Iraqi Journal of Science, 2021, Vol. 62, No. 9, pp: 3243-3254
DOI: 10.24996/ijs.2021.62.9.37

ISSN: 0067-2904

A Proposed Algorithm for Encrypted Data Hiding in Video Stream Based on Frame Random Distribution

Sura Abed Sarab Hussien[1*], Thair Abed Sarab Hussien[2], Mustafa Abdulsatar Noori[2]
[1]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq
[2]Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq

Received: 1/5/2021 Accepted: 6/6/2021

Abstract

The science of information security has become a concern of many researchers, whose efforts are trying to come up with solutions and technologies that ensure the transfer of information in a more secure manner through the network, especially the Internet, without any penetration of that information, given the risk of digital data being sent between the two parties through an insecure channel. This paper includes two data protection techniques. The first technique is cryptography by using Menezes Vanstone elliptic curve ciphering system, which depends on public key technologies. Then, the encoded data is randomly included in the frame, depending on the seed used. The experimental results, using a PSNR within average of 65 and MSE within average of 85, indicate that the proposed method has proven successful in its ability to efficiently embedding data.

Keywords: Menezes -Vanstone Elliptic Curve, video Steganography, Encryption data, Seed, LSB.

خوارزمية مقترحة لإخفاء البيانات المشفرة في دفق الفيديو بناءً على التوزيع العشوائي للإطار

سرى عبيد سراب حسين[1]، ثائر عبيد سراب حسين[2]، مصطفى عبد الستار نوري[2]
[1]قسم علوم الحاسب, كلية العلوم, جامعة بغداد, بغداد, العراق
[2]كلية الهندسة الكهربائية التقنية, الجلمعة التقنية الوسطى، , بغداد, العراق

الخلاصه

أصبح علم أمن المعلومات مصدر قلق لكثير من الباحثين الذين تحاول جهودهم التوصل إلى حلول وتقنيات تضمن نقل المعلومات بطريقة أكثر أمانًا عبر الشبكة ، وخاصة الإنترنت ، دون أي اختراق لتلك المعلومات و نظرا لأهمية البيانات الرقمية المرسلة بين الطرفين عبر قناة غير آمنة .تتضمن هذه الورقة تقنيتين لحماية البيانات ، التشفير باستخدام نظام تشفير المنحنى الاهليجي Menezes Vanstone يعتمد على تقنيات المفتاح العام .ثم يتم تضمين البيانات المشفرة بشكل عشوائي في الإطار ، اعتمادًا على البذور المستخدمة .تشير النتائج التجريبية باستخدام مقياس PSNR ضمن معدل 65 و MSE ضمن معدل 85 إلى أن الطريقة المقترحة أثبتت نجاحها في قدرتها على تضمين البيانات بكفاءة.

1. Introduction

Since the year 2000, data and information began to increase due to the emergence of many applications and multimedia that represent different sources such as social media, webcams and videos. Therefore, it is necessary to provide security for that data in an integrated manner, and this is considered one of the difficult problems [1]. In addition, since the process of transferring data became

*Email: suraaljanaby8484@gmail.com

easy and fast using the Internet in addition to the widespread use of social media technologies and means, many problems related to data emerged, especially with regard to the security threat, such as stealing confidential data, modifying and deleting it, and many other problems [2].

Therefore, the topic of data confidentiality has taken a wide area in the work of researchers, because it is the main factor that needs attention during the process of data transmission, in addition to the huge increase in the rate of data transmission of various types. Unfortunately, many of the algorithms that are used to maintain security suffer from significant vulnerability in many aspects, including security, limited capacity, lack of clarity, and the ability against a large number of attacks [3].

Secret information should be well secured in order to transfer it; therefore, information security became very important factor to complete the transfer successfully without hacking it. There are many techniques used for this purpose such as Cryptography, Information hiding (Steganography and digital watermarking) to improve the security features in information transfers over the internet [2, 3].

Cryptography is the analysis of mathematical methods to conceal knowledge. The main objective of cryptography is to assist two participants, or more, who use a relatively an unreliable channel so that what is being told could not be known and/or exploited by an attacker. This channel might be a line telephone, computer system, or wireless gateway. Based on the existence of the keys utilized, cryptographic methods could be split into two major groups: asymmetric and symmetric methods [3, 4]. Steganography is a method of embedding secret details in such a manner that no one recognizes the presence of the letter in the cover file other than the sender and planned receiver [5]. It aims to hide secret information into a digital cover file (image, audio, video, etc.) without being dubious.

The most common means of hiding data are images. They can be treated as a binary matrix with positive and true values in which data can be included and easy to retrieve from them. Color images are usually relied upon because they are a mixture of several colors. The hiding process does not affect them much. Therefore, we use in this research a video that consists of a group of images that can cover more data than a single image [6].

