Journal of Information Hiding and Multimedia Signal Processing ©2021 ISSN 2073-4212
Ubiquitous International Volume **12**, Number **4**, December **2021**

Secure Communication by combined Diffe-Hellman key exchange Based AES Encryption and Arabic Text Steganography

Farah R. Shareef Taka
Directorate of Institutional Development and Government Coordination
Baghdad, Iraq
Corresponding author's Email: sabahaliraq2014@gmail.com

Received August 2021; revised October 2021

Abstract. *In this paper, the model of security is suggested which emphasize the notion of security over privacy for texting. During the previous few years, we have lot of tools for security that have been designed to protect the objects of multimedia transmission. But programs for the security of text messages are minimal in comparison. The approach suggested by us collect cryptographic technique known as "Diffie-Hellman approach", and text steganography methods (our previous works) for the purpose of design a real-time crypto-stego system ,that can to perform strong and fast encryption strategy, that can be applied to many areas such as chat software or as standalone third-party software for existing social media software to secure conservation.*
Keywords: Cryptography, Steganography, Diffie-Hellman, AES

1. Introduction. The security of information is a major concern in the latest communication area, and should be taken into account while transmitting data via an a public network. Information access in an a public network is not limited by country borders; anyone from anywhere in the world can access the data. As a result, sending data via the Internet opens the data to unauthorized users. Information-hiding techniques are well-known in numerous fields, such as internet banking, intelligence agencies, medical imaging, online elections and military to reduce security risk [1].
For this manner, steganography and cryptography innovations can be assumed a vital part of the framework of digital information security. Cryptography is important because it protects confidential information by making it incomprehensible [2], see Figure 1.

However, Cryptography has a weakness that the information of encryption can make the doubtful about its privacy and a third party's influence can be tempered though preferred standpoint of steganography is, it shields private information through embedding it into a different digital file thus putting the secret information undetectable so there is a lesser chance of susceptibility. The steganography is a growing research subject with the purpose of providing state-of-the-art information security framework development. [5].
Steganography with Cryptography is a useful approach to conceal the encrypted message in a carrier file so that no one could ever suspect the existence of hidden message [6]. This approach provides more security to confidential message. By hybrid Cryptography and Steganography approach it has the potential to perform Steganography with strong encryption technique. There are several approaches in last years that focused on hybrid many techniques of cryptographic such as RSA, AES, HMAC, etc. [7]. In this work we try to utilize cryptographic technique known as "Diffie-Hellman Approach" in order to design a real-time crypto-stego system that can perform hybrid method with strong and fast encryption strategy.
Whitfield Diffie and Martin Hellman created the Diffie-Hellman protocol in 1976, which is used for exchanging keys between various users engaging in group communication over an unsecured

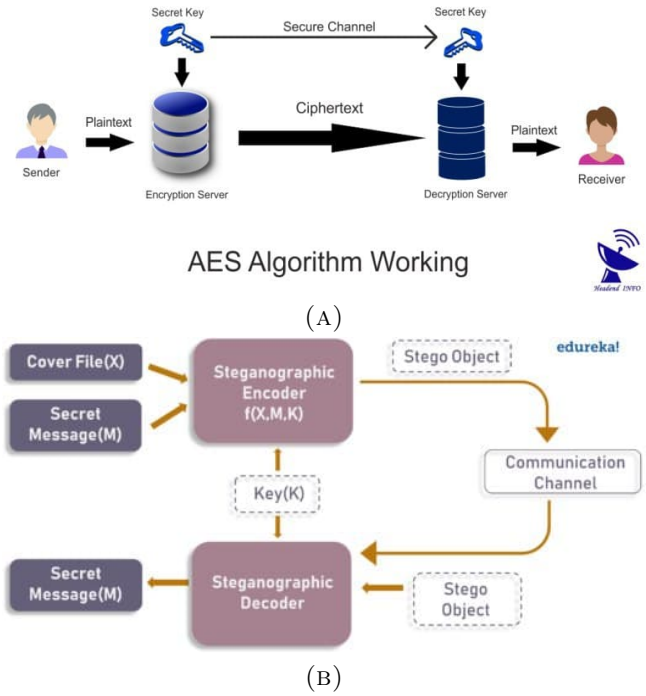


FIGURE 1. Standard security structure for, (a) Cryptography by AES algorithm [3], (b) Steganography [4].

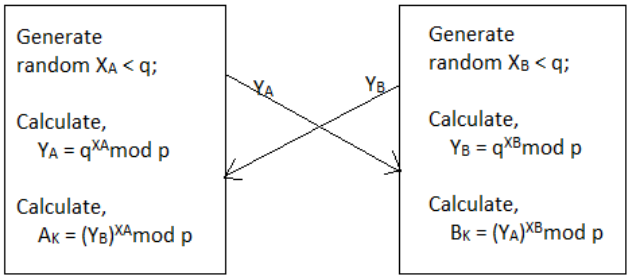


FIGURE 2. The algorithm of Diffie-Hellman key exchange [10].

channel [8]. This will be used as the encryption key for a period of time, especially in order to develop a common key afterwards (Session). The AES algorithm and the Diffie-Hellman key exchange were used to protect data when sending. The first sender of the encrypted file exchanged or produced the key for the ciphered file utilizing the Diffie-Hellman key exchange, following the acquisition of the key, the file would be encrypted and decrypted using the AES technique and the sender would transfer the file to the receiving party over server first to save data, The recipient would then decipher the file to read it. it, allowing a receiver to read it [9]. The application in this work, combined the AES encryption method and the Diffie-Hellman Key Exchange. Figure 2 shows the Diffie-Hellman key exchange algorithm.

