Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 3, August 2020, pp.1741-1751

Robust video data security using hybrid cryptography-steganography technique

Faten H. Mohammed Sediq Al-Kadei

Northern Technical University, Technical Institute

ABSTRACT

The interest in the digital videos confidentiality in the current electronic and interrelated world has increased. Thus, this paper aimed at making a video steganography scheme for an acceptable security with high speed of calculation by embedding data (video frames) in other video frames. The techniques of embedding and encrypting video frames in a cover video file were done through two ways. Firstly, two keys and XOR bit operation were employed to create a large range of different keys for encryption. Secondly, a modified method of Least Significant Bit (LSB) technique was used for hiding high resolution video frames (bitmap color) in selective cover video frames, offering two security layers. The procedures of encrypting and hiding video data were successfully tested on many secret videos such ad Eye Video, Secret Medicine Video and Traffic Video. All experiments were conducted using MATLAB-GUI software, representing an efficient and easy tool for video management supported by powerful testing tools as histograms and mathematics for video quality. Experimental result demonstrated a good performance with low correlation and very high PSNR of the Stego video frames.

Keywords: Video steganography, Data Hiding, Encryption, Frame Extraction, Least Significant Bit Technique, PSNR

Corresponding Author:

Author Name, Faten H. Mohammed Sediq Al-Kade
Departement, Technical Institute
University, Northern Technical University
Address, Kirkuk, Iraq
E-mail: Faten.alqadhi@ntu.edu.iq

1. Introduction

Recently, digital media and data (like voice, text, image, and video) have become increasingly popular in almost all organizations and institutions. The application of steganography, watermarking, and encryption methods to authenticate the digital data origin seems necessary to avoid serious threats and secure wireless data communication. Hence, the content of digital media should be secured in applications like confidential video conferencing, military, pay-per-view TV (PPV), multimedia systems of industry and medicine. Users of wireless portable devices need to protect their private wireless multimedia communications electronically [1, 2] Cryptography is the use of mathematics to secure communication and to ensure powerful confidentiality and privacy by encrypting and decrypting data and converting plain text intelligible data into unintelligible. The word cryptography is composed of two parts: The Greek term “kryptós” which means “hidden” and the suffix “graphin” meaning “writing”. Thus, it means “hidden writing”. Its system contains three algorithms: encryption, decryption and Key generation in addition to the plaintext which is normal and readable, rather than encrypted, messages or data. Encryption is plaintext conversion to cipher text by the use of key and the reverse is decryption. Cryptanalysts could succeed in breaking the ciphers through the analysis of the contents of cipher text to retrieve the plaintext. To control the cryptosystem, key information is used; this key is known by the sender and receivers only. There are three dimensions, which are independent, of cryptographic systems:

1.1. Plaintext operation

Two operations on plaintexts happen in the conversion from plain to cipher text. In the first operation, the elements substitute each other in the cipher text and map from one to another such as Caesar cipher. In the

second operation, the characters are transposed with each other on the bases of mapping controlled by the key. Here, the characters of the plain texts remain the same but with movements into different places for example Rail Fence cipher. The majority of the systems are systems of products of many stages of substitutions and transpositions.

1.2. Used key numbers

When the sender and receivers use the same encrypt and decrypt key for the plain text, the system is symmetric, use single secret key. When different public and private keys are used for the encrypting and decrypting of the plaintext, the system is asymmetric, and sometimes called public key encryption or two – key encryption.

1.3. The plain text processing

Groups of bits, referred to as blocks, are used to operate the block cipher and constantly produce a cipher element each time while operating.

Steganography is an art and a science to hiding information within data. Steganography has two image embedding techniques in steganography. The first is spatial domain and the second is the transform domain.
In the spatial domain, messages are directly embedded in the Least Significant Bits (LSBs).
In transform domain, the frequencies of the image coefficient of the cover such as Fourier, discrete cosine, or the wavelet are modified [3-5].
The reason for the comparison between the stego and cover images is to evaluate their quality. In this comparison, stego-image quality is measured by the use of Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The former is to quantify the variation between the initial cover and the Stego image which is noisy or distorted.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right) \quad \text{.....(1)}$$

