Hiding Secret Data in Color Video Applying Modify RSA for Cryptography with Randomly Select Frame and Pixel to Steganography

Hatem Nahi Mohaisen [1], Mohammed Q. Mohammed [2], Mustafa Hatem Nahi [3]

1 Ministry of High Education and Scientific Research/Minister's office, Baghdad, Iraq.

2 University of Information Technology and Communications, Baghdad, Iraq.

3 Al-Esraa University, Baghdad, Iraq.

ha19652010@yahoo.com

dr.mohammed@uoitc.edu.iq

mustafa1234432111@gmail.com

Hiding Secret Data in Color Video Applying Modify RSA for Cryptography with Randomly Select Frame and Pixel to Steganography

Hatem Nahi Mohaisen[1, a)], Mohammed Q. Mohammed[2,3, b)] Mustafa Hatem Nahi[3, c)]
[1] Ministry of High Education and Scientific Research/Minister's office, Baghdad, Iraq.
[2] University of Information Technology and Communications, Baghdad, Iraq.
[3] Al-Esraa University, Baghdad, Iraq.

ha19652010@yahoo.com
dr.mohammed@uoitc.edu.iq
mustafa1234432111@gmail.com

Briefly:
In this study paper, we will explain how to conceal sensitive notification in a color movie by selecting a frame at random and then using a mathematical calculation to split the frame into (R G B) and random pixels from that frame. This method goes through five basic stages, the first stage, transform the video to frames, which represents the number of frames that make up the video, the second stage choice one frame from this frames randomly, after that transform the frame to digital and separating the frame to three matrix (R, G, B), third stage transform secret message the encryption using the RSA. The number of pixels choose dependent on the length encryption secret message. Fourth stage hiding the encryption message in the frame randomly in (R, G, B). Then we return the selected pixels to their original positions in the frame. The five stages, return the frame in original place in video and send the video to the recipient. The statistical measures were used the Structural Similarity Index Measure (SSIM), peak signal to noise ratio (PSNR), histogram and mean square error (MSE). The outcomes achieved are excellent. The recipient to extract the secret message follows the same secure keys to arrive the hid secret and same steps from the first four stages.
Keywords: Information concealing, Video, SSIM, PSNR, MSE, and Modified RSA cryptography, Seed number, Histogram.

INTRODUCTION

These days, information security is crucial to the storage and transmission of data, particularly when high levels of anonymity are needed. The video or images are rentals in considerable part in many businesses. Because of this, it's important to protect video and image data from prohibitive arrival or from being decrypted by an unexpected user. Attackers and other intruders interfere with the majority of systems globally, altering or tampering with critical data that is transmitted through those systems. The secrecy of digital videos has become more important in today's technological and connected society. Numerous researchers have come up with numerous strategies to avoid these issues and stop them from disclosing or altering information in order to tackle these concerns. The most well-known techniques for preserving crucial data while it is being sent are cryptography and steganography. An inclusion technique for hiding encrypted messages in random and non-contiguous pixel locations along borders and in smooth areas of pictures [1]. Steganography is a technique for concealing information in media, whereas cryptography encrypts data and uses an appropriate key [2, 3, 4]. Utilizing a hash function to generate a modality for data hiding into the carrier media's LSB of RGB pixel values [5]. In the temporal domain, a mixed steganography and encryption technique is used. First, the secret handwritten signature's image is encrypted using RSA; the final three bits are then randomly entered based on mathematical randomized [6]. By integrating many cryptography phases—the DNA algorithm, GZIP algorithm, AES and image, multiplying by worker along the last step of DNA encryption, and LSB image steganography technology—the encrypted letter is disguised in a high-quality image steganography [7]. An innovative asymmetric picture encryption method relied on the Arnold transformation and RSA algorithm. First, the quantum logistic chart's prime values are