2. Literature Survey. The steganography can be utilized adding to cryptography by concealing a ciphered message in the cover text; this is referred to as double steganography. [11]. This method of adopting has been employed in a number of research [12]. When they encrypted the concealed message before hiding it, they got good results.. A general process of crypto-stego hybrid method involves three steps [13], as shown in Figure 3. As shown from Figure 3, stego message, "StM" is the result of the crypto-stego process that has a secret message embedded in it. For text steganography, the text is used as the cover medium. A produced stego message should be like main cover message to prevent third parties from discovering the

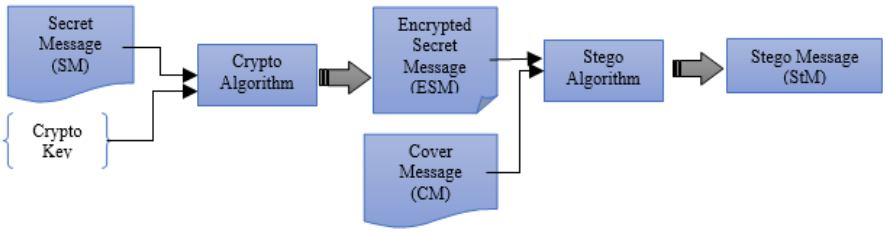


FIGURE 3. Typical crypto-stego method scheme

concealed message. In [14] proposed a scheme of text watermarking based on hiding objects. It solved problem from the level of programming objects in office and concealed these objects that could record information, this method yielded better outcomes in terms of robustness, and a similar time possesses the good embedded capacity and the faster embedded speed. In [15] suggested a method that employs the use of traditional Chinese characters, which have been encoded by the Big5 standard, and some traditional characters, called coherent characters, had the equivalent look as well as their simpler counterparts different encoded by the GBK standard. The advantage of suggested method was hiding conduct data by altering the coherent characters' encodings, and the incoherent characters were already utilized to raise the speed of embedding.

In recent years, there are several approaches that combined text steganography and cryptography. [16], proposed a hybrid crypto-stego system that combined AES cryptography together with text steganography. In their model, the main message is encrypted and then embedded in the text of cover. This accomplished by scrambled the main text message initially by using the algorithm of AES encryption and after that it will be concealed by Arabic cover text. Additionally, they study the best stego method that can be used to concealing the encrypted data in the text of cover, so as to protect it from attackers in such a way that receiver receives a secret message in a trusted mode, our proposed method's improvement on [16], by using Diffe-Hellman key exchange to provide more security for online secret messages [17], explain a mathematical formula as well as the number system and making use of AES as encryption algorithm as well as steganography in which text message is often used as a cover medium, the proposed method's distinction is using large secret messages that can be concealed in Arabic text cover depending on Diffe-Hellman key exchange [6], proposed a reliable system for security that designed for concealing categorized Arabic text-data on minimal processors devices gaining from the hybrid two methods: steganography for Arabic text and lightweight cryptography. There work considers that in order to secure the secret text-data on devices have minimal computational resource. In their work, they make use of two-layer technique, in which it firstly encrypts the secret text-data of Arabic by evaluating strength of various LWC algorithms, such as AES, DES; then, concealing the data that is encrypted within diacritics inside the media of Arabic text cover. The test results show the potential for employing LWC security of DES and AES encryption by take inconsideration their appropriate effect on stego-cover of the text, the advantages of the proposed method is using Diffe-Hellman key exchange based on AES encryption combined with two strong methods for concealing secret messages than diacritics method which is attract the attention of readers.

For using cryptography based Diffie-Hellman key exchange, there are various studies investigates the utilize of Diffie-Hellman key exchange for secure communication. [18], designed a system represents the public-key cryptosystems in which it provides fixed size cipher texts classes, where it provides high performance of keys decryption accessible for all the encrypt text which have been produced. The owner of data can release a single key with a set size and maintain encrypted files that always confidential. Hence, these single keys may be sent to others or it will be stored in a card by using limited number of storage units. [19], suggested, Due to the lack of entity authentication in the Diffie-Hellman key exchange protocol, it is prone to man-in-the-middle and impersonation attacks. The Algorithm of AES and Diffie

Hellman can be used to enhance the security of the sole method; the distinction in our proposed technique is providing more security by using combination of Arabic text steganography with Diffe-hellman based on AES encryption. [9], proposed a model that collect the Diffie-Hellman Key Exchange with the encryption algorithm (AES). This application was the first to employ Diffie-Hellman Key Exchange to exchange a keys that are shared. The outcomes showed that utilizing Diffie-Hellman with 1024-bit keys, provided the same level of security as using the 3DES 2 key technique, If Diffie-Hellman uses a 2048-bit key, the security is equivalent to 3DES 3, If Diffie-Hellman uses a 3072-bit key, the security is identical to AES-128, and if Diffie-Hellman uses a 7680-bit key, the security is identical to AES-182, If Diffie-Hellman was used with keys of 15360 bits, the security was equal to AES-256 bits.