The coordinates of the image are X and Y are and N,M are the number of columns and rows of the input image respectively. The produced image is Sxy and the cover image is Cxy.
PSNR=10 log 10 (C2max /MSE) …..…… (2)
MSE is the mean square error which can be calculated by the equation (1) and Peak Signal-to-Noise Ratio (PSNR) calculated by the equation (2)[6, 7].
Nowadays, internet becomes a key source for transferring information, online shopping, online money transfer, and online payment. However, to avoid the interception, cryptography helps to secure information effectively. When cryptography is used, attackers could not hack the videos because they lose control over their data before transmission and it becomes difficult to retrieve the original ones. There are two main kinds of cryptography: Symmetric and Asymmetric Keys Cryptographies. However, steganography could conceals secrete data of plain texts, images, videos and/or audios in different media formats [8-10].Embedding efficiency and embedding payload are two determining factors in the performance of steganography. Embedding efficiency is the size of the data to be concealed in the cover file; whereas embedding payload is steganography system capacity to conceal the largest data possible with less distortion. Generally, they correlate negatively[8, 11, 12]. The video steganography technique has a big hiding capacity which is the extent of embeddable information). This is significant component for the design of an algorithm of steganography[11, 13, 14]. Furthermore, hiding data in video files provides additional security in the event of third party attack or accidental receipt because of the relative complexity of video structures in comparison with those of images and audios. This technique uses pixel mapping method to hide data in video cover files. Basically, different frames are combined to produce any frame fixed rate video. A novel framework to conceal images in videos is replacing one LSB of each pixel in video frames. This framework makes it very difficult for intruders to guess the content of the image [15, 16].
There are a number of studies available on the video confidentiality and how to secure video contents. Some of these studies failed to keep the content intact such [17-19]. Some studies use a hybrid of method. For example, [20, 21] and [22] used a hybrid of image (not video) encryption using a private XOR operation and fractals, utilized three random parameters as secret keys to create many random fractal images. The majority of other studies such as [23-27] and attach more importance to the image rather than the whole content of the video.
In addition, Indrabi presented a new method of video steganography where Data Encryption Standard (DES) algorithm was utilized to encrypt data and LSB mechanism was applied to embed data in the cover video

frames[28].However, my study was different from these studies in that it used a presented a robust and secure hybrid model of video encryption and steganography and aimed to keep the content intact. This model has two security levels for communicating secret information; an efficient new symmetric encryption algorithm was used to encrypt secret video data before embedding them in another video.

2. Proposed method

The overall objective of this paper was to design a method for embedding secret video in other video files keeping the original content intact and concealing any hint to the intruder. Other sub-aims were following points (see Figure 1):

i. Encrypting a secret video file to increase security.

ii. Hiding encrypted secret video file in a carrier AVI video file format.

iii. Un-hiding encrypted secret video file.

iv. Decryption and secret video recovery.

In the method proposed by this study, AVI file was used as secret and carrier. The study confirmed that the performance of video steganography is greater than other methods of steganography in terms of the amount of embeddable data t. The encryption of secret video data was done using two keys prior to embedding in the cover video to increase the information security. Since the frame was embedded by modifying only LSB, no significant change in the intensity of the cover frame was observed. The main steps for performing the proposed method were as follows:

Firstly, a secret AVI video file was read and then distributed to the photo frames through utilizing a MATLAB code. Then, the frames were stored in sequence. Each frame contained a combination of three layers red, blue and green. After that, those frames were extracted based on such information as their number, height, width and frames per second. Secondly, a new symmetric key cryptography algorithm was employed to encrypt the secure video by using two keys and bit XOR operation. One key was used with first byte of each channel (RGB) and the result became the key for the second byte. Then, a matrix was generated from the two keys that could be incremented by any value to randomize the key range and encrypt the video frames by using bit XOR operation (see Figure 2). Thirdly, a modified LSB technique was applied to embed the encrypted secret video frames in the LSB of each pixel of the cover video frames. LSB-based steganography was one of the simplest techniques for hiding a secret image in LSBs of pixel values without any noticeable misrepresentations. The secret video frame was converted into a new 1-dimensional matrix (size x3), and was hidden in cover video frame (fill in red, in green and in blue) (see Figure 3). The following steps summarized the main algorithms of encryption and hiding employed in this study (see Figure 4):

Step 1: Select the secret AVI video file.
Step 2: Extract frames from the secret video file.
Step 3: Encrypt the secret frames using two keys and XOR operation.
Step 4: Select the cover AVI video file.
Step 5: Extract frames from the cover video.
Step 6: Hide the encrypted Secret frames in
Step 7: Cover frames using modified LSB technique.
Step 8: Combine stego frames to make video.
Step 9: Output Stego video.
Step10: The end.

The above steps are put in reverse to restore the original (Secret) video, to un-hiding and decrypt, see (Figure 5):

1: Inputting Stego Video.
2: Extracting frames from Stego video.
3: Getting the encrypted secret frames.
4: Inputting secret keys.
5: Decrypting the secret frames through utilizing the keys in reverse encryption steps to obtain the original frames.
6: Outputting the secret video.
7: The end.

3. Results and discussion

The system was applied through utilizing Matlab Graphic User Interface (GUI), representing an efficient and easy tool for video management supported by powerful testing tools like histograms and mathematics for image quality. Various examples were shown in figures 7 to 12. The suggested method was tested on different secure videos (Eye, Medicine Cells and Traffic) and different cover videos (Space, Plants and Bird). Experimental results revealed a good performance with low correlation and very high PSNR of the Stego video frames. The new system became operational and applicable using designed GUI system as follows:

a) The first stage is the use of bit XOR operation to encrypt all secret video frames to create a large range of different keys to make is the security of a symmetric cryptography with two keys used for creating a large range of different keys by. This means that more than one key could be used for encrypting each secret video frame.

b) When the histograms of the secret and encrypted video frames were compared, the encrypted frame pixels had a high correlation (see Figure 6).

c) In the second stage, the encrypted secret video frames were hiding a high resolution bitmap color frames in selective cover video frames by using LSB method. Then, PSNR was computed to determine the quality of each cover frame.

d) All results revealed that all cover frames in hiding operation were characterized by a high quality. Hence, PSNR exceeded 50 Db (see Table 1).

