DOI: https://dx.doi.org/10.21123/bsj.2022.6142

Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel

Mohammed Abdullah Naser *Saif M. Kh. Al-alak* *Ahmed Mohammed Hussein**
Majid Jabbar Jawad

Department of Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq
*Corresponding author: wsci.ahmed.mohammed@uobabylon.edu.iq
E-mail addresses: wsci.mohammed.abud@uobabylon.edu.iq, saif.mahmood@uobabylon.edu.iq , wsci.majid.jabbar@uobabylon.edu.iq

Received 17/3/2021, Accepted 6/10/2021, Published Online First 20/5/2022, Published 1/12/2022

Abstract:

Attacking a transferred data over a network is frequently happened millions time a day. To address this problem, a secure scheme is proposed which is securing a transferred data over a network. The proposed scheme uses two techniques to guarantee a secure transferring for a message. The message is encrypted as a first step, and then it is hided in a video cover. The proposed encrypting technique is RC4 stream cipher algorithm in order to increase the message's confidentiality, as well as improving the least significant bit embedding algorithm (LSB) by adding an additional layer of security. The improvement of the LSB method comes by replacing the adopted sequential selection by a random selection manner of the frames and the pixels with two secret random keys. Therefore, the hidden message remains protected even if the stego-object is hacked because the attacker is unable to know the correct frames and pixels that hold each bit of the secret message in addition to difficulty to successfully rebuild the message. The results refer to that the proposed scheme provides a good performance for evaluation metric that is used in this purpose when compared to a large number of related previous methods.

Keywords: Information Security, Least Significant Bit (LSB), Randomness Public Network Channel, RC4, Video Steganography.

Introduction:

In this era of development technology, the Internet is a most using channel for exchange information over the world. All types of information (audio, video, image, and text) are transferred over Internet.Numerous protocols are developed by researchers and to support the safe transfer of data. The security schemes which are used to provide a safe environment for transferring critical data are classified intocryptography and steganography [1,2]. Encryption changes the data into seemingly meaningless bits, called ciphertext, using a modern and robust algorithm. The targeted person retrieves the original data by a secret key. Other people see an encrypted message as incomprehensible bits, because they are missing a secret key [3]. Steganography has a set of algorithms to hide a transferred message through seemingly harmless carriers to conceal the presence of the data [4,5]. Unlike the other forms of security, the aim of using steganography is to pass a message to the target receiver without any evidence that makes the attacker feel of suspicious message. A steganography scheme tricks the other, where the transmitted message is disappeared inside a cover without any evidence. A good steganography scheme must have perceptual transparency and high data rate. The quality of stego-object is evaluated by its accuracy. A stego-object accuracy is computed by Human Visual System (HVS), which is unable to find minor distortions of stego-object [6,7]. The wide distribution of using video in the internet and social media leads to increase the attention of researchers to secure the transmitted video. Video steganography is important topic in video security field. Most of the currently schemes to achieve video steganography are missing a preprocessing for a transferred message and a cover. [8,9,10]. Furthermore, currently steganography schemes are facing many problems, which are including lack of security, inability to resist attack, less cover capacity for embedded message, and imperceptibility. To override the weakness of cryptography, information hiding techniques are suggested. Combining the two techniques cryptography and steganography can be consolidated to give one more level of insurance. This consolidated approach will fulfill the three objectives of information concealing: security, limit, robustness [11,12].

The proposed work is trying to increase of confidentiality of messages that sent over the Internet or any network system. This is done by mixing cryptography and steganography together, in addition to the principle of randomness in designing all phases of the system. The proposed system contribution includes improving the security of the system.

The structure of the paper is as following: the next section demonstrates a related work. The third section explains the proposed work. The fourth section shows the experimental results. The last section gives conclusions of the work.

Related Works:

Thousands of papers are written which are related to steganography and cryptography. In the following section some of related modern papers are demonstrated.