3. The Main Methodology The aim is to design a real time crypto-stego model. The suggested model's cryptography combines the Diffie-Hellman Key Exchange and the encryption algorithm (AES). The model is first using Diffie-Hellman Key Exchange to perform the aim of transforming shared secret key. Then it would utilize the mechanism for encrypting data with a private key, AES for encrypt the message. The second part is the stego part, in which the encrypted message is concealed inside a text cover message via one of two stego methods, which are MSCUKAT (our previous models in [16]) or Bloodgroup (our previous models in [20].

The proposed model is used Diffie-Hellman Key exchange to make a shared secret key between two clients that made text chat between them (client A and client B) by utilizing the user entered p, g, client A secret key and client B secret key. Then, the model would keep going utilizing the algorithm of AES encryption with the produced shared secret key to cipher the message of user when the user presses on the "send" button. In addition, there is an option to compress the encrypted message (the compressing method is based on GZIP compression as described in [21]), so it can reduce the cover message length in stego part. However, the user should select the desired stego model and write or uploaded the cover message (or it can be selected automatically by model from various cover messages saved in data base. This stego processes is also done when user press "send" button where the encrypted message is contained in the cover message and sent from client A to client B and vas various. At the receiving point, the client first should be select the desired stego method too. The client B should receive the client A stego message instantly and run decoding/decryption processes directly by first decoded stego message and retrieve the encrypted message and would also decrypt the ciphertext and display the decrypted result to the user. Figure 4 shows the architecture of proposed model.

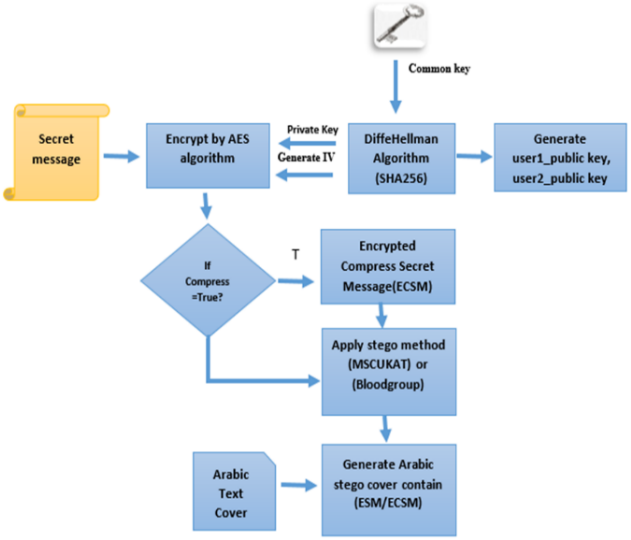


FIGURE 4. Encryption/Encoding Scheme

3.1 Proposed Model Algorithms The proposed model algorithms can be described in following steps.

3.1.1 Main Encryption/Encoding Algorithm His algorithm represents the overall algorithm steps of model that includes encryption with Diffie-Hellman Key exchange and hiding by text steganography using our model (BloodGroup or MSCUKAT

Algorithm 1
Input: Arabic cover text ,cipherd message
Output: Arabic Stego Text.

1- Start..
2- The numbers g and n were generated by the server.
3- The client produces the number x while using the server's g and n values to compute $X = g^x$ mod n.
4- The X number is sent to the server as a result.
5- While receiving the numbers g and n from the server, the client (receiver) generates the y number.
6- Compute $Y = g^y$ mod n. The Y value that results is delivered to the server.
7- The client computes $K = Y^x$ mod n and stores K in the database as the private key to encrypt the Y value sent by the receiving client.
8- Check compress if compress is selected then compress encrypted message. If not ignore this process.
9- Determine the stego method (MSCUKAT or Bloodgroup)
   a. **If MSCUKAT**
      1- Delete Kashida inside the Arabic cover text.
      2- Analyse the Conditions of the Arabic Letters:
         • The zone of the Arabic Code.
         • The letter, which is not at the end of a word or at start.
         • The letters should not between ل and ا.
         • Kashida table.
      3- Kashida should be placed according to the technique (MSCUKAT).
         • Put Kashida after the current letter in the cover if the secret bit is equal to one and the current letter in the cover is appropriate (dotted or non-dotted).
         • The cover counter should be increased, if the secret bit is 0
      4- Aggregate the letters' outcomes.
      5- Stego output.
   b. **If Bloodgroup**
      1- Determine two cases of characters: previous characters (P) or current characters (C).
      2- Test blood group classes for dotted letters, non-dotted letters, and isolated letters (Group A for dotted letters, Group B for non-dotted letters, and Group AB for isolated letters).
      3- Test Rules:
         3.1 - If the preceding letter was from group A or B and the present letter is from group A or B, the bit of text message is equal to one. Then:
            a. Test for Kashida inside the Arabic cover text and remove it if it appears.
            b. Test the conditions for letters of Arabic:
            • Arabic Code area..
            • It doesn't start with the word or end with the word.
            • It does not exist between ل and ا.
            • Kashida table.
            c. After the previous letter, write "Kashida.".