generated using the RSA algorithm's asymmetric public key. Secondly, the Arnold chart's parameters are computed. The process of investigating the rough concealing of picture information on a typical image is called the Arnold creeping operation. Third, the image's columns and rows are each assigned different units, and exclusive-OR (XOR) diffusion is then used [8]. Combining the human skin-color offer with the LSB algorithm—which can choose the inclusion zones—is an additional choice. This theory is based on the observation that the Human Vision System (HVS) tends to concentrate its attention on selecting specific visual sight structures rather than the entire image [9]. Secret data was concealed in a grayscale digital image using a different technique. Combining RSA encryption with steganography has advantages. This method relies on looking for two-by-two congruence bits between the values of the image pixels and the secret data bits. The confidential data bits are hidden at the drag (LSB) least significant bits in the event that the bits are not congruent. To apply the steganography technique, two types of images are used: a bright grayscale image and a dark grayscale image [10]. Arnold Mapping is utilized to guarantee extreme jumbleness in both copartner pixels and random spreading, hence excluding any potential interaction with the main picture placate, architecture enlarged visual cryptography design for color images and increased security [11]. A mix of three techniques to increase the system's overall security level: altered RSA cryptography, steganography-encrypted text, and random pixel selection from an image [12]. Use a mathematical equation to randomly pick the number of bytes in a color image that contains confidential information. The long of the confidential message determines how many randomly chosen bytes will be included in the digital picture once it has been transformed [13]. Combining cryptography and steganography results in a strong system that can use the RSA technique to encode a secret message. The sophisticated LSB approach is utilized to disguise the message [14]. This work uses the affine transformation approach as a display steganography method to hide data. The coefficients of the video frames' integer wavelet transform include the secret data. The affine transformation is used to disperse the pixel values during embedding [15]. This article illustrates the two approaches' various applications. A communication is encrypted while it is being transferred over a network from one source to another using steganography and cryptography. These methods are frequently employed to ensure the security and privacy of data. While stenography is used to conceal the cover medium, such as audio, photos, or videos, cryptography keys conceal information using a private key or public key, preventing third party from accessing the data. These methods have been applied to entity authentication, basic authentication, confidentiality, and security of data[16]. Suggested encrypting images with second-order equations and embedding the resultant encrypted image within the movie. To strengthen the security layer, the image is embedded based on the equations rather than sequentially. The experimental findings indicate that a high embedding ability is achieved by the suggested strategy. Additionally, as compared to alternative information-hiding techniques, the suggested system is more secure and resilient due to encryption and non-sequential frame and bit-hiding location selection [17]. In order to conceal data in video files, this project presents the Least Significant Bit Substitution approach using elliptical curve cryptography. Data hiding, a type of cryptography used in this research, inserts data into digital media for identification and annotation purposes [18]. This study looks at the histogram that forms inside the frame as well as the forecast error that arises between two consecutive frames of a video binder. The resulting stego_file's frame count and composition remain unchanged despite these updated forecast inaccuracies [19]. Video frames can be encrypted and conceal into a cover video binder using one of two techniques. First, a wide variety of distinct keys were generated for encryption using two keys and the XOR bit operation. Second, to provide two security levels, a improve version of the least significant bit (LSB) technique was used to hide bitmap color, high quality video frames in specific cover video frames. Encryption and data masking techniques were successfully tested on numerous classified recordings, including Traffic, Secret Medicine, and Ad Eye videos [20].

This study offers a novel approach to stop hackers, intruders, and cryptanalysis from accessing, changing, or tampering with sensitive data. Using five methods, video splitting, RSA modification, unspecified of the chosen frame from color video, selection of pixels from a single frame based on the length of the secret message, and concealment technique employing (LSB).

FUNDAMENTALS

RSA Cryptography

One of the earliest and most commonly employed methods for public-key encryption is the RSA algorithm. This cryptographic technique was introduced in 1977 by a team of MIT-affiliated researchers led by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA is frequently utilized for creating public and private key pairs [21]. The RSA algorithm operates in an asymmetric manner, involving the use of two keys: one for the public and another for the private. Next, it proceeds with the key generation procedure in five steps:

1. Select (p and q) two huge prime numbers.
2. Determine n = p * q.
3. Φ (n) = (p − 1) * (q − 1) must be calculated.
4. Select a number e such that 1 < e < Φ (n), and:
(a) Ascertain that gcd (e; Φ(n)) = 1.
(b) Make sure Φ (n) and e are coprime.
5. Calculate an integer d such that d = e−1 mod Φ (n).

Both the produced asymmetric keys and the decryption process can use them. The public key is made up of (n, e), whereas the private key is made up of (d). Kprivate = (d, n), Kpublic = (e, n) [22].

Pseudo-random number generator

For computers, creating unspecific numbers for cryptography is a difficult process. A function for pseudo-random number creation, after receiving a starting seed, produces a series of digits that appear random to an observer without knowledge of the seed value [23]. The linear congruential random number generator (LCRNG) is used to create a unspecific set from pixels, initially put forth by Lehmer [24], is used. One of the most popular methods for creating a series of unspecific numbers is the LCRNG (x0,x1,.....) within range [0, n−1]. The number of seeds is x0. Any successive random number xi+1, can be get using the following formula:

$$xi+1 = w * xi + s \bmod m \quad (1)$$

Where m is the modulus, s is the increment, and w is the constant multiplier.

LSB Concealing

The purpose of concealing is to hide sensitive information within the transmission medium so that an adversary cannot detect the presence of the hidden message. Steganography can be used with various forms of data such as audio, video, and images, and has the ability to hide a wide range of digital content. The least significant bit, or LSB, is one of the most straightforward techniques for cancelation of spatial domain images [8]. The following algorithm makes hiding easier and easier to implement. The goal of data embedding is to obliquely add a message to each pixel's least significant bit on the bearer medium. View the following example:

Bitmap picture file: 10101101 11001010 10111010 01011001
Piece of Information: 0010
Stego Picture: 10101100 11001010 10111011 01011000

Later, other researchers proposed and put into practice some expanded versions of this technique. According to a study [25], bit replacement can also be performed on the sixth, seventh, eighth, and even on their combination.