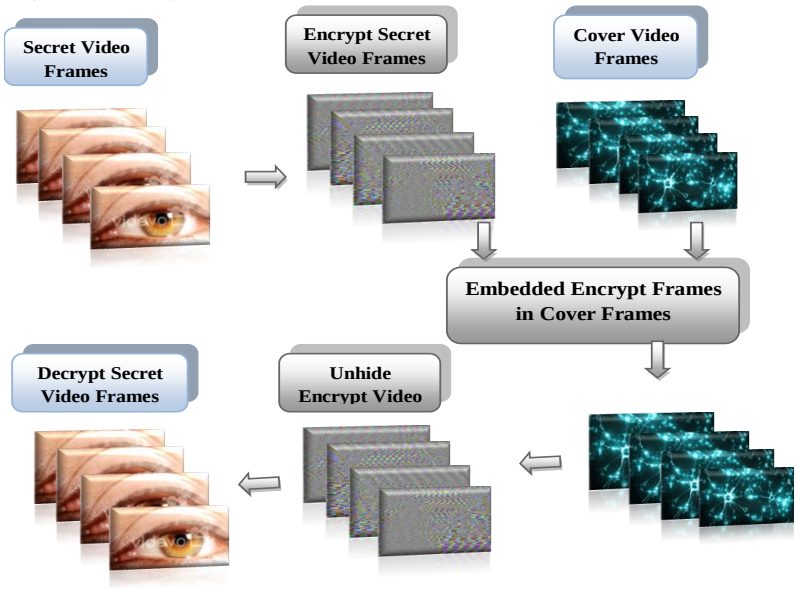

Figure 1. The diagram of proposed system

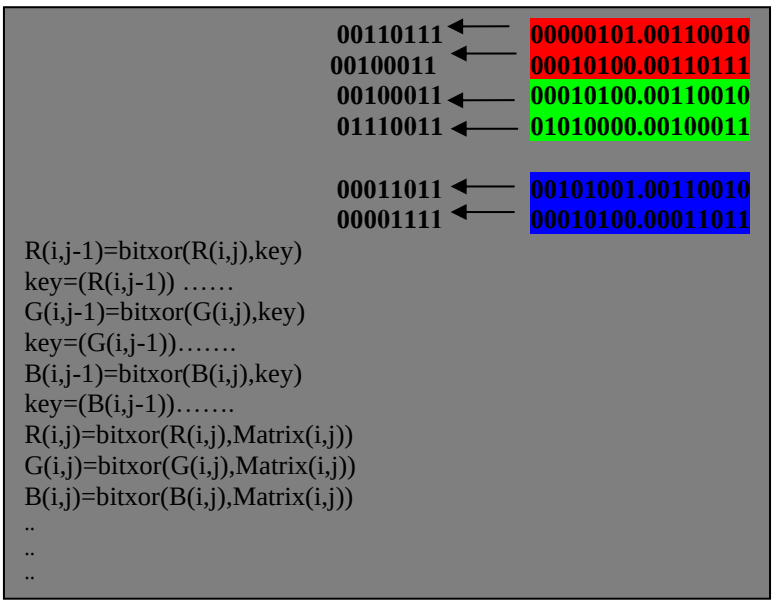

Figure 2. The generation of key ranges

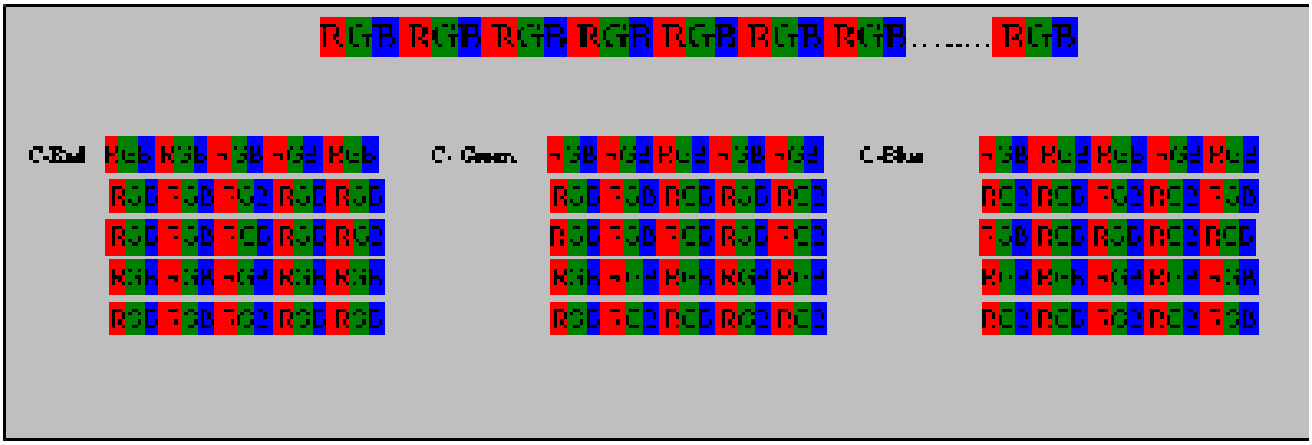

Figure 3. Hiding encrypted secret video frames in cover video

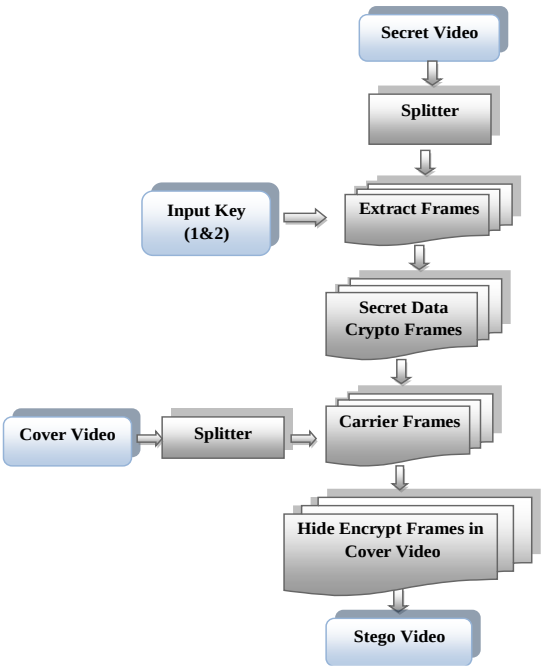

Figure 4. Encrypting and concealing hiding stages

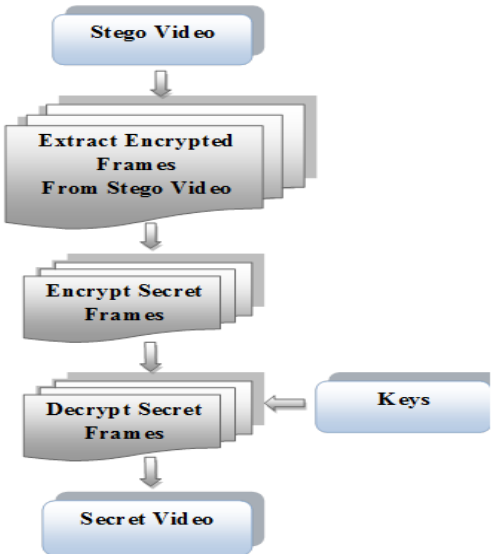

Figure 5. Decrypt stages