3.2 - In case when the bit of text message is equal to 1 and if the previous letter is from group A and the current letter is from group AB, start modifying of the Unicode to medium class of the current letter.

3.3 - In case when the bit of text message =1 and if the preceding letter is from B group and the current letter is from group AB, start modify the Unicode to medium class of the current letter.

3.4 - In case when the bit of text message=1 and if the previous letter is from group AB and current letter is from group AB, begin by modifying the Unicode to isolate the present letter's class.

4- Aggregate outcomes.

5- Generate Arabic stego text.

10- Send message.

11- End

The decoding process can be illustrated in figure 5:

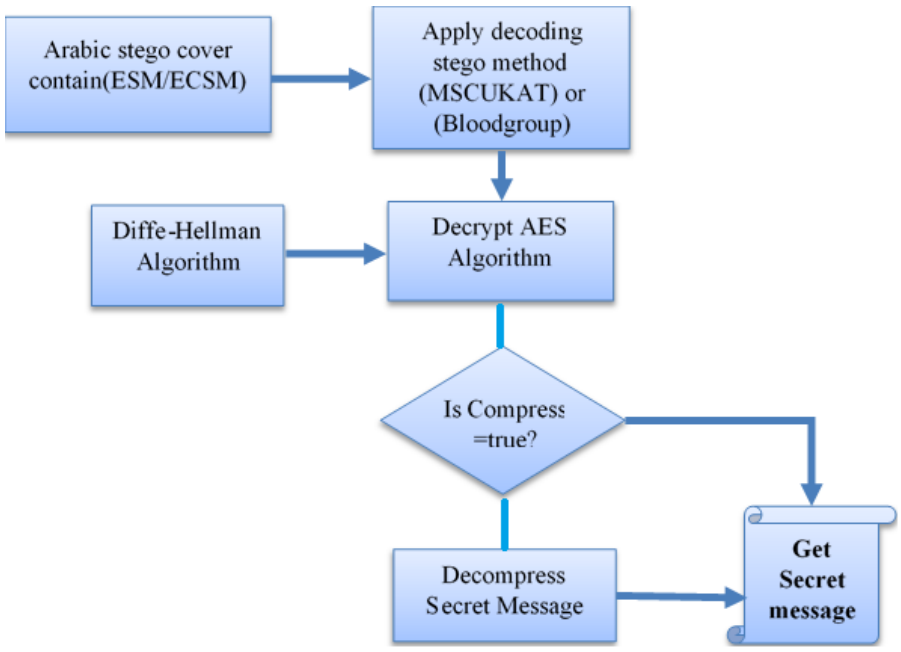


FIGURE 5. Decoding/Decryption Scheme

Algorithm 2. MSCUKAT Extracting..
Input: Stego in Arabic Text.
Output: Arabic cover text ,ciphered message

1- Transform the stego-cover text message to UTF-8.
- If Kashida appears in a text message and there is an appropriate letter (dotted or non-dotted) before Kashida, return one.
- If there is no Kashida and there is an appropriate letter, return zero.

2- Get every 8bits to obtain byte and after that transform it to string.

Algorithm 3. Method of Extracting Blood Group .
Input: Stego in Arabic Text
Output: Arabic cover text ,ciphered message

1- The stego should be converted to (UTF-8).
2- Checking conditions:

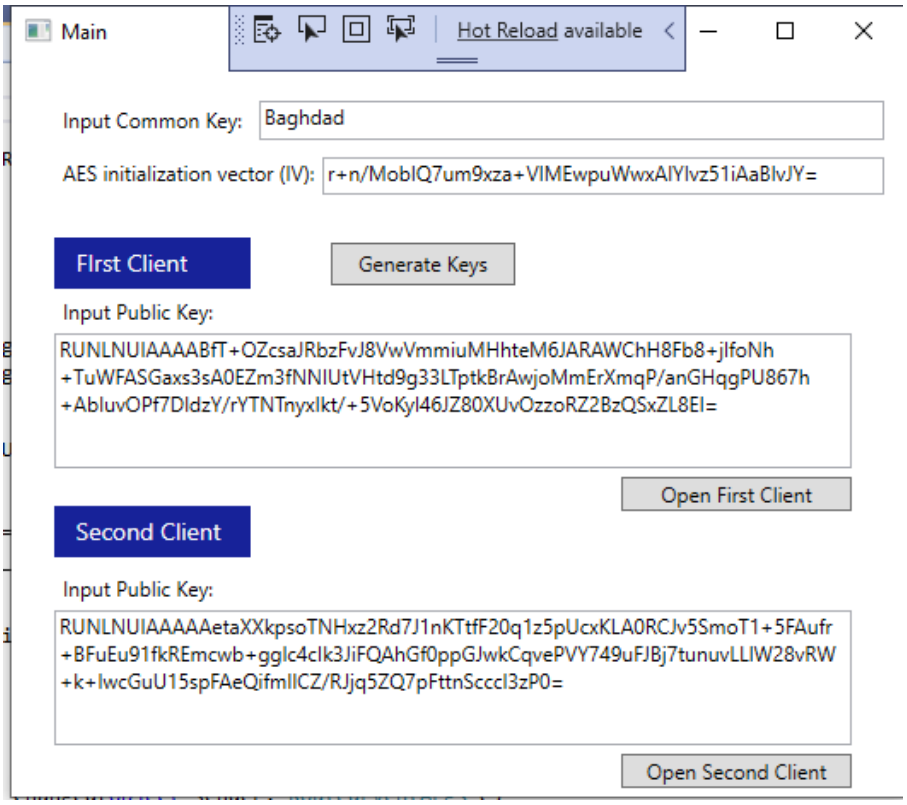
- In case the preceding letter is from group A and the current letter is from group A and if Kashida code is exist then return one.
- In case the previous letter is from group B and the current letter is from group B and Kashida code is exist then return one.
- In case the previous letter is from group A and the current letter is from group AB and if the medium class code of the current letter is existing then return one.
- In case the previous letter is from group B and the current letter is from group AB and if the medium class code of the current letter is existing then return one.
- In case the preceding letter is from group AB and the current letter is from group AB and if the isolated class code of for current letter is exist then return one.
- Otherwise, return zero.

3- Aggregate every 8-bits to return one byte and then transform it to string.

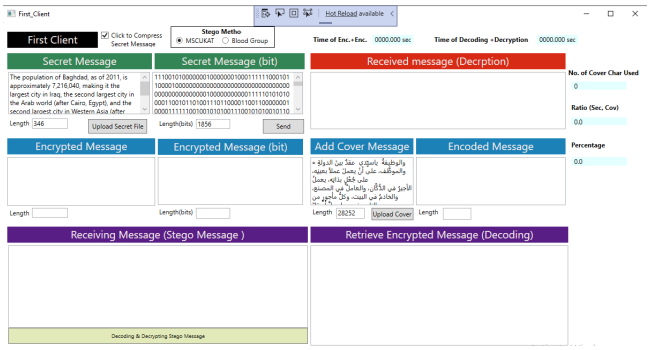
3.2 EVALUATION There were two equations, which had been used in the proposed method [22]:

1. **Cover Percentage Capacity (PC):** It is used to calculate the percentage of cover media. *P.C=Real used of cover/Length of cover *100*
2. **Ratio(secret/cover):** It is useful to be aware of the ratio between the total number of hidden bits that need to hide within the number of characters of the cover media which are sufficient to conceal such hidden bits.
   *Ratio (secret/cover) =Real used of cover*8/hidden bits.*

4. Outcomes and Discussion In this section, we will introduce our experiment details and results. The program is written in C#. and test on one PC a simulate both sides of client and server. Figure 6 demonstrates GUI of client A, B and server.
From figure 6 (A), the server window shows the key input and generated key. The AES algorithm contains encryption of Initialization Vector along with a crypto key for ciphertext generation, where the common key is the secret key that taken from database (in proposed model we use manual mode to made common key input by user) and the IV is generated randomly. The "Generate Key" button is used to produce the public key of both clients (Client A and Client B). After generated these keys it can run bot clients chat windows to start real time Text chatting. In text chatting windows (figure 6 (B,C) and figure 6 (D,E)) the overall encryption/encoding and decoding/decryption results included input of secret messages selection of stego method, selection compressing option, writing, or adding cover message showing the received stego message, retrieve encrypted message after decoding, retrieve original secret message, overall processing time for both encryption/encoding and decoding/decryption processes and shows the number of character needed from cover message, ratio of secret message to cover message and percentage.



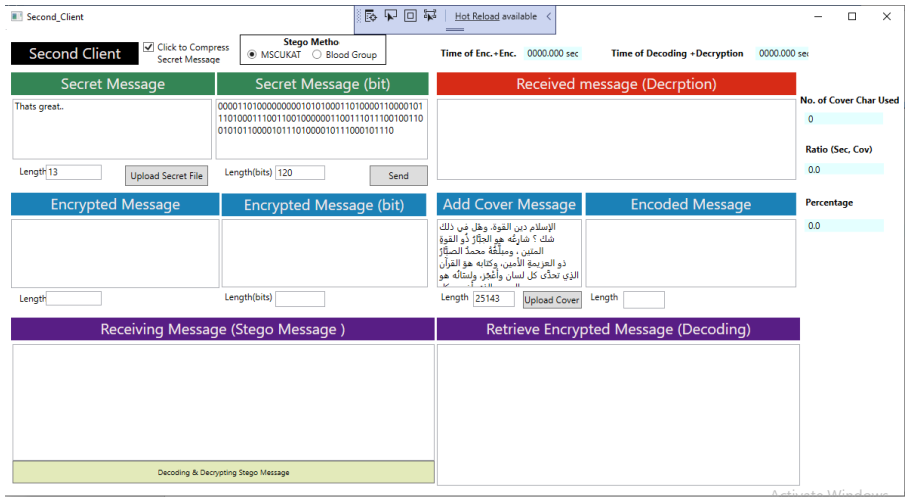
(A)