Dedication Measure

The degree of change between the original image and the stego-image is estimated using these kinds of measurements. The following are the most well-known measurements [26]:

Equation of (MSE)

It is the average of two photos' square errors:

$$MSE = \frac{1}{RC}\sum_{y=1}^{C} \quad \sum_{x=1}^{R} \quad (f_0(x,y) - f_e(x,y))^2 \tag{2}$$

Equation of (PSNR)

The PSNR values, which assess the ratio of distortion and are derived from equation (3) for color images, are used to compare the original and stego-image:

$$PSNR = 10Log_{10}\left(\frac{\left(Max_{xy}f_0(x,y) - Min_{xy}f_e(x,y)\right)^2}{MSE}\right) \tag{3}$$

And in gray scale is:

$$PSNR = 10\ Log_{10}\left(\frac{255^2}{MSE}\right) \tag{4}$$

Where $Min_{xy}f_e$(x, y) = 0, and $Max_{xy}f_0$(x, y) = 255 denoted the original and embedded images, respectively, f_0 and f_e.

Equation of (SSIM)

Together with MSE and PSNR, a more recent metric like the structural similarity index metric (SSIM) can provide a comparison. Greater similarity is indicated by a high SSIM around one. SSIM can be computed using:

$$SSIM(x,y) = \frac{(\mu_x\mu_y + n_1)(2\sigma_{xy} + n_2)}{(\mu_x{}^2 + \pi_y{}^2 + n_1)(\sigma_x{}^2 + \sigma_y{}^2 + n_2)} \tag{5}$$

The constants $n_1$and n_2 > 0 are employed to ensure stability when other parameters are approximated to zeros, where σ is the standard deviation and μ is the mean intensity.

ENHANCED RSA AND THE SYSTEM'S STRUCTURE

The suggested system introduces a enhanced to the RSA formula, involving multiplication of the typical RSA formula by an integer for encryption and division by the same integer for decryption. This integer incorporates any additional keys included in both the private and public keys. This adjustment results in a modified RSA equation for encryption, with 'E' representing the cipher text. Now, the equation of RSA becomes:

$$E = (M_e mod\ n) * I \tag{6}$$

Where the integer, I is positive. Equation (7) represents the decryption equation.