The most common way to encrypt data is the public key, which allows two parties to encrypt with public keys and decrypt with private key of each party without being identified by others. Elliptic curves are one of the types of public key-dependent encryption. It was first applied in 1985. In Elliptic-curve cryptography (ECC), 160-bit keys are provided, which reduces the computational cost of the coding process, especially if the data is very long, and also reduces processing time. This paper deals with encoding data using ECC as a new method for generating public and private keys, as each sender is allowed to produce his/her own private key without sharing it through internet channels that do not have security [7]. The research includes several parts. The first part deals with previous works within the field of our research. As for the second part, it describes the topics covered by the research and the proposed method, followed by the results and discussion.

2. Related works

This section reviews in brief some of the previously proposed methods related video Steganography.

Aagarsana *et al*. [8] provided a combined method between hiding and encryption at the same time. They encoded the audio signal using AES algorithm and then it was hidden in color image using circular LSB algorithm.

Singh *et al*. [9] proposed a robust video steganography based on frequency domain. The embedding position is the redundant coefficient. The authors applied DWT on the video file. Then, using LSB process, the hidden data was embedded in the lowest plane. In this approach, to increase the robustness of the design, redundancy is used. In addition, the key used to improve the embedding and extraction operations is also used to increase the layer of the security.

Saurabh *et al*. [10] introduced a method for hiding the image within the video using the LSB algorithm, for each pixel in the video frames includes in the odd frames. They used this technique as a safe hiding method because it is difficult to analyze multiple frames for a video, especially as the video size increases.

Kelash *et al*. [11] provided a method for hiding the image within the video. They divided each pixel inside the frames into two parts. The number of bits which will be embedded in the right part are counted in the left part of the pixel. It involves hiding a large amount of data where the hiding was random.

3. Methodology

The proposed method includes two parts, which are encrypting confidential data to increase its security and hiding the data after encrypting it inside a video.

3.1 Elliptic Curves Cryptosystem

Elliptic curves have been studied by a number theorists for about a century, not for applications in mathematics or computing science, but because of their intrinsic mathematical beauty and interest [12, 13].

An elliptic curve over a prime field is defined by

$$E_p(a,b): y^2 = x^3 + ax + b \bmod p$$

Where the elliptic curve group consists of all points that satisfy the elliptic curve [7].

Elliptic Curve Addition Operation over Fp Given two points $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ on E, with x_1, x_2, y_1 and y_2 in Fp.The addition low $Q_3 = (x_3, y_3) = Q_1 + Q_2$ is:

$x_3 \equiv (\lambda^2 - x_1 - x_2)\ modp,$

$y_3 \equiv (\lambda(x_1 - x_3) - y_1) modp$

Where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad Q_1 \neq Q_2 \\ \frac{3{x_1}^2 + a}{2y_1} & \text{if} \quad Q_1 = Q_2 \end{cases}$$

EXAMPLE

Consider an elliptic curve over the field with and , the elliptic curve equation is . Then the points that satisfy this elliptic curve equations are:

(0,11), (0,18), (1,3), (1,26), (4,9), (4,20), (5,0), (6,6), (6,23), (9,6), (9,23), (10,7), (10,22), (11,8), (11,21), (12,0), (14,6), (14,23), (18,2), (18,27), (21,7), (21,22), (25,4), (25,25), (27,7), (27,22), (28,1), (28,28). Then the is 29 points, these points may be illustrated graphically as show in Figure-1.