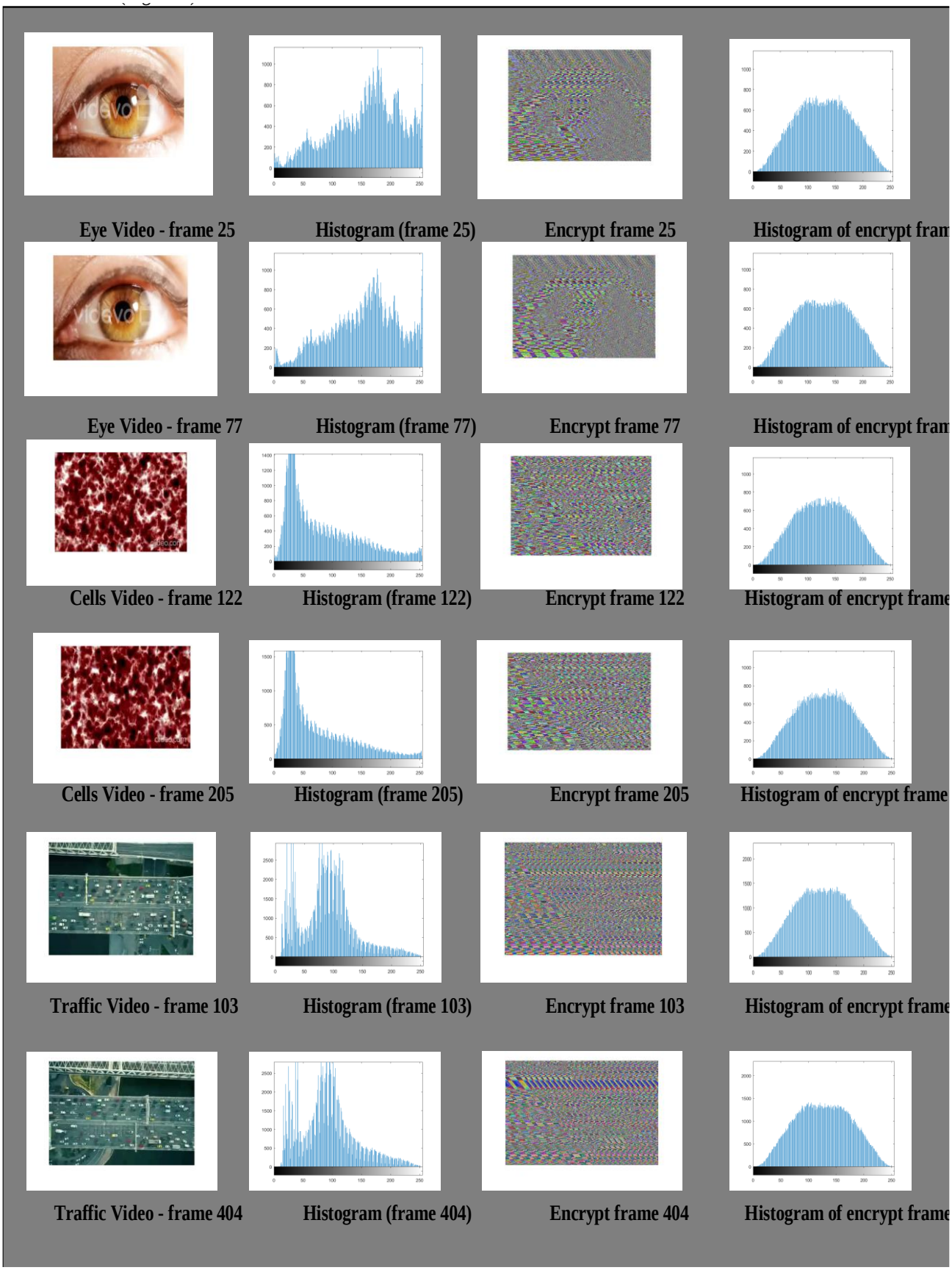

Figure 6. The original and encrypted secret video frames: *(a) Secret video frames; (b) Secret frames; (c) Encrypted secret video frames; (d) Encrypted secret frame;*

Table 1. the PSNR of cover video frames after hiding operation

Frame No.	Cover Video Frame	Stego Video Frame	PSNR
90			52.9871
150			52.9869
55			52.9848
232			52.9898
46			56.6998
262			56.7008