$$M = \left(\frac{E}{I}\right)^d\ mod\ n \tag{7}$$

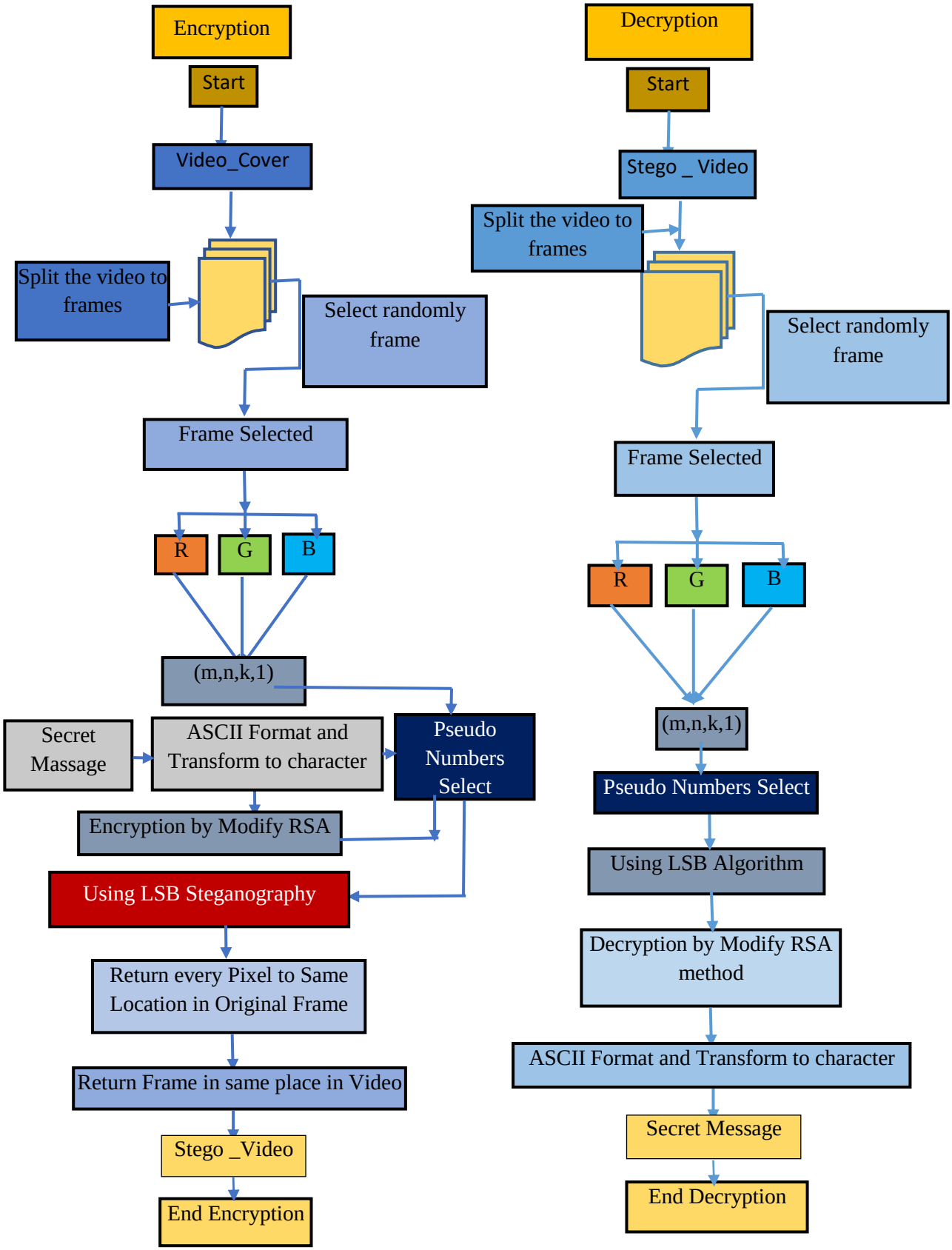

FIGURE 1. The encryption and decryption flowchart

PROPOSED METHOD

The suggested appr through two algorithms: one for encryption and one for decryption. When this algorithm is employed on a color video, it involves the following steps: splitting the video into individual frames, randomly selecting one or more frames,

separating the chosen frame(s), performing encryption, embedding secure data, and finally, decrypting and extracting the secure data. Algorithms 1 and 2 elaborate on each of these phases.

Algorithm 1 (transmitter portion)

Input: video cover, message, seed number, p, q, and integer I.

Output: stego_video.

A. Utilize the cover video
B. Divide the video into individual frames.
C. Randomly choose a frame using equation (1).
D. - Convert the message into ASCII format.
E. Employ equation (6) for message encryption.
F. Calculate the length of the ciphertext.
G. Split the selected frame into a 1-dimension (m * n * 3, 1), giving every pixel an index.
H. Using the equation (1) with a seed number to obtain a unspecific pixel from step (F) based on the long of the ciphertext.
I. Utilize LSB cancellation to hide the information in the randomly chosen pixel from (G).
J. Restore each pixel to its original position based on the frame's index.
K. Convert the one-dimensional representation of the selected frame back into a three-dimensional format (n, m, 3) to reconstruct the original frame.
L. Return the chosen frame to its original location in the video.
M. Transmit the video to the recipient as "Stego_video."

Algorithm 2 (recipient portion)

Input: video cover, message, seed number, p, q, and integer I.

Output: confidential message.

A. The Stego_video.
B. Divide the Stego_video into individual frames.
C. Randomly choose a frame using equation (1).
D. Transform the selected frame into a one-dimensional format (m * n * 3, 1).
E. Utilize equation (1) and input the message length together with the transmitter seed number.
F. Utilize LSB to extract the secure data from the pixels selected in step (E).
G. The ASCII form of the message can be obtained by applying equation (7) with the same values for I, p, and q.
H. Transform the ASCII characters into the original message.
I. The concealed confidential message.

TRIALS AND OUTCOMES

The suggested solution was put into practice on an HP PC running Windows 7 with an Intel(R) Core (TM) I5-7200U processor, 2.5 GHz CPU, 4.00 GB of RAM, and MATLAB 2014a software. The program was used on video file type (VIA), and the frame BMP type as cover video. The split of video shown that in Figure (2). The Figure (3A, 3B) depicts the façade of the proposed system apparenting the methods of encryption and decryption. The outcomes demonstrate that the suggested algorithm accomplishes a significant security. The findings demonstrate that the recommended method satisfies a significant security note, as indicated by figures 4 through 9 and the fidelity measure values listed in Table 1. The frame from figure (4), shown as a random numbers selection made from the frame following the message's encryption, and figure (5) represented of the frame 25 represent original and stego-frame and histogram (R, G, B) to the random frame selected, and frames from figures (6, 7, 8, 9) represented the frames (56,126,187,377) with the original frame and stego-frame and histogram caparison between original and stego-frame. The histogram of the original frame with the same length message is compressed when different frames are taken; the viewer is not aware of the subtle change in the histogram's form. A sample of choose random number from color frame of size 400 × 300 of message" hello hatem how are you i hope you are good health", Figure (4) displays the results for 88 generation of pixels.

The suggested approach can be used with color video and is described through two algorithms: one for encryption and one for decryption. When this algorithm is employed on a color video, it involves the following steps: splitting the video into individual frames, randomly selecting one or more frames, separating the chosen frame(s), performing encryption, embedding secure data, and finally, decrypting and extracting the secure data. Algorithms 1 and 2 elaborate on each of these phases.

Algorithm 1 (transmitter portion)

Input: video cover, message, seed number, p, q, and integer I.

Output: stego_video.

A- Utilize the cover video
B- Divide the video into individual frames.
C- Randomly choose a frame using equation (1).
D- - Convert the message into ASCII format.
E- Employ equation (6) for message encryption.
F- Calculate the length of the ciphertext.
G- Split the selected frame into a 1-dimension (m * n * 3, 1), giving every pixel an index.
H- Using the equation (1) with a seed number to obtain a unspecific pixel from step (F) based on the long of the ciphertext.
I- Utilize LSB cancellation to hide the information in the randomly chosen pixel from (G).
J- Restore each pixel to its original position based on the frame's index.
K- Convert the one-dimensional representation of the selected frame back into a three-dimensional format (n, m, 3) to reconstruct the original frame.
L- Return the chosen frame to its original location in the video.