Reddy V in[13] suggested a system that uses cryptography and steganography to secure a transmitted message. The message is encrypted with ascii code then it is hided in a video cover. Rajalakshmi and Mahesh in [14] used a Patch Wise Code (PWC) in their proposed technique for improving transferred message security. PWC is used to improve security of transferred videos. At the beginning, the system uses Patch Wise Pixel (PWP) grouping for compressing the video to provide a space in a cover video for holding a transferred message. The video is divided into patches. In each patch, the frequent position of pixels is found and the estimated positions of pixel are set then the value of pixel is set. The message hiding process is achieved by using LSB algorithm after completing frames' compression. Gupta et. al. in [15] demonstrated many techniques to embedding a critical information inside a cover video. It is obviously that the communication channels are securing by encryption; however, the data is known after decoding. Steganography is used to hide the existing communications. The critical information is embedded inside data (video, audio, image, and text) of host then it is sent to targeted receiver. Dalal et. al. in [16] demonstrated how a space domain is used for video steganography, and the meaning of stereotypes (invisible communication science). When steganography and encryption are mixed, a security improving for transferred message is achieved. Three characteristics are considered for a good steganography scheme, they are: capacity, imperceptibility, and robustness. Since the video supports mentioned characteristics and it has a big size and complex statistics, then it is considered a good choice for steganography. Rana et. al. in [17] has considered highly secure video steganography on BCD encoding. The message is encoded (using BCD) as a first step before embedding it inside a cover. The hiding process of a message is achieved by using the coefficients of DWT in a frame. The researchers are compared their proposed scheme to LSB insertion scheme. They found that their proposed scheme has better performance in compare to LSB insertion.Patani and Rathod in [18] proposed a scheme that is based on 3-bitLSB to hide image inside a big cover image. The data image is encrypted by ECC algorithm before steganography operation. Rusul et. al. in [19] suggested to use two techniques that is including encryption and concealment for securing a text message. The message is encrypted then hided in a cover image using LSB algorithm. Agarwal et. al. in [20] mixed steganography and cryptography to secure a transferred message. The LSB steganography technique is adopted to hide bits in different channels selected dynamically using key.

The Proposed System:

This work is an attempt to address some security issues related to the text to be hide securely, in addition to improving the method of embedding. The secret message is encrypted by the RC4 (Rivest Cipher 4) as a one of popular stream ciphers, and the most vastly used of all stream ciphers. Also, replace the existing sequential pixel selection in LSB method by randomly selecting of frames/pixels that are controlled by the seed keys using the pseudo-random algorithms. The hidden message remains protected even after the stego has been hacked because attackers still need to know the correct frames/pixels that carry each part of the secret message as well as their arrangement to successfully rebuild the message. It can be divided into many main procedures as follows:

Encryption Phase

In order to increase the security level of the proposed system, RC4 encryption algorithm is used. The proposed algorithm consists of two steps: the key generation and the encryption, where each step (operation) is performed with each new key. The random key generation step is very important, which is performed by the key generator according to a symmetric secret key agreed between the two parties, after which the encryption process is done by the RC4 algorithm. It is worth noting that generating the key used for encryption and decryption involves many steps. The first, it initializes two state values (S1 whose value lies between 0 and 255, S2 which includes a duplicate number from the chosen key) followed by permutations on the value of S1. The second, it is to perform several operations, for example swapping the values of S1 and S2. Then, after the key stream is initialized, the encryption is performed by the XOR bit with a bit of plain text to produce the cryptographic text. Then the encryption text is XOR with the keys flowing to retrieve the plain text through decoding.The process of random key generation and text encryption by RC4 is described in the following algorithm:

Algorithm 1: Encryption Algorithm

```
Input: secret message (plaintext), initial vector,
secret key(k1).
Output: ciphertext.
Begin
Step 1: Convert the secret message to binary format.
Step 2: Create S and T arrays
Step 3: Full S with (0-255) and fill T selected key
Step 4: Perform the initial permutation of S based
on the value of T.
Step 5: Randomize the S value within itself to
generate the key stream.
Step 6: Ciphertext = XORed (secret message, key
stream)
End.
```

Embedding Phase

This phase is implemented from the sender side as shown in the following Fig. 1. The second random key (key2) that is used to select a number of random frames is generated to be used in the embedding process, in addition to generating the third random key (key3) that is used to select a number of random pixels to be used in the same process. It is worth noting that the choice of both keys was based on two random values that are agreed upon between the two parties (sender and recipient); those values are seed 2 and seed 3, in addition to the seed 1 that was adopted in generating the first random key (key1) that was used in encrypting the secret message referred to in section (**Encryption phase**).

