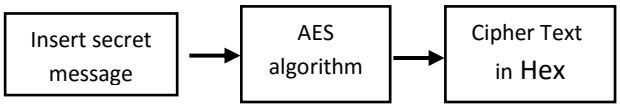

Figure (4): Encrypt the secret message model.

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.

4.1.2 Compress Encrypted Secret Message

The gzip algorithm has been used to compress the encrypted secret message. The gzip give a good compression ratio to secret message that encrypted with AES Algorithm. For Compressed Module basically we compressed the encrypted text using Huffman algorithm (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).

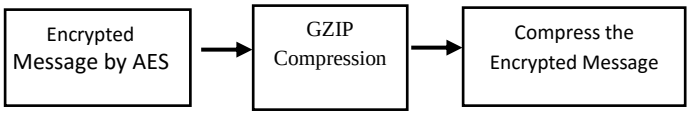

Figure (5): Compress secret message model.

Algorithm of Encryption with compression

Input: Secret message, cryptography keyword
Output: Encrypt Compressed Secret Message(ECSM)

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.

Step 6: - Call GZIP compression to compressed data.
Generate encrypt compressed secret message (ECSM).
Step 7: End.

Algorithm of Decryption

Input: Encrypted Compressed Secret Message (ECSM)
Output: Secret Message.

Step 1: Start.
Step 2: Decompressed (ECSM) by used GZIP algorithm.
Step 3: Convert the message (which is decoded from stego-cover) to UTF-8.

Step 4: Grab *salt1* and *salt2* (8-byte for each one) from Encrypted Message.
Step 5: Derive Crypto key from salt1 and Authentication key from salt2.
Step 6: Use Authentication key for HMAC SHA256:
- Grab (*Sent-Tag* 32byte) from Encrypted Message.
- Calculate Tag (HMAC SHA256) by using Authentication key and Encrypted Message.
- Compare between *Sent-Tag* and *Calculation Tag* to check the integrity of the message

Step 7: Grab *IV* (16 byte) from Encrypted Message:
- Use Crypto key and IV for AES decryption in order to get bytes of secret message
- Convert bytes to string

Step 8: 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 proposed a good stego model (Modified Fatha) which based on using "Harakat" to be hybrid with AES encryption.

One of the characteristics of Arabic language is the use of Araabs i.e. (Fatah, Kasra, and Damma). Where Fatha is slash like symbol and is written over the character, whereas Kasra is also a slash like symbol but is used below the character and Damma is number nine like symbol which is also placed over the character. In our work we used a new modified Fatha which in same direction of original Fatha but little oriented to be like original one and not be suspicious and observed as abnormal sign (Figure 6). The Stego algorithm and implementation for this method are described in follows:

(a) (b)

Figure (6): Fatha shape: (a) Normal, (b) Modified.

4.1.4- Implementation

We use these steps for using new font:

1) Create the new font which is called Modified Fatha.
2) Install New Modified Fatha font in the Windows Fonts.
3) Using the font in word processing software like MS Word 2013, to implement Modified Fatḥa technique.

We used software named Font Creator version 9.0 and predefined fonts for the Arabic language are used in this research. The process begins by editing a glyph Fatha in Arabic Typesetting font family having Unicode $064E to glyph new Modified Fatḥa having same Unicode in the same font family.

STEGANOGRAPHY ALGORITHM (ENCODING NEW MODIFIED FATHA)

Input: Encrypt Compressed Secret message (ECSM)
Output: Arabic Stego Text

Step 1: Start.
Step 2: Insert cover text (with Harakat includes Fatha), encrypt compressed secret message.
Step 3: Prepare two fonts. One is normal font, and the other is modified fatha font. If we use another sign, there should be corresponding font.
Step 4: Split the cover text with a special delimiters including punctuation marks and space and non- Arabic letters, and especially Fatha (and the other signs if they are used).
Step 5: Iterating secret bits, embed it to the cover text.
Step 6: Find the next text segment including Fatha.
Step 7: If the current secret bit is 1, change the font of segment to modified Fatha font and then embed in the fatha.
Step 8: If the current secret bit is 0, change the font of segment to normal Fatha font and then remain all harkat.
Step 9: Output Arabic Stego.
Step 10: End.