M- Transmit the video to the recipient as "Stego_video."

Algorithm 2 (recipient portion)

Input: video cover, message, seed number, p, q, and integer I.

Output: confidential message.

A- The Stego_video.
B- Divide the Stego_video into individual frames.
C- Randomly choose a frame using equation (1).
D- Transform the selected frame into a one-dimensional format (m * n * 3, 1).
E- Utilize equation (1) and input the message length together with the transmitter seed number.
F- Utilize LSB to extract the secure data from the pixels selected in step (E).
G- The ASCII form of the message can be obtained by applying equation (7) with the same values for I, p, and q.
H- Transform the ASCII characters into the original message.
I- The concealed confidential message.

TRIALS AND OUTCOMES

The suggested solution was put into practice on an HP PC running Windows 7 with an Intel(R) Core (TM) I5-7200U processor, 2.5 GHz CPU, 4.00 GB of RAM, and MATLAB 2014a software. The program was used on video file type (VIA), and the frame BMP type as cover video. The split of video

shown that in Figure (2). The Figure (3A, 3B) depicts the façade of the proposed system apparenting the methods of encryption and decryption. The outcomes demonstrate that the suggested algorithm accomplishes a significant security. The findings demonstrate that the recommended method satisfies a significant security note, as indicated by figures 4 through 9 and the fidelity measure values listed in Table 1. The frame from figure (4), shown as a random numbers selection made from the frame following the message's encryption, and figure (5) represented of the frame 25 represent original and stego-frame and histogram (R, G, B) to the random frame selected, and frames from figures (6, 7, 8, 9) represented the frames (56,126,187,377) with the original frame and stego-frame and histogram caparison between original and stego-frame. The histogram of the original frame with the same length message is compressed when different frames are taken; the viewer is not aware of the subtle change in the histogram's form. A sample of choose random number from color frame of size 400 × 300 of message" hello hatem how are you i hope you are good health", Figure (4) displays the results for 88 generation of pixels.

FIGURE 3 B. The frontage of the suggested system to decryption

FIGURE 3 A. The frontage of the suggested system to encryption

```
The value of (N) is: 7663
The public key (e) is: 5
The value of (Phi) is: 7488
The private key (d)is: 4493
ASCII Code of the entered Message:
  Columns 1 through 17

   104   101   108   108   111    32   104    97   116   101   109    32   104   111   119    32    97

  Columns 18 through 34

   114   101    32   121   111   117    32   105    32   104   111   112   101    32   121   111   117

  Columns 35 through 50

    32    97   114   101    32   103   111   111   100    32   104   101    97   108   116   104

Cipher Text of the entered Message:
 Columns 1 through 8

      41478        28842        42090        42090        28272        34908        41478        37248

 Columns 9 through 16

      42948        28842         4236        34908        41478        28272        26322        34908

 Columns 17 through 24

      37248          408        28842        34908         6348        28272         7968        34908

 Columns 25 through 32

      28992        34908        41478        28272        20724        28842        34908         6348

 Columns 33 through 40

      28272         7968        34908        37248          408        28842        34908         6498

 Columns 41 through 48

      28272        28272        43362        34908        41478        28842        37248        42090

 Columns 49 through 50

      42948        41478
```

FIGURE 4. After the message has been encrypted, a random number is chosen from the frame.

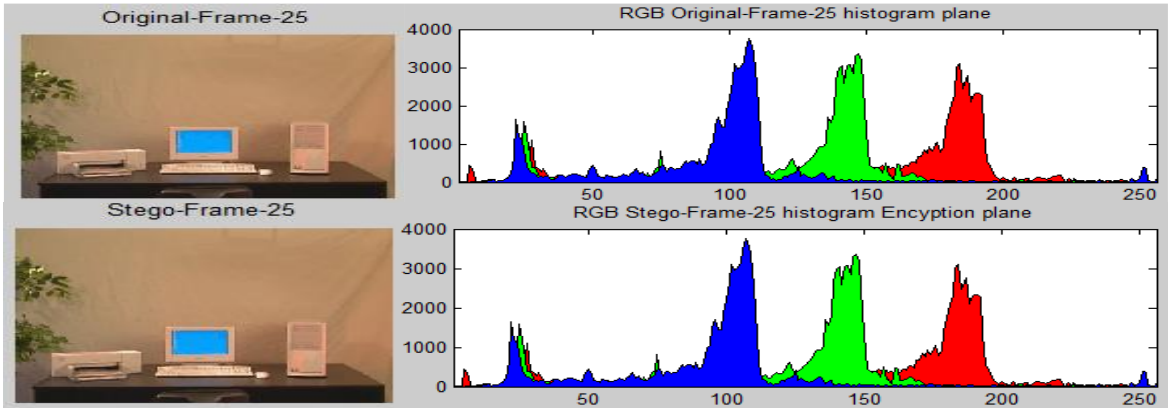

FIGURE 5. Frame 25 represent original and stego and histogram (R, G, B)

