

8-15-2021

Hide Secret Script Encryption in Video Frames Based on Magic Square

Maisa'a Abid Khodher

a Computer science/ University of Technology-Iraq, Maisaa.a.Khodher@uotechnology.edu.iq

Follow this and additional works at: <https://qjps.researchcommons.org/home>

Recommended Citation

Khodher, Maisa'a Abid (2021) "Hide Secret Script Encryption in Video Frames Based on Magic Square," *Al-Qadisiyah Journal of Pure Science*: Vol. 26: No. 4, Article 50.

DOI: 10.29350/qjps.2021.26.4.1442

Available at: <https://qjps.researchcommons.org/home/vol26/iss4/50>

This Article is brought to you for free and open access by Al-Qadisiyah Journal of Pure Science. It has been accepted for inclusion in Al-Qadisiyah Journal of Pure Science by an authorized editor of Al-Qadisiyah Journal of Pure Science. For more information, please contact bassam.alfarhani@qu.edu.iq.



Hide Secret Script Encryption in Video Frames Based on Magic Square

<p>Authors Names a. Maisa'a Abid Ali Khodher</p> <p>Article History Received on:10/6/2021 Revised on: 24/8/2021 Accepted on: 30/8/2021</p> <p>Keywords: Hide texts, Cipherring, LSB, Frame of Vidium, Magic square.</p> <p>DOI: https://doi.org/10.29350/jops.2021.26.4.1442</p>	<p>ABSTRACT</p> <p>The objective of this article is to hide mystery encryption texts in vidiums using cipher method, that work is conceal big datum in frame of video. The fast of increased developments communication nets technologies. Thus, it can be suggested modern manner for conceal mystery texts that big size into frame of vidium efficiently, powerful and height capacity. This system depends on of three main steps: the first step: partition texts and cipherring in 2 caser methods, the second step: partition vidium to a collection of frames, and the final step: hide mystery texts in frame of vidium uses mystery key is magic square. The outcomes of system are excellent in conceal big text without sensible by attacker, through utilized the evaluation of system in each vidium frame in "PSNR, MSE, Entropy, Histogram, and correlation coefficient".</p>
---	--

1- Introduction

The technique of mystery telecommunication through embedding secure information at other source like as script, picture, sound, and video has called data hiding. Data hiding is the process of secret embed datum inside some original medias without alteration its sense by human eye. And became the Internet and original medias are more and more generic request of secure transmission of collection of information and increased [1].

The information hiding is methods of conceal secret letter/datum like as scripts, picture or picture in another exporter analogous picture or video, so is hidden to the undesirable persons [2].

The steganography is approach which is used to conceal the letter and prohibit the discovery of conceal letter. The video steganography is a new method of conceal data in a way that the unauthorized people cannot access the data [3].

In 2017. Youssef Bendraou, proposes an algorithm that aims to discover a sudden shot transition among sequential frames only through measurement the likeness. See the volume at vector contains spaces, in which modeled through a record ordinary distribution ago every values are positive.

Piecemeal shot transition concurrence is a harder job while comparing to cut off discovery. Generally, a piecemeal transition may share likeness advantages as a dynamical segment together cameras or object motions. This proposal is called Singular Value Decomposition (SVD). The SVD is an execution to this work features from the spatial area to the singular space. the outcome features are decreases and more accuracy, which makes the residual jobs is easy [4].

In 2017. Baharathi D. A., Anitha P., and Kiran S. M., Proposes for A high-security datum conceal method for chosen frames from video are cuts into 4 equal parts, a block of secure datum is concealing in every three channels. The frame division process. The divided process uses the LSB method int limited sequence and then the divided pictures are connected to fetch the stego picture/frame. This stego frame is substitute in video in original position. The studies a compared is performed among proposed method and existing techniques utilized vary metrics like as visualization exam, MSE, PSNR and CPU time. The outcome show that proposed method is more security comparison to the existing techniques [2].