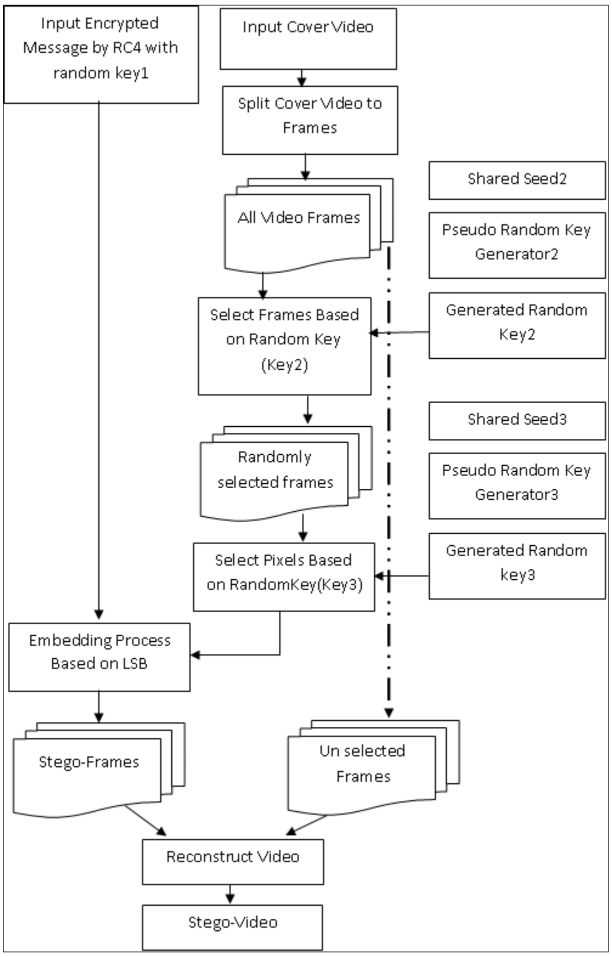

Input Encrypted Message by RC4 with random key1
Input Cover Video
Split Cover Video to Frames
Shared Seed2
All Video Frames
Pseudo Random Key Generator2
Generated Random Key2
Select Frames Based on Random Key (Key2)
Shared Seed3
Randomly selected frames
Pseudo Random Key Generator3
Generated Random key3
Select Pixels Based on RandomKey(Key3)
Embedding Process Based on LSB
Stego-Frames
Un selected Frames
Reconstruct Video
Stego-Video

Figure 1. General block diagram of proposed embedding phase at sender site.

This procedure ensures that the secret message can be recovered during the extraction and decryption processes, through the agreed three symmetric secret keys. Also, this procedure is safer because the message is embedded through the entire frames instead of the left part of the frame, and it is also fast because there is no need to read the entire cover frames, but only the pixels is used in embedding based on the chosen locations. However, at the end of this process, the stgo frames will be combined with the other video frames to create the final output, which is stego-video.

Extracting Phase

At the receiver side, the process of extraction, the method input is stego video, the second and third random keys. Firstly, extract the stego –frame for the video using the second random key to reach the related frames, next use the third random key to extract the embedded bits of the encrypted secret message. Fig. 2 shows the extraction phase in details.