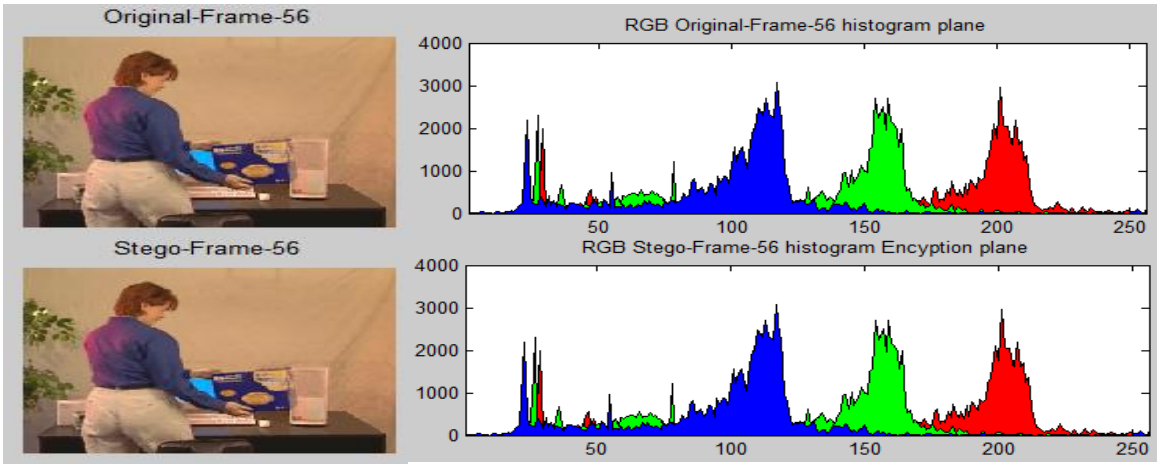

FIGURE 6. Frame 56 represent original and stego and histogram (R, G, B)

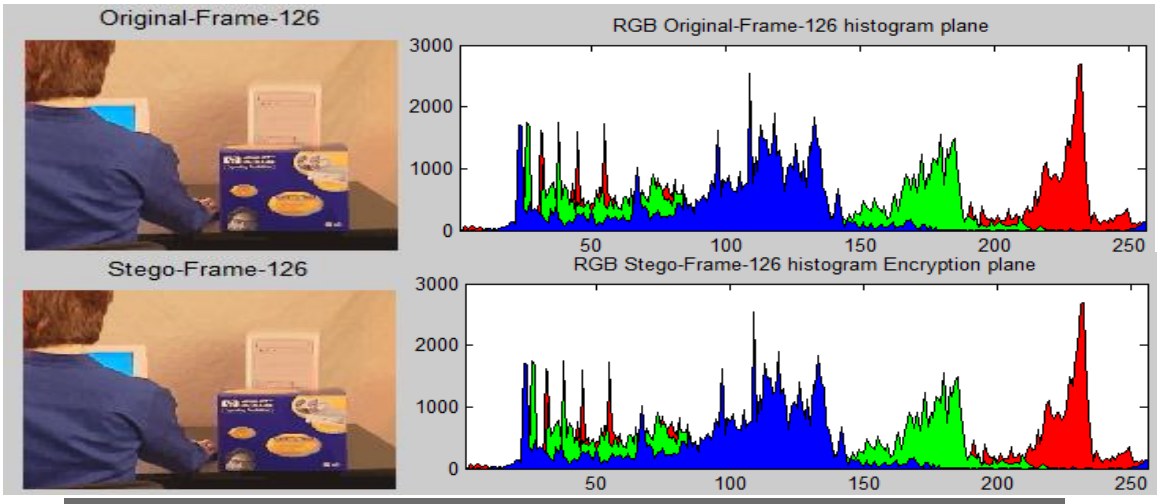

FIGURE 7. Frame 126 represent original and stego and histogram (R, G, B)