In 2019. E. Hassan, S. Wessam M., and A. Yasmine, proposes two novel encrypting algorithms for security vidium transfer. The two algorithms employed vary kinds of chaotic maps to generated the key stream for encrypted the vidium frames. Both algorithms include an exchange stage and an alteration stage to realize confusion and spread requires of a security encrypted planed. For efficient transfer, the vidium file is compressed before encrypting. The executed of both algorithms, MPEG-2 criterion is utilized as a compressed method. Its utilizing MPEG-2 in executed because, it's simple and easiness of programming. and it yet find using in TV broadcasting, and it's using without loss in compressed to explain suggested schemes are public and that their secure is independent of the compressed method employed. [5].

In 2021. R. Vinay D, and J. Ananda Babu, proposes newly for data embedded in vidium sequences over the encrypted area. The video signal is encrypted utilizing chaos method who used multiple chaotic maps for encrypted. This proposal reversible video information hiding scheme (RVIHS) offers an innovative property that, at the decryption side and it can perfect extraction the data over together carrier vidium without any blurring. The results of proposed is used real time vidium for embedded the data. The outcomes of proposal work job get on better embedded capacity, comparing to existing methods [6].

- The contribution of proposed system, is hiding large text in video after partition the text, and applied the 2 caser method (repeat the caser method) for encryption text. and hide in video frames, without sensitive by attackers. It is using secret key for magic square to selected of location in each video frame. To conceal secure letter.

2. Video Frame

Video is the techniques that takes moves pictures electronically. These moves images are actually solely a series of static pictures that variation so rapid that it sees like the image is moves.

The video is complexed, but easy terms the lens of the camera concentrate picture into a sensor, and the sensor transform the picture into an electronically signal, and stocked on strip, disc, hard-drive, or memory-card [6].

The general method to constructing a vidims is via takes use of a shot structure, when shots are delimited via moves. Ago data on the moves is not ready in the vidimus form, automated shot border discovery has significant step in video management and retrieve device [7].

The Vidimus processing techniques has revolutionized the world of multimedia with production as like (DVD), (DSS), (HDTV), digital static, and Vidimus cameras. The various domain of Vidimus treatment contain: (1) Vidimus Compressed, (2) Vidimus Indexed, (3) Vidimus Segmented, and (4) Vidimus tracked etc [8], [9].

3. Steganography

The multimedia Steganography is the technique in which the science conceal connection; information hiding system so secret information is embedded in general multimedia so as not to outrage an eavesdropper's suspiciousness [10], [11]. Secure digital datum connection is constantly a worry. Cryptography and Steganography are the outstanding areas in secure digital datum connection. Through vision an innocent picture it is very hard to imagine that, the picture is doing the task of a messenger [11]. This section has provided steganography methods for data concealing that involved protected for applications versus revelation and protected versus deleted such as copyright protected for multimedia, watermarking, fingerprinting and datum embedded [12], [13].

4. Evaluation System

This section is offered number of evaluates, like mean square error (MSE), peak signal-to-noise ratio (PSNR), correlation, histogram, and entropy [14], [18].

4.1 MEAN SEQUAR ERROR

The equation (1) is used in the lower error value at the MSE in down:

$$MSE = \frac{\sum_{M \times N} [I1(M,N) - I2(M,N)]}{M \times N} \tag{1}$$

4.2 PEAK SIGNAL TO NOISE RATIO

The equation (2) is used in the computation of the PSNR in down:

$$PSNR = \frac{1 - \text{Log}_{10} R2}{MSE} \tag{2}$$

4.3 CORRELATION COEFFICIENT

The equation (3) is used the coefficient r can be calculated, the correlation coefficient r has the measure of the domain and direction of the linear set of 2 random variables (0,1). When the 2 variables are closely connected, when the correlation coefficient is near from the value of 1. When the coefficient is near from 0, the 2 variables are not related as follows [15]:

$$r = \frac{\sum_i (X_i - X_m)(Y_i - Y_m)}{\sum_i \sqrt{\sum_i (X_i - X_m)^2} \sqrt{\sum_i (Y_i - Y_m)^2}} \quad (3)$$