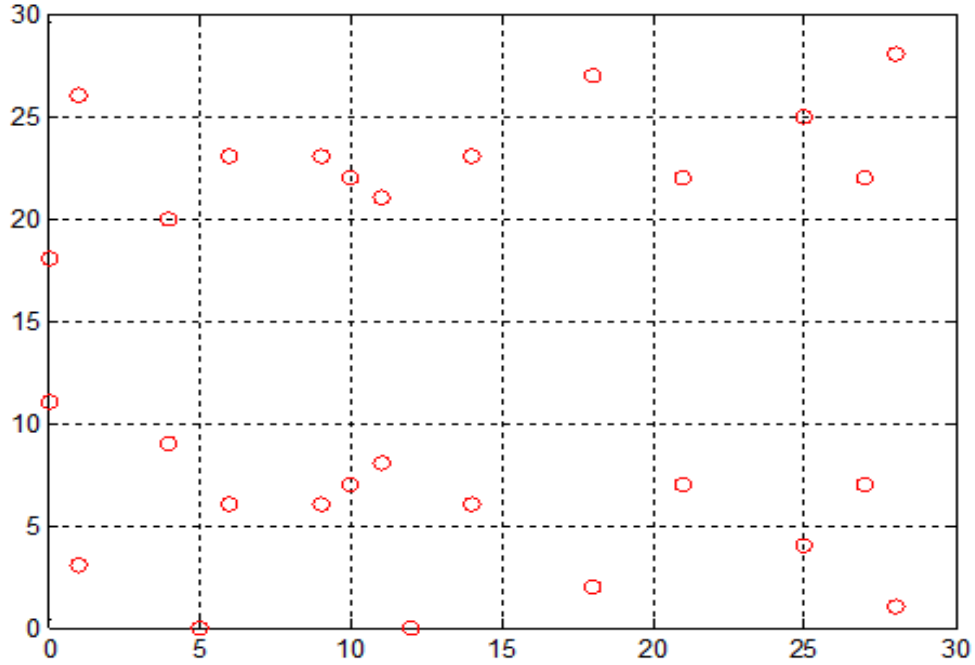

Figure 1- Elliptic curve over .

3.2 Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

MVECC system introduced by Menezes and Vanstone in 1993. Actually it has no analogue for ECDLP, this means that it does not depend on discrete logarithm problem like ElGamal cryptosystems. Therefore, sender does not need to embed the plaintext on the EC but only mask it. In MVECC no needs for mapping but only replacing each character with an ordered pair that is not required to be a point on an EC and this makes MVECC more efficient than ElGamal technique [14, 15].

where this type of encryption algorithm does not depend on the difficulty of solving the ECDLP. According to our encoding method, first the data is divided into blocks containing only two numbers, these two numbers allow us to express the message as a point. Thus, it is not necessary to send the knowledge of each character's point to the recipient [16].

Algorithm MVECC for audio and image

Input: Plain Text
Output: ***Cipher audio and image***
Begin:
1. If Bob wants to encrypt and send a message to Alice, then they do the following setup:
2. Bob and Alice agree upon an elliptic curve and a base point .
3. Alice first selects a private key and generates a public key.
4. Bob wishes to encrypt and send a message to Alice, he chooses a random positive integer and produces the cipher (*audio and image)* send it to Alice, where and:

$c_i = m_i \cdot k_i mod\ p$,

$c_{i+1} = m_{i+1} \cdot k_{i+1} mod\ p$,

$$eQ = (k_i,\ k_{i+1})$$

Where *i=1,* *2…,* *n.*

5. When Alice likes to decrypt the cipher data, she computes the following:

$m_i = c_i \cdot k_i^{-1}\ mod\ p$,

$$m_{i+1} = c_{i+1} \cdot k_{i+1}^{-1}\ mod\ p$$

End

• **Example:** Let be an EC define over with parameters, where and. If Alice wants to send any message (image, sound, text) to Bob using the algorithm of the proposed algorithm, they have to implement the following steps:
• Since is prime number then, every point on is base point. So, if we choose, the domain parameters for are{12,23,331, (1,6)}
• Bob first selects a private key and generates a public key.
• If Alice wishes to encrypt (247, 247, 248, 248) and send to Bob, she chooses random positive integer and produces the cipher image.
• She computes:

$$eB = (281,62)$$
$$eQ = (38,111) = (k_1, k_2)$$

Then she computes:

$c_1 = p_1 * k_1 mod\ p = 247 * 38\ \ mod\ 331 = 118$
$c_2 = p_2 * k_1 mod\ p = 247 * 111\ mod\ 331 = 275$
$c_3 = p_3 * k_1 mod\ p = 248 * 38\ \ mod\ 331 = 165$
$c_4 = p_4 * k_1 mod\ p\ = 248 * 111\ mod\ 331 = 55$

• She sends it to Bob.

1. If Bob would like to decrypt the ciphered data, he computes the following:

$$(k_1, k_2) = e(dB) = (38,111)$$
$$k_1^{-1} = 38^{-1} mod\ 331 = 61$$
$$k_2^{-1} = 111^{-1} mod\ 331 = 167$$

Then

$p_1 = c_1 * k_1^{-1} mod\ p\ = 118 * 61\ mod\ 331 = 247$
$p_2\ = c_2 * k_2^{-1} mod\ p = 275 * 167\ mod\ 331 = 247$
$p_3\ = c_3 * k_1^{-1} mod\ p = 156 * 61\ \ mod\ 331 = 248$
$p_4\ = c_4 * k_2^{-1} mod\ p = 55\ \ * 167\ mod\ 331 = 248$

• **3.3 Embedding Secret Data Encrypted**

After the data sent is encrypted using the above algorithm, it is included within the video frames non-sequentially depending on the seed and according to the following algorithm:

• **Embedding Process**: This stage includes the process of embedding encoded data into a video consisting of the following steps:

Algorithm hiding Data.
Input: Video and Encryption data **Output: Embedding data and product steno video.** **Begin** **Step One:** Read video and Encryption data. **Step Two:** Convert the encrypted data to binary with bit test**.** **Step Three:** Calculate the total number of bits of the message resulting from the previous step. **Step Four:** Calculate the number frames in video. **Step Five:** The third step compared with the fourth step. If the third step is more, then not hidden. **Step Six:** If the fourth step is more, the (image, or audio) will be hidden inside the video. **Step Seven:** If the seed (According to the agreement between the sender and the recipient, it can be a date, name, symbols and random numbers. Here the date of transmission was used day, month and year) value is odd, it will be hidden in odd pixel, not even, and vice versa. **Step Eight:** If the seed values are within the sequence of frames, we will include them in that frame, and if they are not within the sequence, we will make a mode for the value, Hide is done on odd sites only and from bottom to top. **Step Nine:** Performance of the PSNR and MSE and UACI measure between the original and the original frame after hidden. **End**

• **Extracting Secret Data Process**

The steps below include a mechanism to extract the encrypted data from the hiding video:

Step 1: Choosing the hidden video. Step 2: divide the video into many frames. Step 3: Choosing the hidden frame with same embedding way. Step 4: Extracting the encrypted data from the selected hidden frame.

The Figures-2 and 3 illustrate the work of the proposed method. The Figure-2 shows the process of hiding the encrypted image within the video, as well as the Figure-3 demonstrates the process of extracting the image from the video for the recipient. The Figures-4 and 5 shows the work of the proposed method, but for the audio as well, the Figure-4 shows the hiding process and the Figure-5 shows the extraction process.

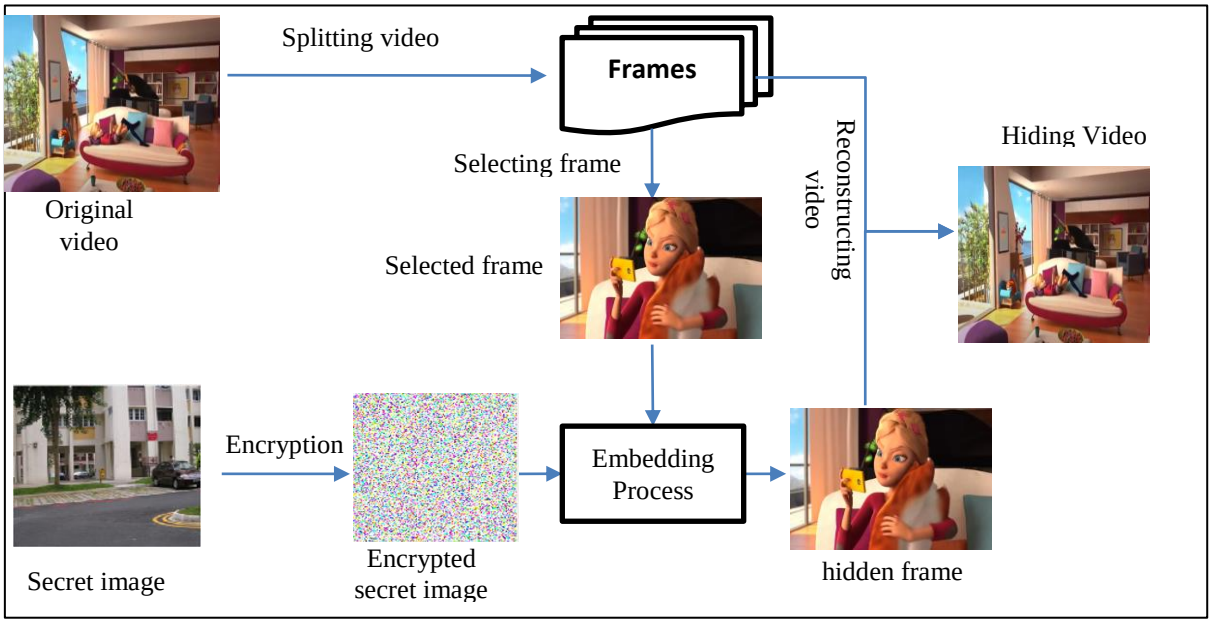

Figure 2- Explain the process of hiding an encrypted image inside the video.