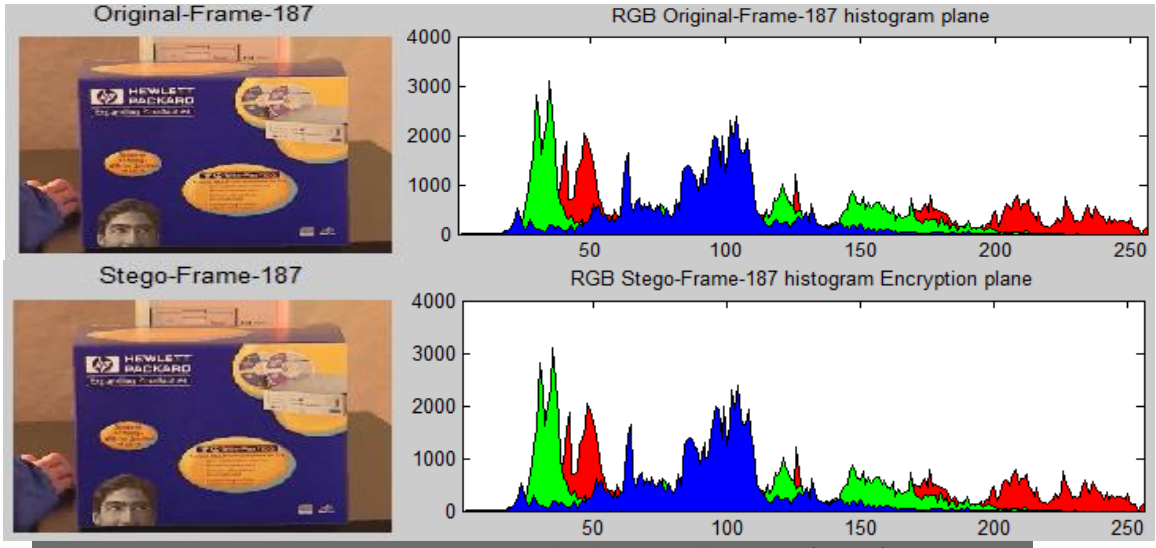

FIGURE 8. Frame 187 represent original and stego and histogram (R, G, B)

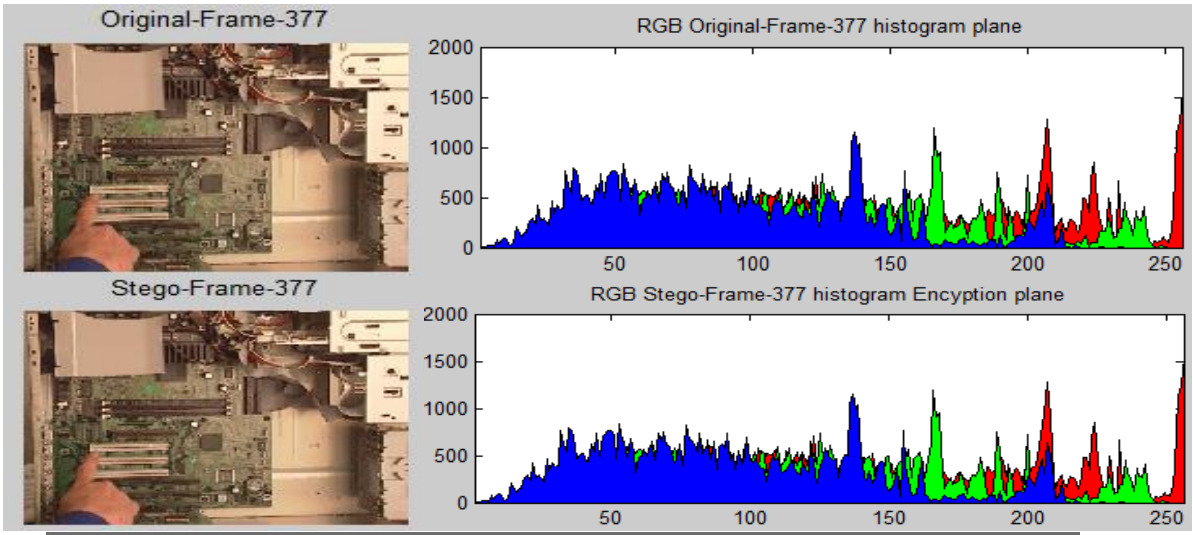

FIGURE 9. Frame 377 represent original and stego and histogram (R, G, B)

TABLE 1. Represent the variation value statistical measure for different frames

No.Frame	MSE	PSNR	SSIM	Histogram_Error
25	0.001675	75.8898	0.999997	5.8119E-07
56	0.001588	76.1208	0.999998	1.50553E-07
126	0.001684	75.8673	0.999997	4.8828E-08
187	0.0017231	75.7677	0.999998	1.8344E-07
377	0.0016666	75.9123	0.999999	9.0533E-08

IN CONCLUSION

Observes that by using video frames with strong color intensity and frame-to-frame differentiation, the following findings are made:

A- The (SSIM)is very near to 1, the MSE is very tiny, and the PSNR values are very high.

B- The original and stego-frame histograms are nearly the same.

C- A unique approach that can stop any attackers or intruders was created by combining randomized pixel selection from the frame with LSB steganography and altering RSA.

D- By using cryptography to tweak the RSA method and provide an alternative, an attacker or intruder will find it extremely difficult to predict the factor that adds to the RSA algorithm—particularly when adding a new element.

E- In order to avoid repeating the amount of pixels, it is preferable to select appropriate values for the seed number, p, q, and I.

F- The suggested system receives the algorithm, which is safe to hide any sensitive information and ensures that the video is not altered—even in the event that hackers or attackers try to access it.

H- The suggested system functions efficiently, rapidly, and well.

I- Using video in the process of hiding information gives you more space and flexibility, in addition to the possibility of revealing confidential information easily.

References

1. M. Juneja and P. S. Sandhu, “An improved LSB based steganography technique for RGB color images”, *Int. J. Comput. Commun. Engin*. 2(4) (2013) , pp:513–517.
2. K. Kordov and S. Zhelezov, “Steganography in color images with random order of pixel selection and encrypted text message embedding”, *Peer J. Comput. Sci.* 7 (2021) e380.
3. S. Majumder and M. M. Rahman, “Implementation of security enhanced image steganography with the incorproation of modified RSA algorithm”, *Int. Conf. Elect. Comput. Commun. Engin*. (2019) ,pp:1–5.
4. M. E. Saleh, A. A. Aly and F. A. Omara, “Data security using cryptography and steganography techniques”, *Int. J. Adv. Comput. Sci. Appl.* 7(6) (2016) ,pp:390–397.