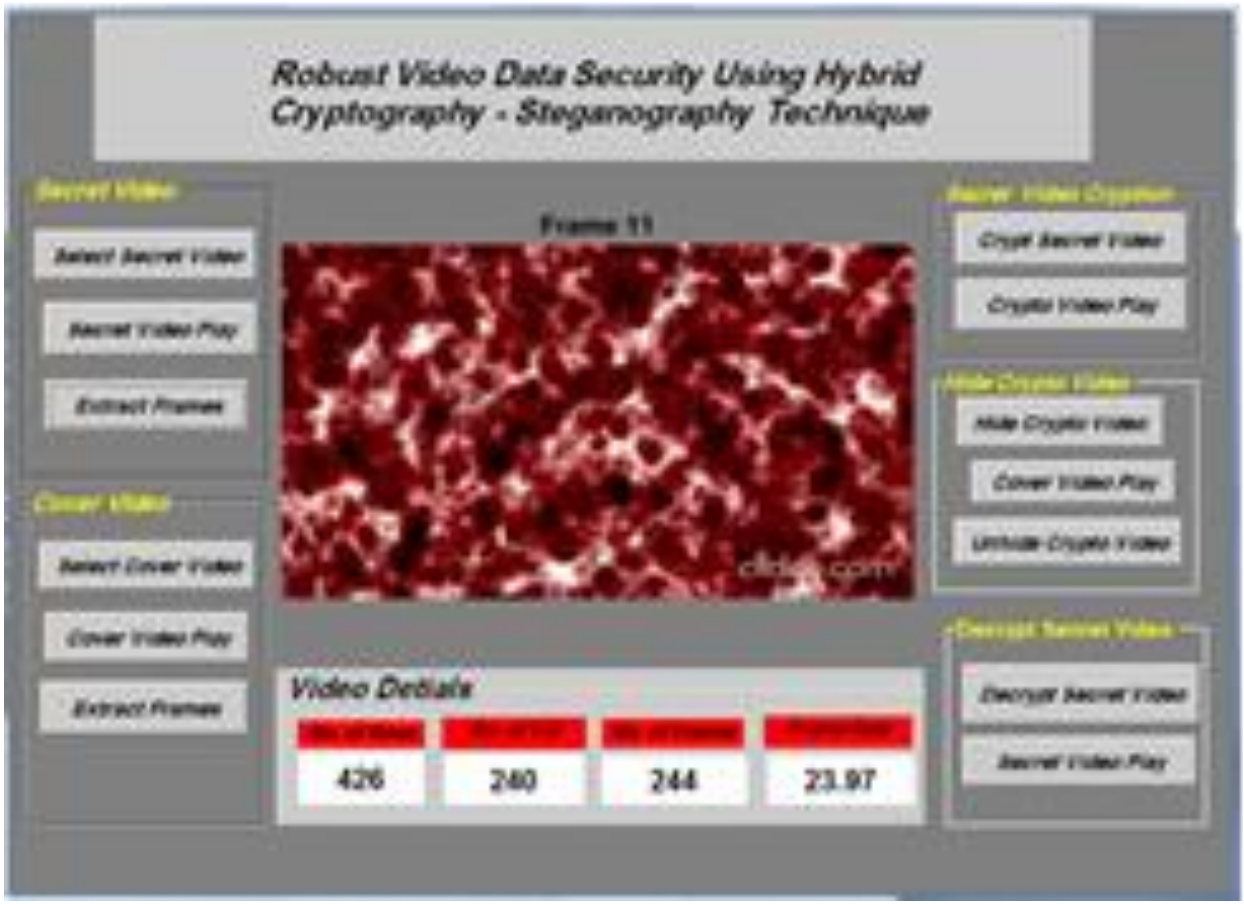

Figure 7. GUI the secret video frame

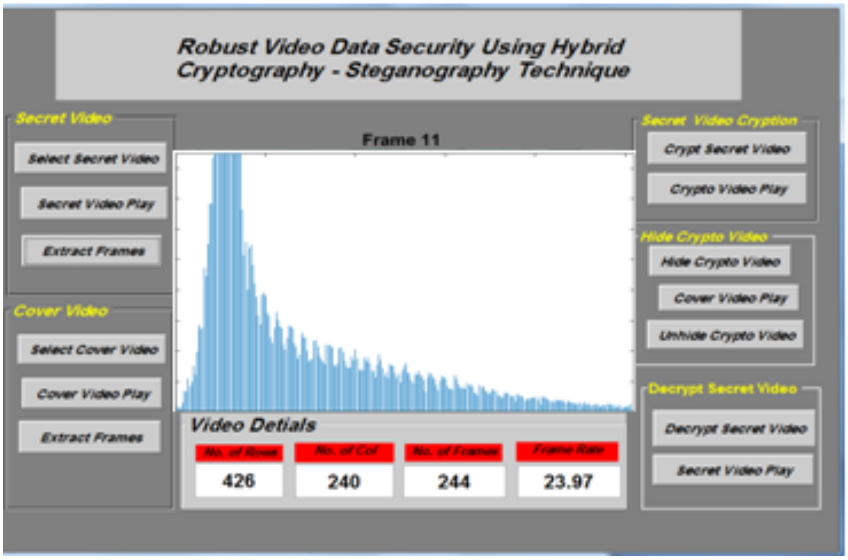

Figure 8. GUI the secret video frame histogram

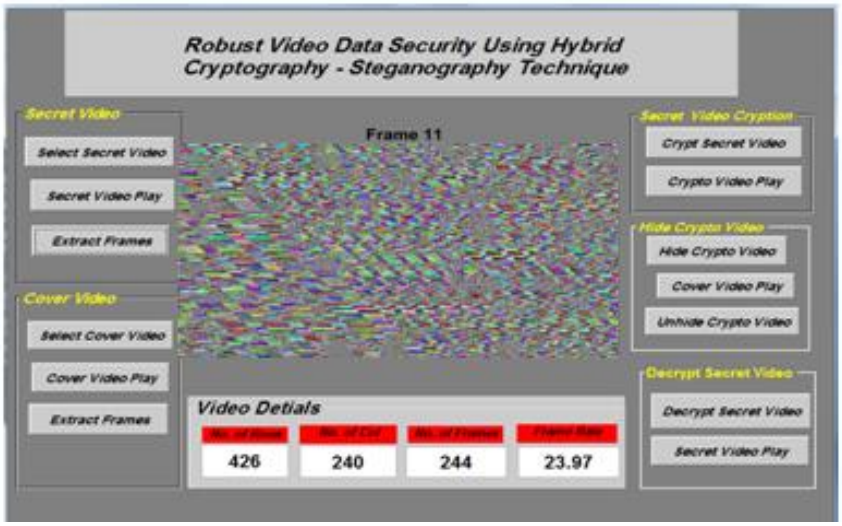

Figure 9. GUI secret video frame encryption

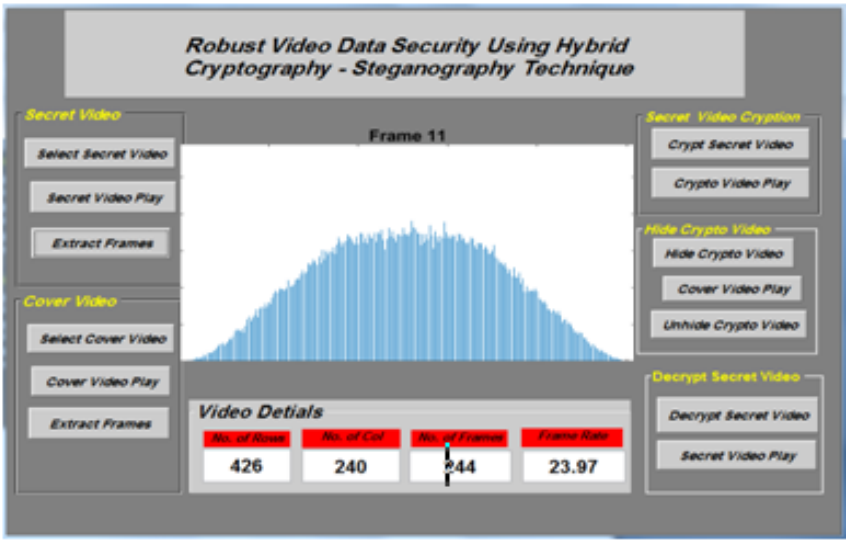

Figure 10. GUI secret video frame encryption histogram

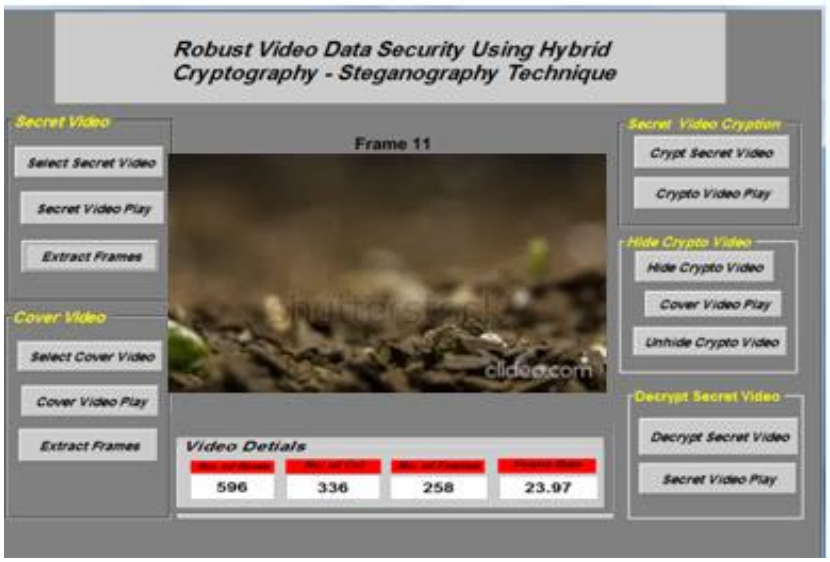

Figure 11. GUI showing the Cover video frame

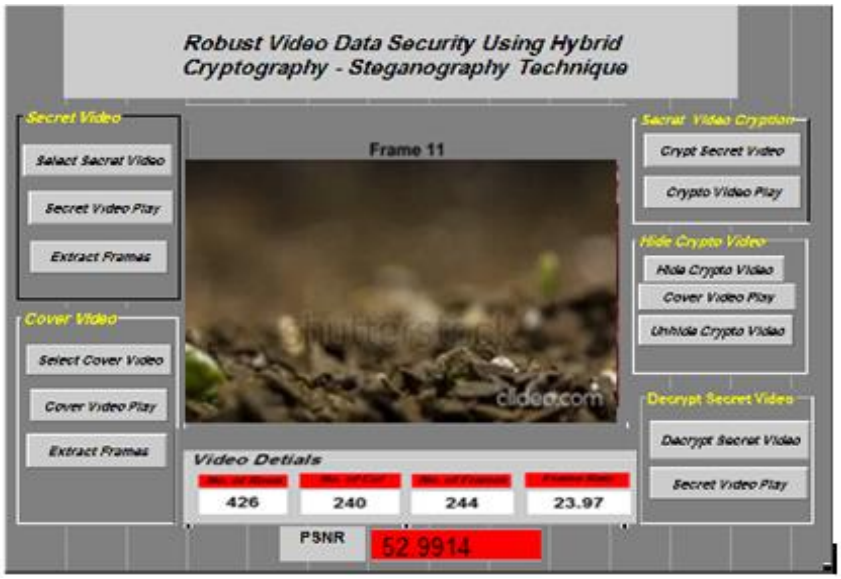

Figure 12. GUI with the stego video frame

4. Conclusion

With the increase in the digital media, data security has become a major concern. Mere steganography is not a good solution to secrecy nor is mere encryption. However, integrating both methods provides an effective tool enabling people to communicate without possible eavesdroppers. Therefore, this paper