4.4 HISTOGRAM

An image histogram is a graph offers how many pixels there are at all scale or at all index for the indexed color image. The histogram contain data that are substantial in image equalization, when the image pixels are stretched for given a sensible contrast [16]. With the histogram, the equalization manner can improve. Equalization stretches the scale domain of the pixel level for the full domain to develop the dissimilarity of the given image. To uses this manner, the equalized new pixel value is redefined in equation (4) [16].

$$p(m \times n) = \frac{\text{number of pixels with scale level} \leq (m \times n)}{\text{Total number of pixels}} x (\text{maximum scale level}) \quad (4)$$

4.5- Entropy

The secure of a steganography system can be measured in terms of entropy. Let e_1, e_2, \dots, e_m be m possible elements with probabilities $P(e_1), P(e_2), \dots, P(e_m)$. The entropy values is given as:

$$H(e) = - \sum_{i=0}^{m-1} P(e_i) \log_2 P(e_i) \quad (5)$$

This equation output an estimate of the range of lower number of bits that is needed to encryption a series of bits on the basis of hesitation of symbol [17], [18].

5. Proposed System

In this article, the proposed system is used to conceal secret script encryption in video frames, Figure (1) is a flowchart for explaining the proposed algorithm that conceal secret message uses embedding algorithm, and extraction algorithm, as see in Figure (2).

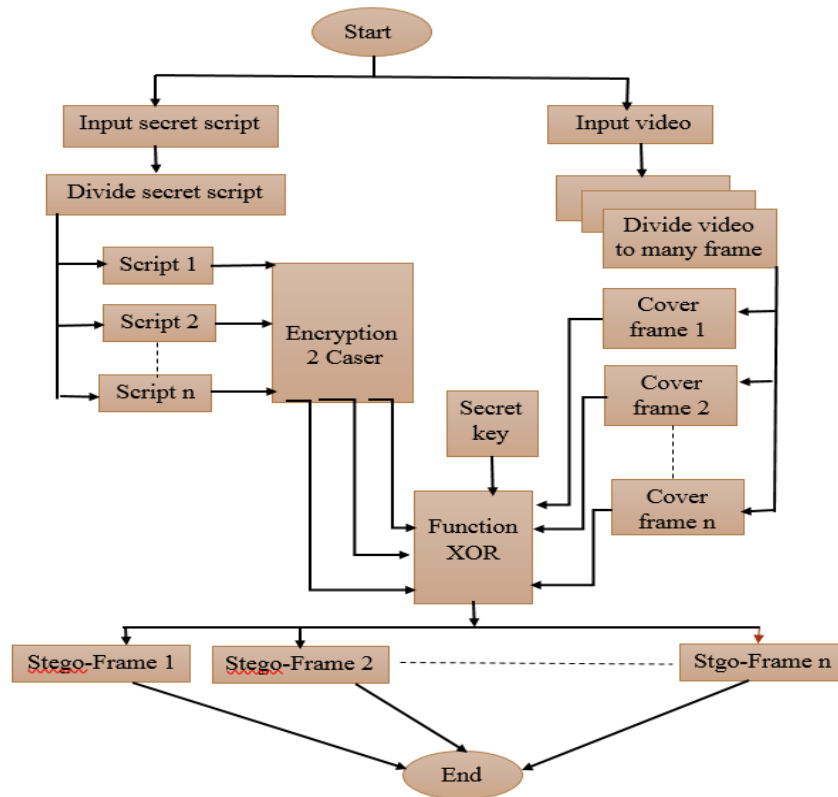


Figure (1): The embedded algorithm.