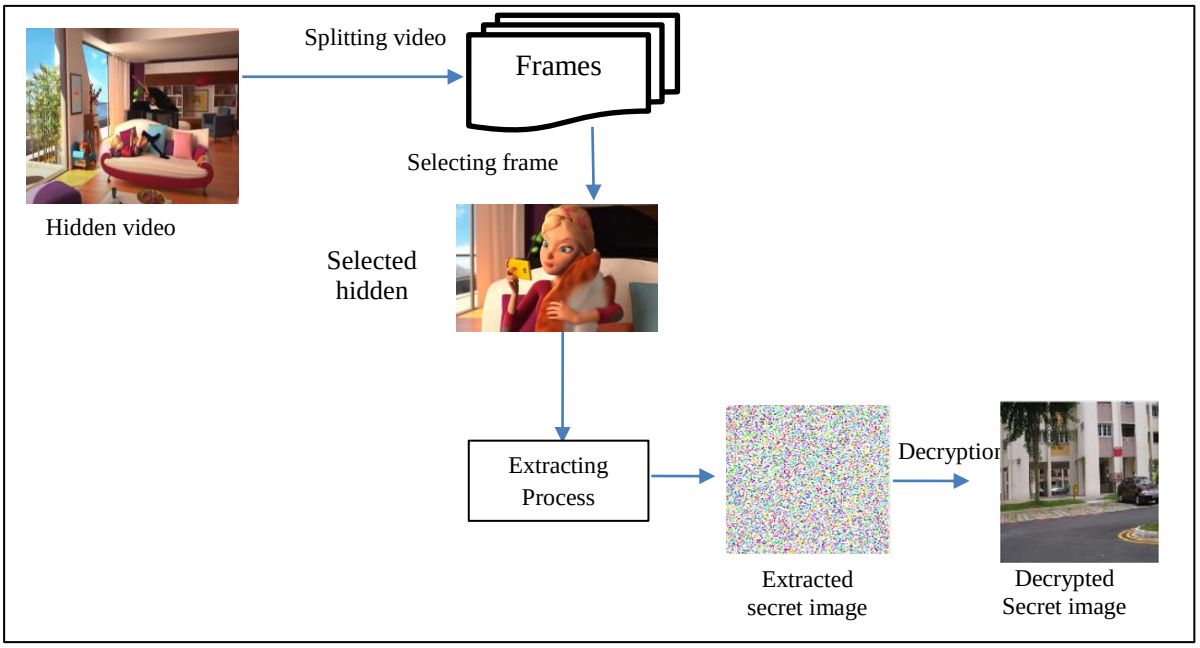

Figure 3- Explain the process of extraction an encrypted image from the video.

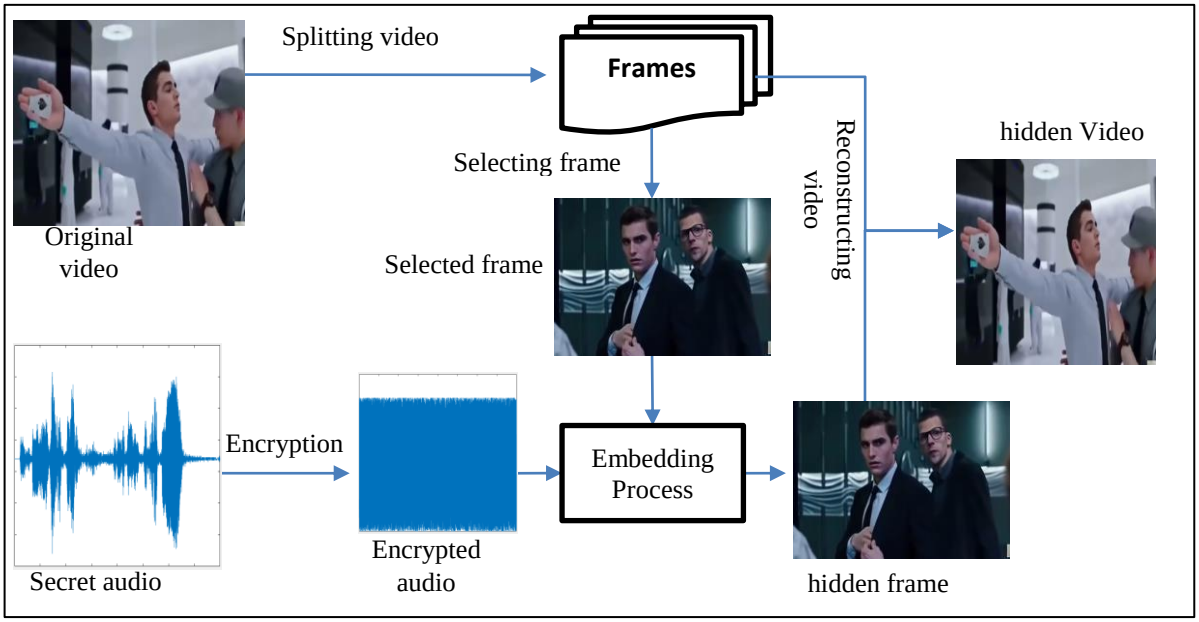

Figure 4-Explain the process of hiding an encrypted audio from the video.