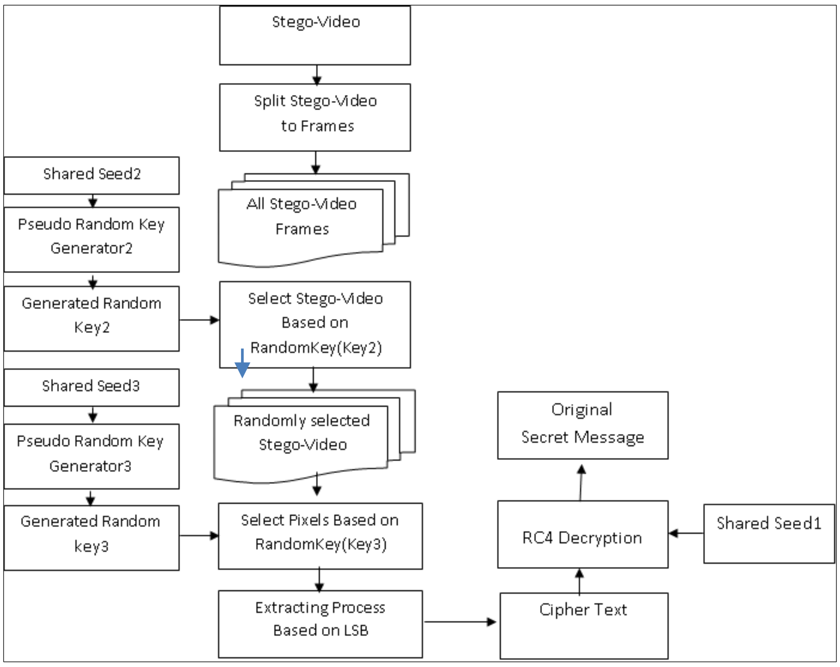

Stego-Video
Split Stego-Video to Frames
All Stego-Video Frames
Shared Seed2
Pseudo Random Key Generator2
Generated Random Key2
Select Stego-Video Based on RandomKey(Key2)
Shared Seed3
Pseudo Random Key Generator3
Generated Random key3
Randomly selected Stego-Video
Select Pixels Based on RandomKey(Key3)
Extracting Process Based on LSB
Cipher Text
RC4 Decryption
Shared Seed1
Original Secret Message

Figure 2. General block diagram of proposed extracting phase at receiver site.

Decryption Phase

After retrieving the encrypted text from the arrived stego video, the decryption process begins with the same symmetric encryption key used in the encryption process through XOR process between them, thus retrieving the original secret text. The algorithm 2 shows the details of the decoding phase:

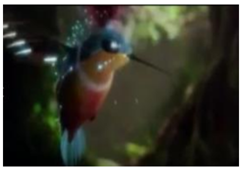
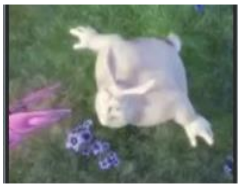
Algorithm 2: Decryption Algorithm

```
Input: ciphertext, initial vector, secret key(k1).
Output: Secret message.
Begin
Step 1: Convert the ciphertext to binary format.
Step 2: Create S and T arrays
Step 3: Full S with (0-255) and fill T selected key
Step 4: Perform the initial permutation of S based on the value of T.
Step 5: Randomize the S value within itself to generate the key stream.
Step 6: Secret message = XORed (Ciphertext, key stream)
End.
```

Results and Discussion:

The work is using pre-posttest experimental design to compute the result of the experiments. The system has been examined with different videos of the same file type (AVI) to test its performance. The names and features of these videos are present in the Table 1 below:

Table 1. Some videos used in the experiments

FileName	First Frame	Number of Frames	Size of Each Frame
Rhino		114	240*320
Boy		53	120*160
Dog		99	240*320
Canary		287	240*180
Bird		137	200*240
Animation		121	400*300

Unfortunately, it is not possible to present all the experiments and results that were performed in the proposed method because it is large and expansive. Therefore, to prove the effectiveness of the embedding process that was implemented by our method, this research lists below the results of the embedding process only in one of the video examples that this research have referred to in Table 1 above (Bird AVI video) in addition to experimenting with many system input values.

Table 2. Embedding process using Bird AVI video for 4 types of secret message selection with random values of Key1 and Key2.

FrameNo.	Cover frame	Key 1	Key 2	Secret message size	Stego frame
F49		81	14	2kb	
F127		52	76	6kb	
F16		43	35	10kb	
F81		20	88	20 kb	

Finally, two performance measurement tools were used: Peak Signal to Noise Ratio (PSNR) and Error Square Error (MSE) to comparing it with the original frame.

Table 3. Values PSNR and MSE for different video and keys values.

Video Name	Key 1	Key 2	Message Size	PSNR	MSE
Rhino	11	90	2kb	64.943	0.02
	45	4	6kb	59.299	0.07
	77	55	10kb	57.131	0.12
	91	78	20kb	53.944	0.26
Canary	55	95	2kb	61.606	0.04
	61	31	6kb	55.943	0.165
	9	13	10kb	53.875	0.266
	11	20	20kb	50.0951	0.318
Bird	81	99	2kb	63.034	0.032
	52	77	6kb	59.809	0.0679
	43	5	10kb	55.234	0.194
	20	37	20kb	52.08	0.4027
Animation	32	10	2kb	65.38	0.018
	27	89	6kb	59.737	0.069
	85	63	10kb	57.605	0.112
	3	44	20kb	54.429	0.234

It is noticed in the Table 2 that the PSNR values decrease, while the MSE values increase as the message size increases. This means that when the message size is large, the frame resolution decreases, and the masking of information causes distortion in the cover frame. Table 3 shows how the values PSNR and MSE reflect the quality of the results that obtained by applying the proposed method on images of different video and keys values with multiple sizes. While Fig.3 and Fig.4 show the relationship between the message size and the PSNR for various AVI videos. Many related work were mentioned in related work section, however; there is not a work that has high similarity to the proposed work to compare its results.