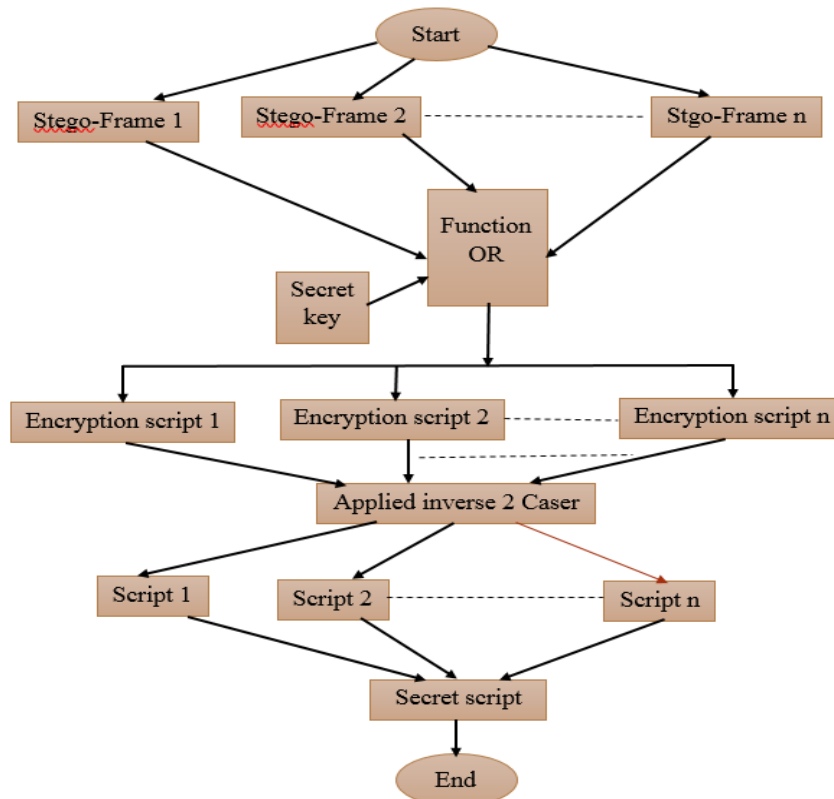


Figure (2): The extraction algorithm.

- This proposed system offers major three phases and two main algorithms in steganography script in video media, embedding and extraction algorithm.

A. The first phase: Partition texts and ciphering.

At this stage, the secret text is divided into small secret text, as each part, consist of 30 rows divided each 3 rows is a set of text, this page includes 10 sets. In the other hand each set is 3 rows, it can be hide in one video frame. The ten sets of rows secret texts (one page), are needed in ten video frames to be hidden. Whereas, the large video is including numbers of video frames can be hiding the large secret text.

Figure (3) explains dividing secret text, its applying 2 Caser method is becoming shift 6 each character in secret texts for encryption, such as example in Figure (4). It can be convert each encrypted character in each set of text to binary digit using ASCII. Each character represented eight bit in ASCII, as can be seen in Figure (5).

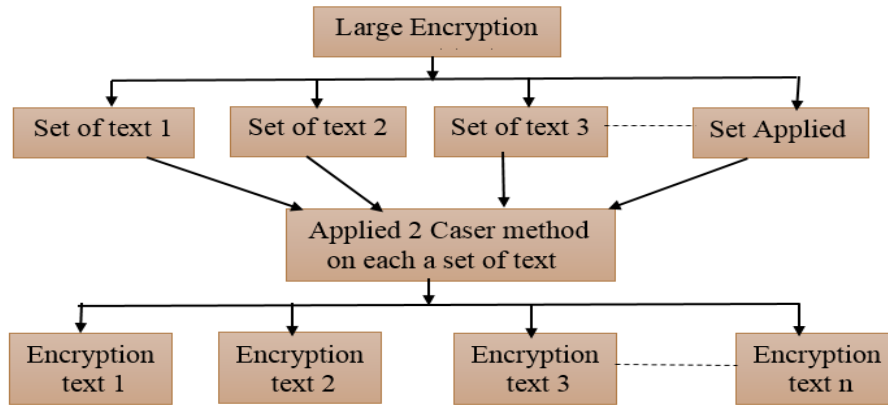


Figure (3): Encryption a set of text.