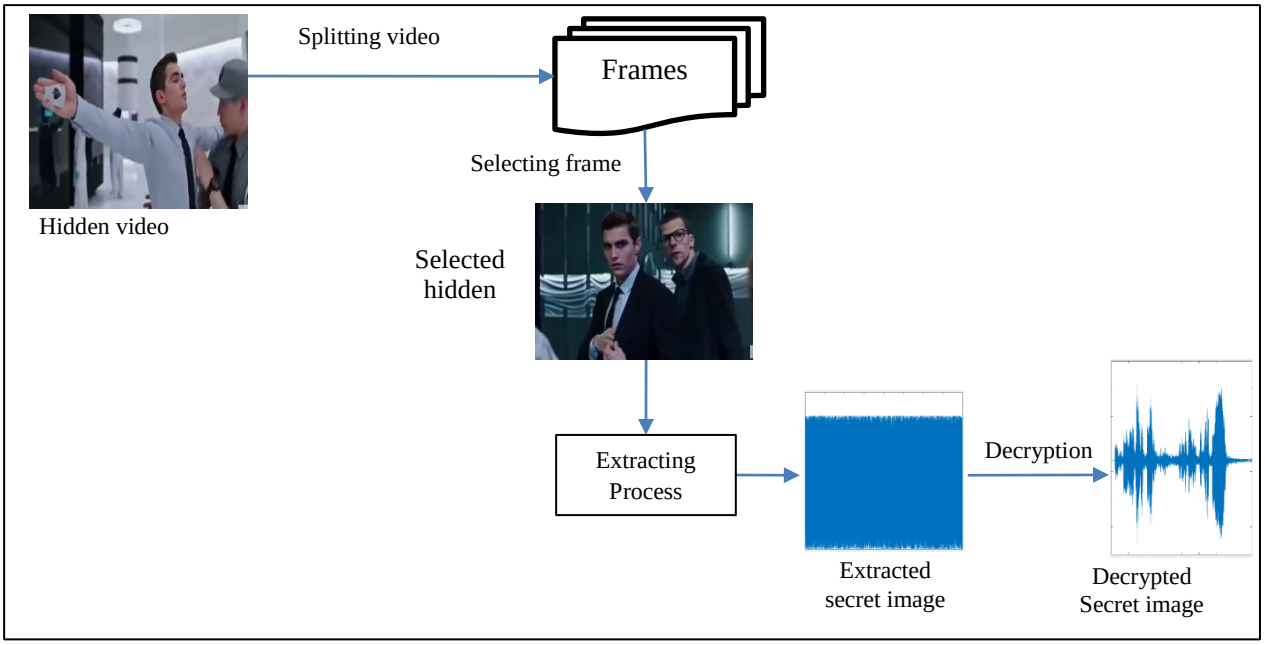

Figure 5- Explain the process of extraction an encrypted audio from the video.

3.4 Performance evaluation

Through the performance measures, we notice the amount of change in the hand of the original video and the video after hiding, so here we use two measures:

1. Mean Square Error (MSE): The average of the squares of the "errors" measured by the mean squared error of an estimator i.e. the difference between the estimator and what estimated. The contrast happens due to randomness or because of the estimator does not calculate information that could result in a better accurate estimate. The PSNR differ inversely with the MSE. The MSE can be found from the following [17, 18]:

$$MSE = \frac{1}{N * M}\sum_{i=1}^{n}\sum_{j=1}^{m}(Origin\_frame\ (i,j) - Ste\_frame(i,j))^2$$

2. Peak signal to noise ratio: The ratio between the power of corrupting noise and the most possible power of a signal that influences the sincerity of its representation is PSNR [19]:

$$PSNR = 10log_{10}(\frac{maxi}{\sqrt{MSE}})$$

3. Unified average changing intensity (UACI)

It is one of the measures used to measure the strength of a coding. It is based on a comparison between the encrypted data and the original data. The lower the value of this scale, the stronger the encryption and the image deterioration, the more it cannot be easily recovered [20].

$$UACI = \frac{1}{n * m}\sum_{i=1}^{n}\sum_{j=1}^{m}(x(i,j) - y(i,j))\Big/_{255} * 100\%$$

Where represents origin image and represent encrypted image, n and m rows, columns of image.

4. Result and Discussion

This part includes several axes, embedding the encryption and concealment mechanism and their results. In addition, metrics are used to measure the efficiency of the proposed method. In this paper, we used two types of data, image and audio, as the transmitted data are varied.