5. R. Halder, S. Sengupta, S. Ghosh and D. Kundu, "A secure image steganography based on RSA algorithm and hash-LSB technique", *IOSR J. of Comput. Engin.* 18(1) (2016), pp: 39–43.
6. Y. M. Wazery, S.G. Haridy and A.A. Ali," A hybrid technique based on RSA and data hiding for securing handwritten signature*", Int. J. Adv. Comput. Sci. Appl.* 12(4) (2021).
7. Q. S. Alsaffar, H. N. Mohaisen and F. N. Almashhdini, "An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image", *IOP Conf. Series Materials Sci. Engin.* 1058(1) (2021) 012048.
8. G. Ye, H. Wu, K. Jiao and D. Mei, "Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion", *Math. Biosci. Engin.* 18(5) (2021), pp:5427–5448.
9. S.A. Naji, H.N. Mohaisen, Q.S. Alsaffar and H.A. Jalab," Automatic region selection method to enhance imagebased steganography", *Period. Engin. Natural Sci.* 8(1) (2020), pp:67–78.
10. S. O. Alsharkasi, M. M. Elsheh and F. O. Ehtiba, "Evaluation of using steganography technique to hide a text in grayscale digital images", *J. Acad. Res. Appl. Sci.* 19 (2021), pp: 1–6.
11. M. O. Alsadeg Ali," Visual cryptography scheme for color images using Arnold mapping and modified RSA algorithm", M.Sc. Thesis, Sudan University of Science and Technology, 2018.
12. Hatem Nahi Mohaisen, Awad Kadhim Hammoud, "Application of modify RSA cryptography and randomly LSB steganography on color images of fluid flow in a channel*", Int. J. Nonlinear Anal. Appl.* 12 (2021) No. 2, 1725-1734,http://dx.doi.org/10.22075/ijnaa.2021.5312.
13. Awad Kadhim Hammoud, Hatem Nahi Mohaisen, Mohammed Q. Mohammed, "Secret information hiding in image randomly method using steganography and cryptography", *Int. J. Nonlinear Anal. Appl.* Volume 12, Special Issue, Winter and Spring 2021, 1283-1291 http://dx.doi.org/10.22075/ijnaa.2021.5644.
14. John K. Alhassan, Idris Ismaila, Victor O. Waziri, and Adamu Abdulkadir, "A Secure Method to Hide Confidential Data Using Cryptography and Steganography", International Conference on Information and Communication Technology and Its Applications (ICTA 2016).
15. Mritha Ramalingam, Nor Ashidi Mat Isa, R.Puviarasi, "A secured data hiding using affine transformation in video steganography*", Procedia Computer Science* 171 (2020), pp: 1147–1156.
16. Priya Mathur and Amit Kumar Gupta, "A Study of Data Hiding UsingCryptography and Steganography ", © Springer Nature Singapore Pte Ltd. 2020 D. Goyal et al. (eds.), Information Management and Machine Intelligence,Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-15-4936-6_1
17. Hawra'a Razzak Radhi and Majid Jabbar Jawad, "Combining A Cryptography and Steganography Techniques – Based Securing Transmitted Video Through Unsecure Channel", *Journal of University of Babylon for Pure and Applied Sciences,* Vol. (28), No. (3): 2020.
18. Madhan.S, Manimekala.M, Punithavallai.K andSuganya.V, "Efficient Data Hiding in Encrypted Video Using Cryptography", *IJCRT* Vol.(6), Issue 1 (2018).
19. Tohari Ahmad and Alek Nur Fatman," Improving the performance of histogram-based data hiding method in the video environment", *Journal of King Saud University – Computer and Information Sciences* 34 (2022), pp: 1362–1372.
20. Faten H. Mohammed," Robust video data security using hybrid cryptography-steganography technique", *Periodicals of Engineering and Natural Sciences* Vol. 8, No. 3,(2020), pp.1741-1751.
21. S. Manaseer, A. Aljawawdeh and D. Alsoudi," A new image steganography depending on reference and LSB", *Int. J. Appl. Engin. Res.* 12(9) (2017), pp: 1950–1955.
22. S. Asjad, "RSA Algorithm", University of South-Eastern Norway Campus Kongsberg, (2019).
23. F. Koeune, "Pseudo-Random Number Generator", In: H. C. A. van Tilborg (eds) Encyclopedia of Cryptography and Security Springer, Boston, MA, 2005.
24. D. Lehmer, "Mathematical methods in large-scale computing units", In: U. S. N. D. B. o. Ordnance and H. University (eds) Proceedings of the second symposium on large-scale digital computing machinery, Harvard University, 1951, pp:141–146.
25. K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El- Rabaie and G. M. El-Banby," High security data hiding using image cropping and LSB least significant bit steganography", *Colloq. Inf. Sci. Tech*. (2017), pp:400–404.
26. H.N. Mohaisen, "Secure data hiding technique using steganography and watermarking", M.SC. Thesis, College of Science, Baghdad University, 2016.