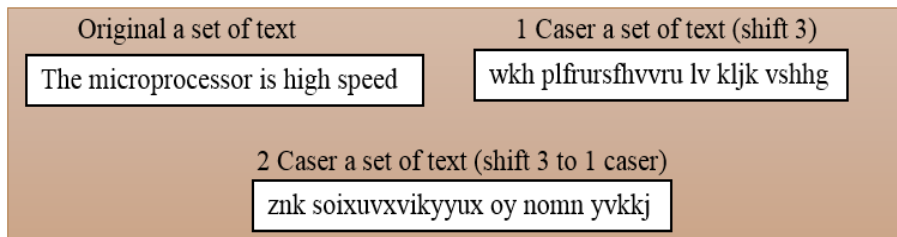


Figure (4): Encryption script.

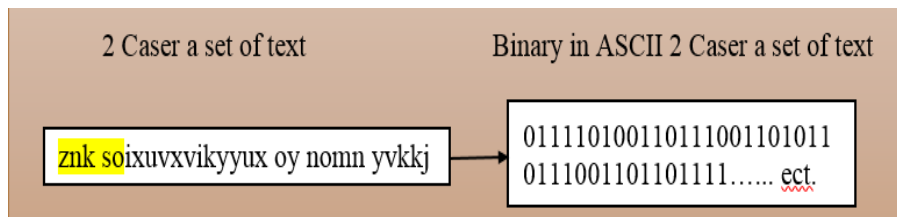


Figure (5): Binary Text in ASCII.

B. The second phase: Partition video to a collection of frames.

This phase works on dividing the video media to a set of frames the size of frame is 640×350 using matlab code to obtain a set of frames for conceal a set of secret texts in each

frame. In the other hand, it can be concealing each set of secret text (3 rows) into each of video frame, these video frames consider of cover media to transmission the secret text encrypted from sender to receiver, as see in Figure (6).

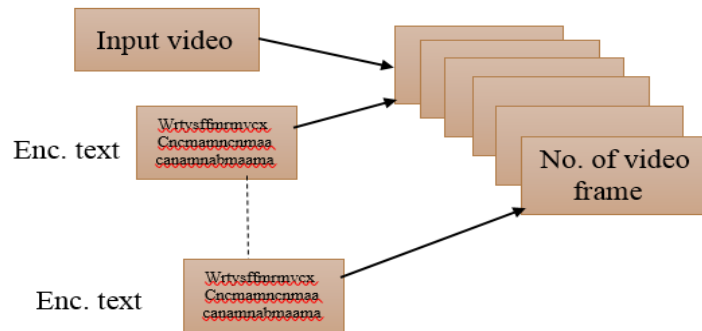


Figure (6): Set of video frame.

C. The final phase: Hide mystery texts in video frame.

In this phase is work to conceal secret texts by using the secret key, the secret key is magic square 4×4, is matrix 4×4 [16 2 3 13; 5 11 10 8; 9 7 6 12; 4 14 15 1], this matrix generates by matlab code each digit in magic square is define the locations inside video frame to conceal one-bit binary from secret text. Whereas the video frame is large size can be hide large size of text into this frame, the secret key as see in Figure (7).

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Figure (7): The secret key magic square 4×4.

The Figure (8) shown the operation of hide conceal secret text in in each one video frame using a secret key. whereas selection each digit from magic square considered one location in video frame to hide one-bit from secret text into vidiums frame, and its repeated this operation for a complete all bits to hide.

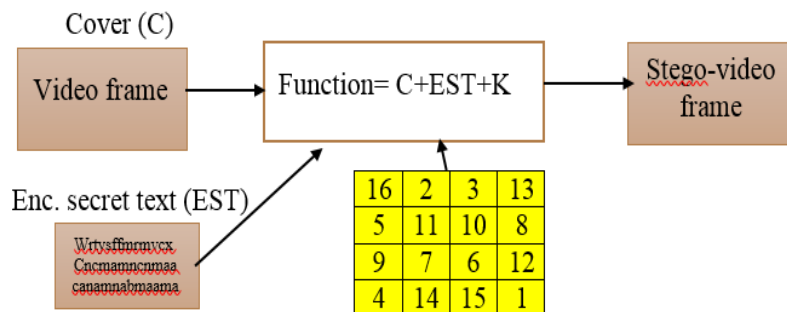


Figure (8): Conceal secret text in video frames.