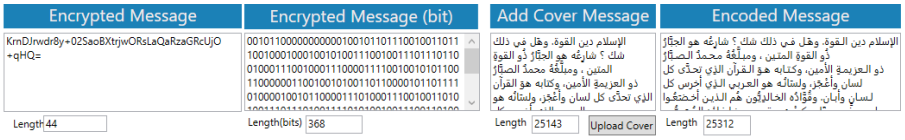
(B)

(C)

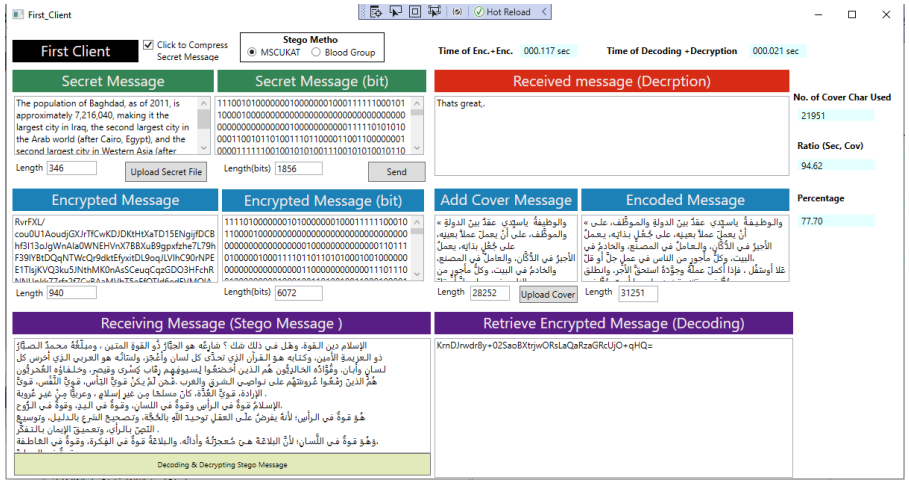
FIGURE 6. The system GUI. (A) Server side (Common key and public key), (B,C) Client A GUI, (D,E) Client B GUI,(F,G)After recieving Message from client A&B.



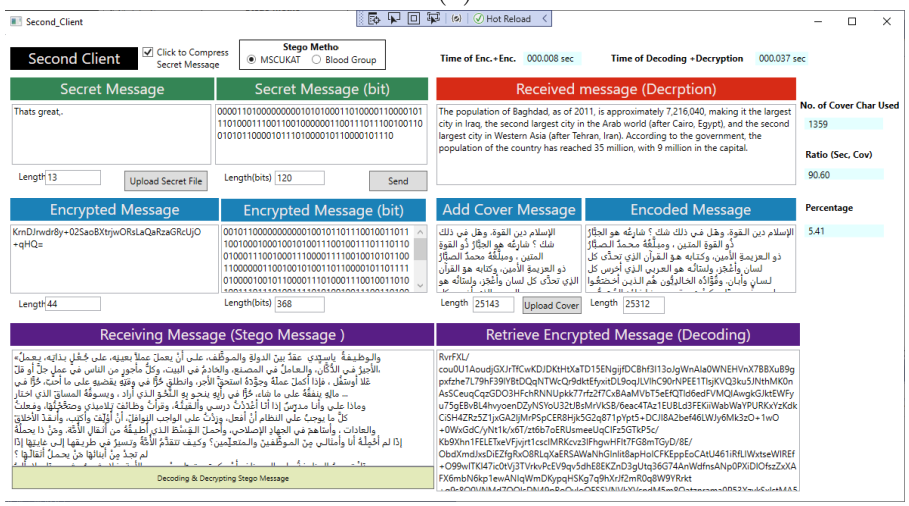
(D)



(E)



(F)



(G)

FIGURE 6. The system GUI. (A) Server side (Common key and public key), (B,C) Client A GUI, (D,E) Client B GUI,(F,G)After recieving Message from client A&B.

In our test we study 4 cases contains 4 lengths of secret message for both clients for different languages. Table 1 shows the covers information the secret messages.

Table 1. The information of covers and secret messages.

Cases for sending and receiving message	Length of Secret Message for (first client)	Length of Secret Message for (second client)	Language (First client to second client)
Case1	346	13	Eng.-Eng.
Case2	1340	23	Arabic-Eng.
Case3	25	2097	Arabic-Arabic
Case4	966	346	Persian-Eng.

The test has completed on both stego model to determine the best stego model in terms of cover capacity and the processing time. Table 2 and table 3 shows the test result for four cases.