The Figures-6 and 7 below illustrate the encryption process for image and sound using the proposed algorithm:

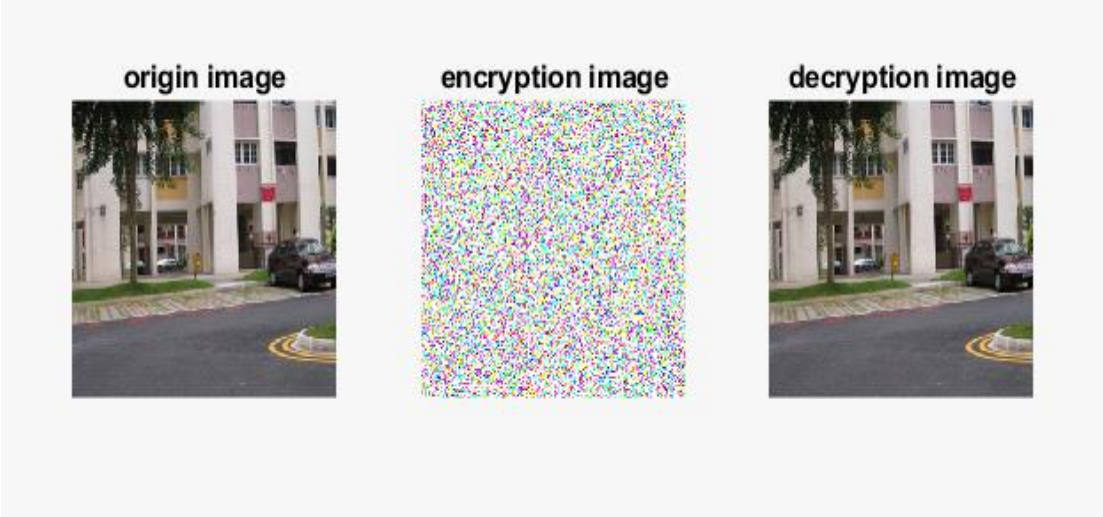

Figure 6- Explain origin image and encrypted image.

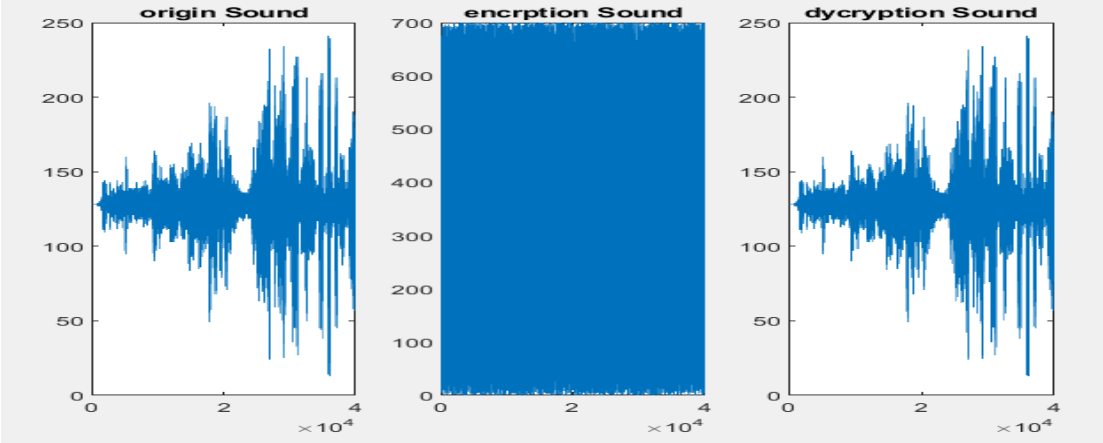

Figure 7- Explain Origin sound and encrypted sound.

Video1 **Video2**

Figure 8- Video frames to hide the data.

1. To illustrate the embedding process, which consists of an image with a size of 200 * 220 and videos of different frame size, as shown in the table, the image is first encoded using the MVECC algorithm.
2. A random seed is chosen (words, letters, numbers, symbols, anything else) agreed upon by the sender and the receiver, which is the basis for choosing the inclusion frames.

3. The seed is converted into numbers, and then every number in the seed is tested if it represents one of the frames, then it is hidden in that frame with a sequence similar to the seed number, and if it is not the same, then a mode of the value is made to be within the number of frames.
4. Not all pixels of the frame are included, but rather only at the odd locations of each pixel, starting from the bottom up, so that it is difficult to identify which pixels contain the data.
5. After that, efficiency measures are applied between the frame in which it was included and the original frame to see the extent of the difference between them.

Table 1-Values of PSNR and MSE for hidden video

Name of Video	Secret Data	MSE	PSNR	Size of Frame	Time\min	UACI
Video1	**Image**	**95**	**65.2865**	**400×550**	**3**	**30.55**
Video1	**Audio**	**75**	**67.6504**	**400×550**	**1.5**	**/**
Video2	**Image**	**100**	**64.7736**	**360×640**	**2.5**	**32.112**
Video2	**Audio**	**110**	**63.8205**	**360×640**	**2**	**/**

The above table shows the results of the embedding in the video. Note the overall average for the MSR is between 70 and 100, while the PSNR scale ranges between 60 for all the frames that were included in it.
The PSNR value is calculated for each frame separately, then the values are combined and divided by the number of frames that have been hidden in order to have one result for these measures.