Embedding Process

Embedding algorithm

Processing:

Inputs: vidiums frames, , secret text, secret key, 2 Caser.

Outputs: Stego- vidiums frame.

Initial:

A= Loaded vidiums.

B= Divide video in no. of frames.

C= Load secret text.

D= Load 2 Caser and convert to binary bit in ASCII.

E= Load secret key (magic square).

F= Found location of magic square in video frame.

G= stego-video frame.

Step 1: Load video in A.

Step 2: Divide video for no. of video frames in B.

Step 3: Load secur text and divide in 3 a row into set of text in C .

Step 4: Applied 2 Caser method on all secret text in each set of text in D.

Step 5: Selected locations of conceal secret text uses magic square (secret key) in E.

Step 6: Embed each binary set of text into video frames (cover) in LSB, by found location from magic square key in all video frames to obtain the stego-video frames in F.

Step 7: Results (put the stego-video frame) in G.

End

Extraction Process

Extraction algorithm

Processing:

Inputs: Stego- vidiums frames, secret key, Inverse 2 Caser.

Outputs: Secret text.

Initial:

A= Loaded stego-video frames.

B= Extracted encryption secret text from stego-video frames.

C= Loaded secret key (magic square).

D= Summation binary bit in a set of text.

E= Load inverse 2 Caser.

F= convert binary bit to characters.

G= Extracted secret text.

Step 1: Load stego-video frames in A.

Step 2: Extract encryption secret key (a set of text) from stego-video frame from the LSB in B.

Step 3: Find location from magic square (secret key) in each video frames in C.

Step 4: summation binary bit in all set of text in D

Step 5: Applied the inverse 2 Caser method in F.

Step 6: Convert the all binary bit to character eight bit in ASCII in F.

Step 7: Result (put the secret text) in G.

End

6.
Te
st
of
res
ult

Thi
s
sec
tio
n
dis
cus
ses
the
tes
t of
eac
h
res
ult

for the proposed system using conceal secret text encryption in video frames, the video frames and these frames considers cover media for transmitting secret text encryption between sender and receiver, without sensitive by attackers. The proposed system is good, efficiency, robustness, high capacity, and high security level, through tests each frame during applied a collection of evaluated such as MSE, PSNR, Entropy, Histogram, and correlation coefficient. Like as Table (1) shown the execution proposed system, Table (2) shown a set of evaluated in proposed system MSE, PSNR, Entropy, and correlation coefficient. The Table (3) shown the histogram among original video frame and stego-video frame, and Table (4) shown the detail of correlation coefficient.

Matlab code is used to analyses the PSNR and MSE and the result shows that when using frame's video is the same size 640×530 in all frames, the range of PSNR in original frame from 57.4906 to 98.2103, and the range of PSNR in stego frame from 57.5065 to 98.3116. The range of MSE in original frame from 36.7120 to 79.8409, and the range of Min stego frame from 36.6809 to 79.7803. The range of entropy in original frame from 6.9259 to 7.4440, and the range of entropy in stego frame from 6.9260 to 7.4441. The range of correlation coefficient in original frame from 0.9176 to 0.8550, the range of correlation coefficient in stego frame from 0.8991 to 0.8517.

Table (1): The execution of proposed system.