DECODING NEW MODIFIED FATHA

Input:	Arabic Stego Text.
Output:	Encrypt Compressed Secret message (ECSM).

Step 1: Start.
Step 2: Enter Arabic stego cover text.
Step 3: Convert stego cover to UTF-8.
Step 4: Check:

- ♣ If the font is (Modified fatha font) and (new fatha is exist) then Return 1.
- ♣ If the font is (Normal font) and (Any haraka is exist) then Return 0.

Step 5: Gather each 8-bits to get byte and then convert it to string.
Step 6: End.

V. Results

This part shows the experiments results that leads to measure the performance of the proposed system. 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

5.1- **Capacity**

This part used to calculate the change in size of secret message due to encryption and compression process. At first we calculated the secret messages sizes before and after encryption and compression ratio to determine the changes and the gain from using compression to reduce the message sizes that will be improving the hiding process by reducing cover capacity needed.

Table 1: the secret message capacity with or without encryption and compression

Secret Message	Secret Message Language	Secret Message (length)	Before Encrypt+ Compression		After Encryption(AE)		After Encrypt+ Compression (AEC)		Comp. Ratio
			No. of 1's	No. of char.	No. of 1's	No. of char.	No. of 1's	No. of char.	
S1	Arabic	1340	8871	19152	9659	19736	4261	8472	57.0%
S2	English	3212	11395	25720	13114	26264	6713	13592	48.2%

* Compression ratio= (size before comp. (AE) – size after comp. (AEC)) / size before comp (AE).
** The encryption Key that been used is "*baghdad16*".

From table 1, the results shows that compression with (gzip) is very useful with large secret message that is be practically efficient.

5.2- Hiding capacity

In second part, we calculate the Hiding capacity (in bits/Bytes) need to hide two secret messages with fixed cover. The cover capacity needs for Modified Fatha stego method has been shown in table 2.

Stego Method	Length of cover (real used) With (Encrypt + Compression)					
	Real used of cover	Secret (S1)	Hiding capacity (bits / bytes)	Real used of cover	Secret (S2)	Hiding capacity (bits / bytes)
Modified Fatha	**41886**	**8472 bits**	**20.2**	**67162**	**13592 bits**	**20.2**

Table 2: Hiding capacity of Modified Fatha stego method for 2 secret messages with fixed cover (length=258107).
*(Hiding capacity= secret (bits) / real used of cover (bytes)

5.3- Robustness, Visibility, & Similarity
Robustness is the resistance of the steganography technique against modifying or destroying the secret message. See **Table 3**.

Algorithm	Robustness					Similarity	Visibility
	Printing	OCR	Copying & pasting	Font changing	Retyping		
Modified Fatha	✓	X	✓	X	X	1.0	Hard to notes

Table 3: Robustness, similarity and visibility for Modified Fatha method.

VI. Evaluation Results (Visibility)

Survey is conducted for Arabic text steganography between two models one for *Arabic typesetting* font and the second for *Arabic modified Fatha* font for the same text, on sample of 40 people like teachers, students in the University of Technology.
The results of survey (questionnaire) are:

Number of people didn't find any thing A	Number of people in Doubt but couldn't find any thing B	Number of people find a difference between two models C
25	**10**	**5**