5. Conclusion

In this paper, a method proposed that uses encryption and steganography techniques to provide greater protection for data sent over insecure channels. The encryption method based on MVECC gave good results, Through the results of the UACI scale computes the number of averaged changed intensity between ciphertext images, which was used to measure the strength of a encryption, where results were below 50, which increased the strength of the encryption, as unauthorized people could not know the key without knowing the random seeds that generated using this algorithm. The embedding of even and single-layer frames also makes the video look natural and uninterrupted. The experimental results of this method showed that the inclusion was of high quality and the metric values were close to the ideal value. This indicates that this method fulfills the lack of feeling of the inclusion in the video.

Reference

1. N. Ali & R. Abdul-Sattar **2017**. Data integrity enhancement for the encryption of color images based on CRC64 technique using multiple look-up tables. *Iraqi Journal of Science*, **58**(3C).
2. O. N. Kadhim. **2018**. "A Chaos-Based Steganographic Approach for Information Hiding," Master, Faculty of Computer Science and Mathematics / University of Kufa.
3. W. Stallings. **2014**. *Cryptography and Network Security: Principles and Practice*, International Edition. Principles and Practice.
4. S. Pal and S. K. Bandyopadhyay. **2016**. "Various Methods of Video Steganography," *International Journal of Information Research and Review*, **3**(6): 2569-2573.
5. W. Luo, F. Huang, and J. Huang. **2010**."Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*, **5**(2): 2201-214.
6. N. H. Ali, A. M. Rahma, & A. S. Jamil. **2015**. Text Hiding in Color Images Using the Secret Key Transformation Function in GF (2 n). *Iraqi Journal of Science*, **56**(4B): 3240-3245.
7. Silverman, J. H. **2009**."*The Arithmetic of Elliptic Curves: Graduate Texts in Mathematics 106*" 2nd ed., New York, Springer.
8. Aagarsana, B. G., Anjali, T. K., & Kirthika, M. S. S. **2018**. Image Steganography using secured force algorithm for hiding audio signal into colour image. *IRJET access*, *5*.
9. M. Bilal , S. Imtiaz , W. Abdul , S. Ghouzali , and S. Asif. **2014**. "Chaos based Zero-steganography algorithm," *Multimedia tools and applications*, **72**(2): 1073-1092.
10. Singh, S., & Agarwal, G. 2010. Hiding image to video: A new approach of LSB replacement. *International Journal of Engineering Science and Technology*, **2**(12): 6999-7003.

11. Kelash, H. M., Wahab, O. F. A., Elshakankiry, O. A., & El-sayed, H. S. **2013**.. Hiding data in video sequences using steganography algorithms. In *2013 International Conference on ICT Convergence (ICTC)* (pp. 353-358). IEEE.
12. Abdullah, K. E., & Ali, N. H. M. **2018**. Security improvement in elliptic curve cryptography. *Int. J. Adv. Comput. Sci. Appl*, **9**(5): 122-131.
13. Abdullah, K. E., & Ali, N. H. M. 2018. A Secure Enhancement for Encoding/Decoding data using Elliptic Curve Cryptography. *Iraqi Journal of Science*, 189-198.
14. Menezes, et al. **1993**. "Elliptic curve cryptosystems and their implementation", *Journal of Cryptology*, **6**(4): 209–224.
15. Z. E. Dawahdeh, et al. **2016**. "A new modification for menezes-vanstone elliptic curve cryptosystem" *J. Theor. Appl. Inf. Technol*., **85**(3): 290–297.
16. X. Zhang, X. Wang. **2018**. "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem", *IEEE Access*, **6**: 70025–70034.
17. Rajkumar, S., & Malathi, G. **2016**. A comparative analysis on image quality assessment for real time satellite images. *Indian Journal of Science and Technology, ISSN: 0974-6846,* **9**(34), September 2016. DOI: 10.17485/ijst/2016/v9i34/96766.
18. Ali, N. H. M., & Abead, S. A. **2016**. Modified Blowfish Algorithm for Image Encryption using Multi Keys based on five Sboxes. *Iraqi Journal of Science*, **57**(4C): 2968-2978.
19. Memon, F., Unar, M. A., & Memon, S. **2016**. Image quality assessment for performance evaluation of focus measure operators. *Mehran University Research Journal of Engineering & Technology*, ISSN 0254-7821, **34**(4), October, 2016.
20. Wu, Y., et al. **2011**. "NPCR and UACI randomness tests for image encryption", *Journal of Selected Areas in Telecommunications*, **1**(2): 31–38.