Table 2. Test result of MSCUKAT stego method. Involves: overall time for Encoding/Encryption and Decoding/Decryption of secret messages, no. of used char. from cover, Ratio and percentage capacity

Cases		**Time (Encoding /Encrypting)**	**Time (Decoding /Decryption)**	**Used char.**	**Ratio (sec/cov.)**	**Percentage capacity**	**Cover size**
1	**First-client**	0.117	0.021	21951	94.62	77.7	28252
	Sec.-client	0.008	0.037	1359	90.6	5.41	25143
2	**First-client**	0.597	0.021	78968	79.77	42.05	187782
	Sec.-client	0.02	0.187	2036	81.44	8.1	25143
3	**First-client**	0.022	0.219	2760	60	10.98	25143
	Sec.-client	1.181	0.022	120.492	84.79	46.72	257895
4	**First-client**	0.569	0.153	56029	98.12	21.73	257895
	Sec.-client	0.167	0.239	21739	93.7	11.58	187782

Table 3. Test result of BloodGroup stego method. Involves: overall time for Encoding/Encryption and Decoding/Decryption of secret messages, no. of used char. from cover, Ratio and percentage capacity.

Cases		Time (Encoding /Encrypting)	Time (Decoding /Decryption)	Used char.	Ratio (sec/cov.)	Percentage capacity	Cover size
1	First-client	0.187	0.04	24409	105.21	86.4	28252
	Sec.-client	0.079	0.034	1496	115.08	5.94	25143
2	First-client	0.556	0.021	102451	103.49	54.56	187782
	Sec.-client	0.059	0.188	2346	93.84	9.33	25143
3	First-client	0.075	0.253	3197	69.5	12.72	25143
	Sec.-client	0.828	0.025	151693	106.75	58.82	257895
4	First-client	0.687	0.191	70607	123.65	27.38	257895
	Sec.-client	0.481	0.265	28234	121.7	15.04	187782

From table 2 and table 3, the result shows that the system run fast for all cases for both stego method and it in less one minute which is useful for real-time chatting, however, it can observe that the system with MSCUKAT stego method is run relatively fast than the BloodGroup

method. In term of capacity, the result shows that the MSCUKAT is also achieved relatively high capacity than the BloodGroup method. However, BloodGroup achieved accurate result in visibility more than MSCUKAT as described in [20], hence as the processing time and capacity is fairly near to each other, in addition the processing time is fast enough therefore it recommended to use BloodGroup stego method since it is so difficult to detect.
In summary this work achieved the most significant sides that are affect the strength of communication security along with taking the processing time in consideration. For normal text chat operation, we can conclude the point of strength of the proposed system, moreover, it can be compared to last related works described in section 2.(see Table 4)

Table 4. Comparison between the proposal Model with last related works.

Study	Crypto technique	Stego method	Operation	Processing time (Sec)	
				Encry.	Decry.
Proposed Model	Asymmetric+ Symmetric cryptography (Diffe-Hellman +256bit AES)	Arabic Text Steganography (MSCUKAT + BloodGroup)	Realtime (Chatting)	MSCUKAT (0.597)	0.021
				BloodGroup (0.556)	0.021
[20]	Symmetric (HMAC +256bit AES)	Arabic Text Steganography (BloodGroup)	Text File	0.509	Not specified
[19]	(Diffe-Hellman)	No Steganography	Realtime (chatting)	Not specified	Not specified
[18]	(Diffe-Hellman + 128bit AES)	No Steganography	Realtime (chatting)	Not specified	Not specified
[9]	Diffie-Hellman + 256-bit AES	No Steganography	Realtime (chatting)	Not specified	Not specified
[17]	Symmetric (AES)	Hindi Text Steganography (Numbering)	Realtime (chatting)	Not specified	Not specified
[6]	Symmetric (AES or DES)	Arabic Text Steganography	Text File	Not specified	Not specified

5. Conclusion. This paper shows an approach for improving secure communication (such as chatting services) by using cryptography based Diffe-Hellman key exchange and steganography text by utilized a couple of data concealing methods so as to provides more security than individual operation. The cryptography is utilized to encrypt the data were asymmetric cryptography type Diffe-Hellman key exchange-based AES Encryption has been used to encrypts the data in blocks, and the data is embedded in the cover file using steganography text which is the best choice for a chatting application because it does not give any attraction to observer that the message is has no abnormality, in addition it can be coded and decoded in fast so it useful for real time encoding. The cyphertext message generated is then hidden within another text message by used two stego methods, MSCUKAT and BloodGroup. The test result show that this method is run fast in MSCUKAT method, however, the processing time is less one second in both stego methods and for different secret message length so it can serve the practical real time secure chatting application. For capacity, the outcomes show that the MSCUKAT need less cover capacity than the BloodGroup, but it relatively less size in both methods. The system satisfies all requirements of Crypto-Stego technique. The practical result of the proposed crypto-stego system show it works effectively and smoothly in fast time that have no delay in conservation and for both stego methods which can effectively make the

communication secured and the attacker will have a difficult time detecting the hidden message.. And as a consequence this method can be useful to integrated with social media chat application in order to.