presented a robust and secure hybrid model of video encryption and steganography with two security levels for communicating secret information. An efficient new symmetric encryption algorithm was used to encrypt secret video data before embedding them in another video. The encrypted image histograms were used to find the correlation of the reconstructed images and PSNR was utilized to find the stego quality. This study revealed that integrating cryptography with steganography could enhance the security of information. In addition, there was a high correlation in the histograms resulted, protecting the secret video data. The PSNR value was greater than 50 db, indicating that the differences between the cover and stego frames are not visible to human eyes. Since the frames were embedded by modifying only LSB method, no significant change happened in the image intensity.

References

[1] S. S. Ghazoul, Y. H. Ali, A. T. J. E. Hashim, and T. Journal, "Developed method of information hiding in video AVI file based on hybrid encryption and steganography," vol. 29, no. 2, pp. 359-373, 2011.

[2] S. P. Sahu and S. Verma, "Secured and authentic communication by combined approach of digital watermarking and steganography," in International Conference on Advances in Communication, Network, and Computing, 2011, pp. 595-599: Springer.

[3] G. P. Rajkumar, V. J. I. J. o. C. N. Malemath, and I. Security, "Video Steganography: Secure Data Hiding Technique," vol. 9, no. 9, 2017.

[4] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data security using cryptography and steganography techniques," ed: IJACSA) International Journal of Advanced Computer Science and Applications, 2016.