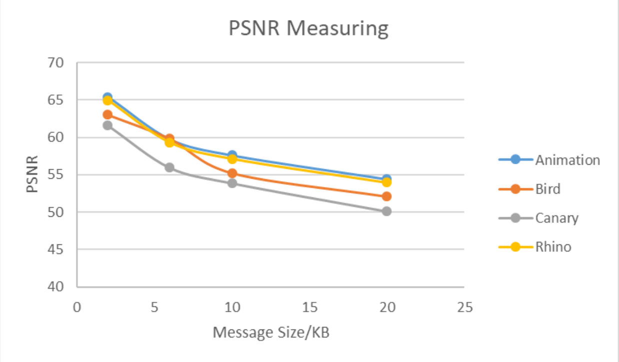


Figure 3. The relationship between message size and PSNR for AVI videos

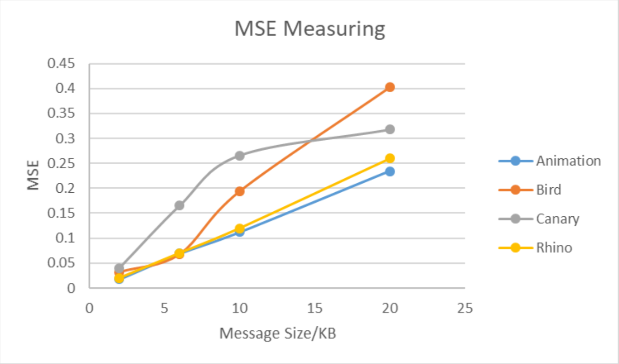


Figure 4. The relationship between message size and MSE for AVI videos

Conclusions:

Security has become a very important issue during the process of transferring information over the Internet, because any unauthorized person can penetrate the data and make it useless or obtain unintended information. The proposed work is intended to develop the steganography technique to obtain a more secure ratio. The suggested approach provides good protection and could protect the message from famous stego attacks. The resolution of the video does not change much and it is almost negligible when this research includes the secret message in it, and the message is protected by the approved encryption algorithm, so the data cannot be destroyed by unauthorized persons. On the other hand, two randomly generated keys were used to randomly select the frame and pixels and use the LSB technology to include secret data, to provide an additional level of protection, so even if the attacker suspects that there is a hidden message inside the video, it is difficult to discover the secret message because of its randomness. Also, the resolution of the video does not change much when the confidential message is included in it, according to what this research observed in the PSNR and MSE values.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Babylon.

Authors' contributions statement:

The authorship of the title above certify that they have participated in different roles as follows:

MA Naser /Suggested the conception and design of work.

SMK Al-alak/Did the analysis and interpretation of result.

AM Hussein/Did the acquisition of data and drafting the MS.

MJ Jawad /Did the revision and proofreading of MS.

References:

1. Easttom C. Modern Cryptography: Applied Mathematics for Encryption and Information Security. New York: McGraw-Hill Education. 1st Ed, Chap16 Steganography; 2015 October: 337-356 P .
2. Pfleeger CP. Security in Computing. Upper Saddle River, NJ 07458: Prentice Hall, Inc. 1st Ed, Introduction Chap1; 1988 Sep 1: 1-34 P.
3. Jeremy Schatten "Using Client-Certificate based authentication with NGINX on Ubuntu - SSLTrust". SSLTrust. Retrieved 13 June 2019. https://www.ssltrust.com.au/help/setup-guides/client-certificate-authentication.
4. Yahya A. Steganography Techniques for Digital Images. Springer International Publishing; Chapter 2 Steganography Techniques; 2019, 1st Ed: 9-42 P.
5. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods Signal Process. 2010 Mar 1;90(3):727-52.