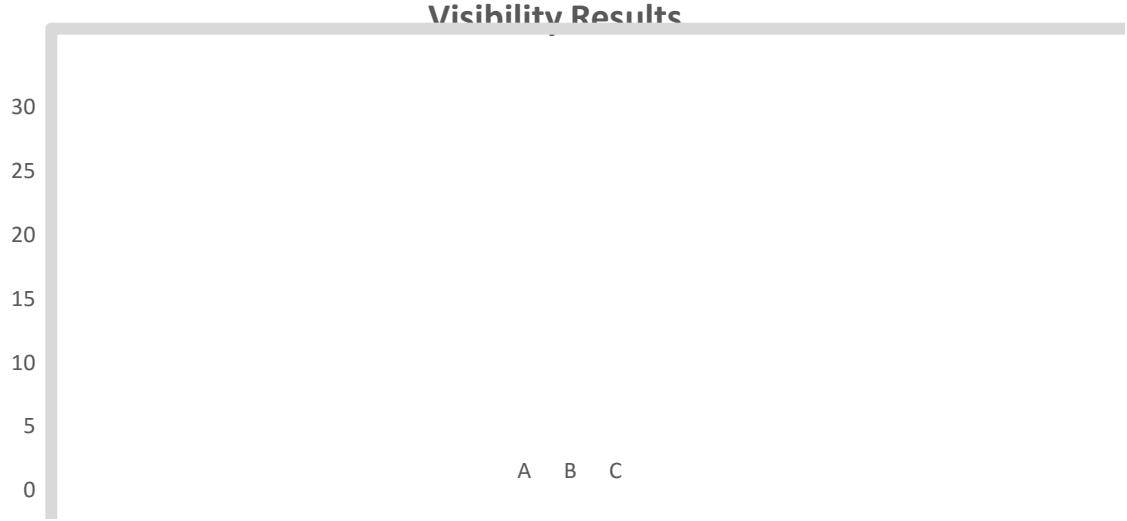

Figure (7) - Bar chart for visibility results obtained in evaluation process

In percentage, the results are:
1- Number of people didn't find anything= 62.5%
2- Number of people in Doubt but couldn't find anything=25%
3- Number of people find a difference between two models=12..5%

Figure 7 shows the statistics that have been calculated from the questionnaire asked in evaluation process. The article with questionnaire was distributed amongst 40 people (teachers and students), 5 could find a difference, and only 10 people were in a doubt while 25 could not find anything suspicious. These statistics show that even by giving the readers a hint for presence of secret message, about 62.5% of the readers neither were able to detect anything nor had any doubt. The remaining 25% of the readers had some kind of doubt about the presence of a secret message between two models and only 12.5% were able to detect the secret message.

VII. Conclusion

This paper is emphasizes on developing the hybrid method that combine cryptography and steganography. In this paper, an AES algorithm has been used to encrypt the secret message. New text steganography technique (Modified Fatha) has been used for hiding the encrypted secret message which will give an improvement in security.

The proposed system can be further improved to have more security, robustness and reduced cover capacity through used new stego method and GZIP compression technique.

References

[1]. Mohammad S., M. Hassan Shirali-Shahreza,An Improved Version of Persian/Arabic Text Steganography Using "La" Word, Proceedings of IEEE 2008 6th National Conference on Telecommunication Technologies and IEEE 2008 2nd Malaysia Conference on Photonics, 26-27 August 2008, Putrajaya, Malaysia.

[2]. Ammar Odeh,"Robust text steganography algorithms for secure data communications", PHD thesis, UNIVERSITY OF BRIDGEPORT, May 2015.

[3]. Bharti P., and Soni R., *"A New Approach of Data Hiding in Images using Cryptography and Steganography"*, International Journalof Computer Applications, Vol.58, No.18, pp.1-5, 2012.

[4]. Mohammed Aabed, Sameh Awaideh, Abdul-Rahman Elshafei,Adnan Gutub, "Arabic Diacritics Based Steganography", *IEEE International Conference on Signal Processing and Communications (ICSPC 2007)*, Pages 756-759, Dubai, UAE, 24-27 November 2007.

[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, pp.232–237, (2008).

[6]. Mujtaba S. M., Asadullah S.," A Novel Text Steganography Technique to Arabic Language Using Reverse Fatha (الفتحة) ",PJETS Volume 1, No 2, 2011 .

[7]. Prof. 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).

[8]. A.Joseph Raphael,Dr.V.Sundaram ., Head & Director, "Cryptography and Steganography-A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630,(2010).

[9]. 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).

[10]. 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)

[11]. Sadkhan Al Maliky, Sattar B., "Multidisciplinary Perspectives in Cryptology and Information Security: Advances in Information Security, Privacy, and Ethics", Book, IGI Global, ISBN : 9781466658097, (2014).

[12]. Shailendra M. P., Sandip R. S., Vipul D. P., 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).

[13]. Ali K. Hmood, B.B. Zaidan, A.A. Zaidan and Hamid A. Jalab, "An Overview on Hiding Information Technique in Images", Journal of Applied Sciences, 10: 2094-2100, DOI: 10.3923/jas.2010.2094.2100, (2010).

[14]. 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).

[15]. 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).

[16]. 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, pp.5696-5699, (March 2014).