6. Future Work A few things could be better and developed. One is to utilize artificial intelligence techniques to select appropriate words from cover text (or dictionary) in such a way that makes the conversation normal and does not cause doubt. The other part is to investigate other crypto and Arabic language text stego methods and other languages to design an integrated system.

References

[1] B. Osman, R. Din, T. Zalizam, T. Muda, MN. Omar, A performance of embedding process for text steganography method, *In 6th WSEAS World Congr. Appl. Comput. Conf. (ACC'13)*, pp.115-119,Nov 17, 2013.

[2] MK. Rahmani, K. Arora, N. Pal, A crypto-steganography: A survey, *International Journal of Advanced Computer Science and Application*; vol.5, pp.149-54, 2014.

[3] Swami U.: Introudction of AES Encyption Algorthim, *https://www.headendinfo.com/aes-encryption/*

[4] Choudary: Steganography Tutorial: A Complete Guide For Beginners, Avalible from: *https://www.edureka.co/blog/steganography-tutorial*.

[5] SS. Tyagi, R.K. Dwivedi, A.K. Saxena, A High-Capacity PDF Text Steganography Technique Based on Hashing Using Quadratic Probing, *International Journal Intelligence Engineering System*, vol.12, no.3, pp.192-202, 2019.

[6] MM. Alkhudaydi, A. Gutub, Securing Data via Cryptography and Arabic Text Steganography, *SN Computer Science*. vol.2, no.1, pp.1-8, 2021.

[7] WW. Arthur, D. Challener, K. Goldman, Basic Security Concepts, *In A Practical Guide to TPM 2.0*, Apress, Berkeley, CA, pp. 7-22, 2015.

[8] H. Van, T. ,S. Jajodia, "Encyclopedia of cryptography and security", *Springer Science & Business Media*, 2014.

[9] YY. Yusfrizal, A. Meizar, H. Kurniawan, F. Agustin, Key management using combination of Diffie–Hellman key exchange with AES encryption, *In 2018 6th International Conference on Cyber and IT Service Management (CITSM) Aug 7*, IEEE. pp. 1-6, 2018.

[10] H. Jeon, SK, Gil, Optical Secret Key Sharing Method Based on Diffie-Hellman Key Exchange Algorithm, *Journal of the Optical Society of Korea (J OPT SOC KOREA)*, vol. 18, No. 5, pp.477-484, 2014.

[11] C. P. Sumathi, T. Santanam , G Umamaheswari, A study of various steganographic techniques used for information hiding, *arXiv preprint*, arXiv:1401.5561, 2014.

[12] TT. Kumar, A. Pareek, J. Kirori, MS. Nehra, Development of Crossover and Encryption Based Text Steganography (CEBTS) Technique, *In Emerging Trends in Computing and Communication Springer*, New Delhi, pp.103-111, 2014.

[13] B. Osman, A. Yasin, MN. Omar, An analysis of alphabet-based techniques in text steganography, *Journal of Telecommunication Electronic and Computer Engineering*, vol.8, no.10, pp.109-15, 2016.

[14] D. Tian, Z. Lu, H. Fan, "A Text Watermarking Algorithm based on Hidden Object", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 10, No. 3, pp. 470-478, September 2019

[15] C. Qin, C. Chang, S. Wang, "A Novel Lossless Steganographic Scheme for Data Hiding in Traditional Chinese Text Files", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 5, No. 3, pp. 534-545, July 2014.

[16] S. Malalla, F.R.Shareef, Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography, *Journal of Engineering Research and Application*, vol.6, no.6, pp.60-9, 2016.

[17] KK. Mandal, S. Chatterjee, A. Chakraborty, S. Mondal, S. Samanta, Applying Encryption Algorithm on Text Steganography Based on Number System, *In Computational Advancement in Communication Circuits and Systems*, Springer, Singapore, pp.255-266, 2020.

[18] SG. Sophia, S. Prabakeran, Efficient and Secure Data Sharing Using AES and Diffie Hellman Key Exchange Algorithm in cloud", *Middle East Journal of Scientific Research 24 (Special Issue on Innovations in Information*, Embedded and Communication Systems, pp.126-131, 2016.

[19] OO. Pal, B. Alam, Diffie-Hellman Key Exchange Protocol with Entities Authentication, *Int J. of Engineering and Computer Science*, vol.6, no.4, 2017.

[20] S. Malalla, F. R. Shareef, A Novel Approach for Arabic Text Steganography Based on the "BloodGroup" Text Hiding Method, *Engineering, Technology & Applied Science Research*, vol.7, no.2 pp. 1482-5, 2017.

[21] S. Malalla, F. R. Shareef, Improving Compression Ratio for Encrypted Secret Message (in AES Encryption) By Using Gzip Compression, *Int. J. of Modern Trends in Engineering and Research (IJMTER)*, vol.3, no.8 pp.182-188, 2016.
[22] F. R. Shareef, A novel crypto technique based on ciphertext shifting, *Egyptian Informatics Journal*, pp.83–90. November 2020.