6. Ansari AS, Mohammadi MS, Parvez MT. A comparative study of recent steganography techniques for multiple image formats, Int J Comput Netw Inf Secur.. 2019;11(1):11-25.
7. Abdulmunem IA, Harba ES, Harba HS. Advanced Intelligent Data Hiding Using Video Stego and Convolutional Neural Networks. Baghdad Sci J. 2021;18(4):1317-.
8. Mstafa RJ. Efficient and Robust Video Steganography Algorithms for Secure Data Communication, , Doctoral Dissertation. The School of Engineering, University of Bridgeport. 2017 June: 1-123P
9. Dalal M, Juneja M. Evaluation of orthogonal and biorthogonal wavelets for video steganography. Inf. Secur. J.: A Global Perspective. 2020 Jan 2;29(1):40-50.
10. Alia MA, Maria KA, Alsarayreh MA, Maria EA, Almanasra S. An improved video steganography: using random key-dependent. In 2019 IEEE Jordan International Joint Conference on JEEIT 2019 Apr 9 (pp. 234-237). IEEE.
11. Cao M, Tian L, Li C. A secure video steganography based on the intra-prediction mode (IPM) for H264. Sensors. 2020 Jan;20(18):5242
12. Sadek MM, Khalifa AS, Mostafa MG. Robust video steganography algorithm using adaptive skin-tone detection. Multimed. Tools Appl. 2017 Jan 1;76(2):3065-85.
13. Reddy V. Improved Secure Data Transfer Using Video Steganographic Technique. IJRSDA. 2017;4(3):55-70.
14. Rajalakshmi K, Mahesh K. Video steganography based on embedding the video using PCF technique. In 2017 International Conference on ICICES 2017 Feb 23 : 1-4. IEEE. doi: 10.1109/ICICES.2017.8070726.
15. Gupta H, Gupta R, Sharma B, Gandotra S. Review On Various Techniques Of Video Steganography. IJSTA. 2018;4(1):161-4.
16. Alwan IM. Image Steganography by Using Multiwavelet Transform. Baghdad Sci. J. 2014;11(2):275-83.
17. Rana S, Bhogal RK. A highly secure video steganography inside dwt domain hinged on bcd codes. In Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices. ADV INTELL SYST (624) 2018 : 719-729. Springer, Singapore. https://doi.org/10.1007/978-981-10-5903-2_74
18. Khan S, Bianchi T. Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region. Int. J. Electr. Comput. Eng. 2018 Feb 1;8(1):2088-8708.
19. Neamah RM, Abed JA, Abbood EA. Hide text depending on the three channels of pixels in color images using the modified LSB algorithm. Int J Electr Comput Eng. 2020 Feb 1;10(1):809.
20. Salim KG, Al-alak SM, Jawad MJ. Improved Image Security in Internet of Thing (IOT) Using Multiple Key AES. Baghdad Sci. J. 2021;18(2):0417-.

تقنيات إخفاء وتشفير المعلومات لنقلها بشكل آمن عبر قناة الشبكة العامة

محمد عبد الله ناصر سيف محمود خلف العلاق احمد محمد حسين ماجد جبار جواد

قسم علوم الحاسوب، كلية العلوم للبنات، جامعة بابل، بابل، العراق.

الخلاصة:

من المعلوم انه غالبا ما يتم مهاجمة البيانات المنقولة عبر شبكة الانترنيت ملايين المرات في اليوم الواحد. ولمعالجة هذه المشكلة، تم اقتراح طريقة آمنة تقوم بتأمين البيانات المنقولة عبر الشبكة. الطريقة المقترحة تعتمد تقنيتين لضمان النقل الآمن للرسالة المنقولة. اذ يتم تشفير الرسالة كخطوة أولى، ثم يتم إخفاؤها في غلاف فيديو معين. تقنية التشفير المقترحة هي خوارزمية تشفير انسيابية (RC4) لزيادة سرية الرسالة، وكذلك تحسين خوارزمية تضمين البتات الأقل أهمية (LSB) لتوفير مستوى أمان إضافي. يأتي تحسين طريقة الـ LSB التقليدية من خلال استبدال الاختيار المتسلسل المعتمد سابقا في طريقة الاختيار العشوائي لكل من الإطارات والبكسل من خلال استخدام مفتاحين عشوائيين سريين على التوالي. لذا، تبقى الرسالة المخفية محمية حتى إن تم اختراق الكائن المخفي(stego) لأن المهاجم سيكون غير قادر على معرفة الإطارات والبكسلات الحقيقية التي تتضمن كل جزء من أجزاء الرسالة السرية بالإضافة إلى صعوبة إعادة بناء الرسالة بشكل صحيح. النتائج المتحصلة من البحث تشير إلى أن الطريقة المقترحة توفّر أداءً جيدًا وفقا لمقاييس التقييم المعتمدة عند مقارنتها بعدد كبير من الطرق السابقة ذات الصلة بهذا النوع من الاعمال.

الكلمات المفتاحية: أمن المعلومات، البت الأقل أهمية (LSB)، العشوائية في قناة الشبكة العامة ، RC4، إخفاء المعلومات بالفيديو.