[5] O. H. Yahya, H. Alrikabi, I. A. J. I. J. o. O. Aljazaery, and B. Engineering, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," vol. 16, no. 03, pp. 107-116, 2020.

[6] M. K. I. Rahmani, K. Arora, N. J. I. J. o. A. C. S. Pal, and Application, "A crypto-steganography: A survey," vol. 5, pp. 149-154, 2014.

[7] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012, pp. 122-126: IEEE.

[8] F. H. M. J. I. J. o. E. E. Al-Kadei and C. Science, "Two-level hiding an encrypted image," vol. 18, no. 2, pp. 961-969, 2020.

[9] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk, and B. J. M. S. Furht, "New approaches to encryption and steganography for digital videos," vol. 13, no. 3, pp. 191-204, 2007.

[10] M. A. a. Roa'a, I. A. Aljazaery, S. K. Al_Dulaimi, H. T. S. J. B. o. E. E. Alrikabi, and Informatics, "Generation of High Dynamic Range for Enhancing the Panorama Environment," vol. 10, no. 1, 2020.

[11] K. N. Jassim et al., "Hybrid cryptography and steganography method to embed encrypted text message within image," in Journal of Physics: Conference Series, 2019, vol. 1339, no. 1, p. 012061: IOP Publishing.

[12] H. T. S. Al-Rikabi, Enhancement of the MIMO-OFDM Technologies. California State University, Fullerton, 2013.

[13] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. J. i. Aziz, "Combination of Hiding and Encryption for Data Security," vol. 14, no. 9, p. 35, 2020.

[14] A. H. M. Alaidi and A. Mahmood, "Distributed hybrid method to solve multiple traveling salesman problems," in 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), 2018, pp. 74-78: IEEE.

[15] S. R. Ratna, J. S. Loret, D. M. Gethsy, P. P. Krishnan, and P. A. Prabu, "A Review on Various Approaches in Video Steganography," in Intelligent Communication Technologies and Virtual Mobile Networks, 2019, pp. 626-632: Springer.

[16] N. S. Alseelawi, E. K. Adnan, H. T. Hazim, H. Alrikabi, and K. Nasser, "Design and Implementation of an E-learning Platform Using N-Tier Architecture," 2020.

[17] E. Najafi, K. J. J. o. i. s. Loukhaoukha, and applications, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," vol. 44, pp. 144-156, 2019.

[18] M. J. W. A. o. S. Ramalingam, Engineering and Technology, "Stego machine–video steganography using modified LSB algorithm," vol. 74, pp. 502-505, 2011.

[19] O. H. Yahya, H. T. ALRikabi, R. a. M. Al_airaji, and M. J. I. J. o. I. M. T. Faezipour, "Using Internet of Things Application for Disposing of Solid Waste," vol. 14, no. 13, 2020.

[20] N. A. Minas, F. H. MohammedSediq, and A. I. J. k. u. j. f. s. s. Salih, "Color Image Encryption Using Hybrid Method of Fractal-Based Key and Private XOR Key," vol. 13, no. 1, pp. 104-117, 2018.

[21] N. A. Hussiena, A. H. M. Alaidib, T. A. Alquraishc, and G. F. Smaisim, "Improvement the Route Discovery Mechanism of Dynamic Source Routing Protocol in MANET."

[22] N. Sharma, J. Bhatia, and D. N. J. P. Gupta, Chandigarh, "An encrypto-stego technique based secure data transmission system," 2005.

[23] N. K. Jain, R. Saini, and P. Mittal, "A Review on Traffic Monitoring System Techniques," in Soft Computing: Theories and Applications: Springer, 2019, pp. 569-577.

[24] S. Arunkumar, V. Subramaniyaswamy, R. J. E. E. T. o. P. H. Logesh, and Technology, "Hybrid Robust Image Steganography approach for the secure transmission of biomedical images in Cloud," vol. 5, no. 18, 2019.
[25] O. Salman, I. H. Elhajj, A. Kayssi, and A. J. A. o. T. Chehab, "A review on machine learning–based approaches for Internet traffic classification," pp. 1-38, 2020.
[26] A. Arya, S. J. I. J. o. F. R. i. C. S. Soni, and C. Engineering, "A literature review on various recent steganography techniques," vol. 4, no. 1, pp. 143-149, 2018.
[27] S. Pal, S. K. J. I. J. o. I. R. Bandyopadhyay, and Review, "Various Methods of Video Steganography," vol. 3, no. 6, pp. 2569-2573, 2016.
[28] S. J. Indrabi, N. Saini, M. J. I. J. o. P. Mohan, and A. Mathematics, "Secure data transmission based on combined effect of cryptography and steganography using visible light spectrum," vol. 118, no. 20, pp. 2851-2860, 2018.
[29] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019.
[30] N. J. Qasim and I. Barazanchi, "Unconstrained Joint Face Detection and Recognition in Video Surveillance System," Jour Adv Res. Dyn. Control Syst., vol. 11, no. 1, pp. 1855–1862, 2019.
[31] H. K. Silman and A. E. Ali, "Breast cancer identification based on artificial intelligent system", Sustainable Engineering and Innovation, vol. 2, no. 2, pp. 41-49, 2020.