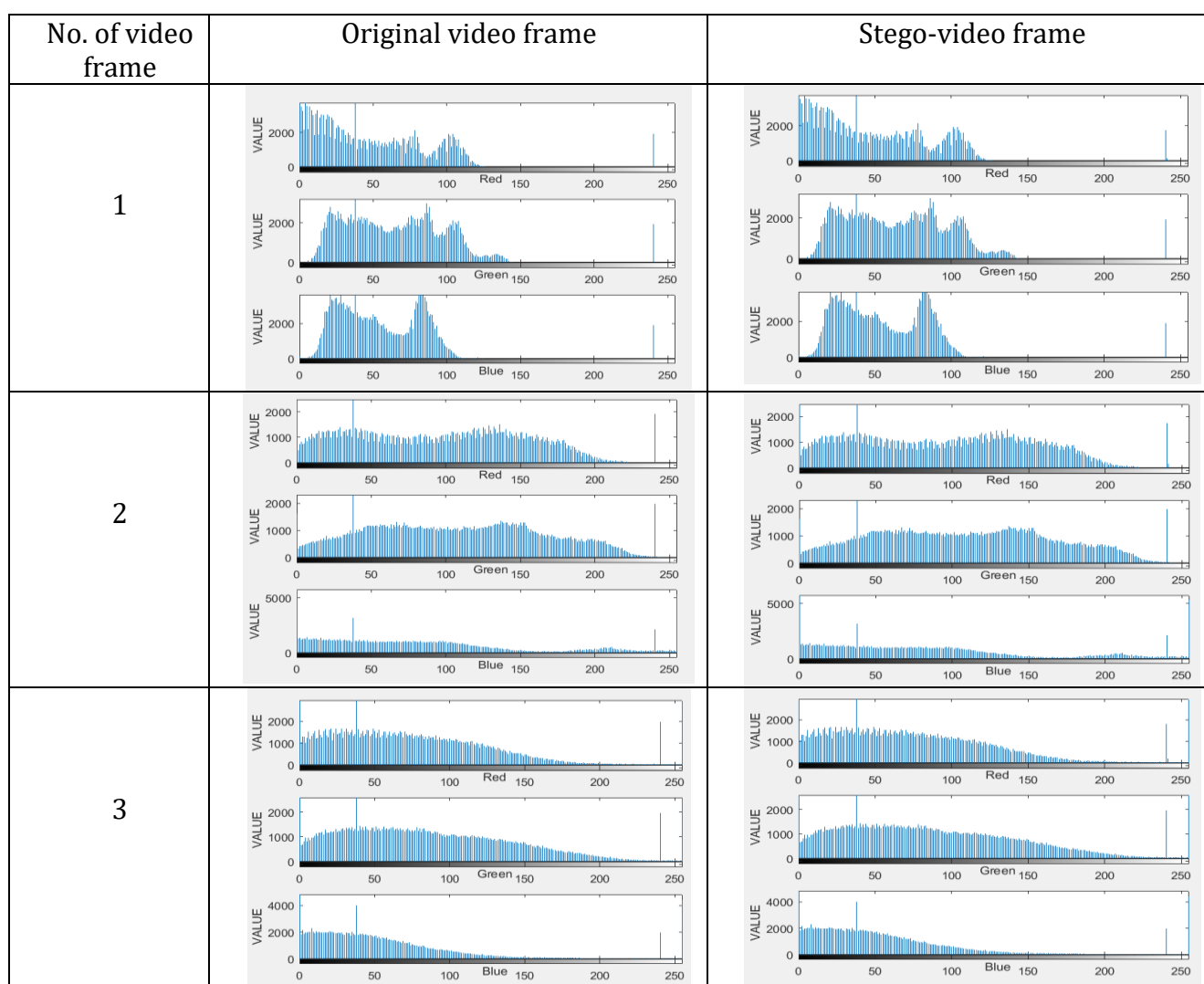
No. of video frame	Original video frame	Size of video frame	Stego-video frame
1		640×350	
2		640×350	
3		640×350	
4		640×350	

Table (2): The evaluated of PSNR, MSE, Entropy, Correlation coefficient.

Video frame Name of	PSNR	MSE	Entropy	Correlation coefficient
---------------------	------	-----	---------	-------------------------

1 Original video frame	57.4906	36.7120	6.9259	0.9176
1 Stego-video frame	57.5065	36.6809	6.9260	0.8991
2 Original video frame	87.6321	64.3384	7.7399	0.9683
2 Stego-video frame	87.6274	64.2981	7.7399	0.9683
3 Original video frame	95.6306	60.2380	7.4678	0.8385
3 Stego-video frame	95.6505	60.1876	7.4678	0.8473
4 Original video frame	98.2103	79.8409	7.4440	0.8550
4 Stego-video frame	98.3116	79.7803	7.4441	0.8517

Table (3) shown the histogram among original video frame and stego-video frame.



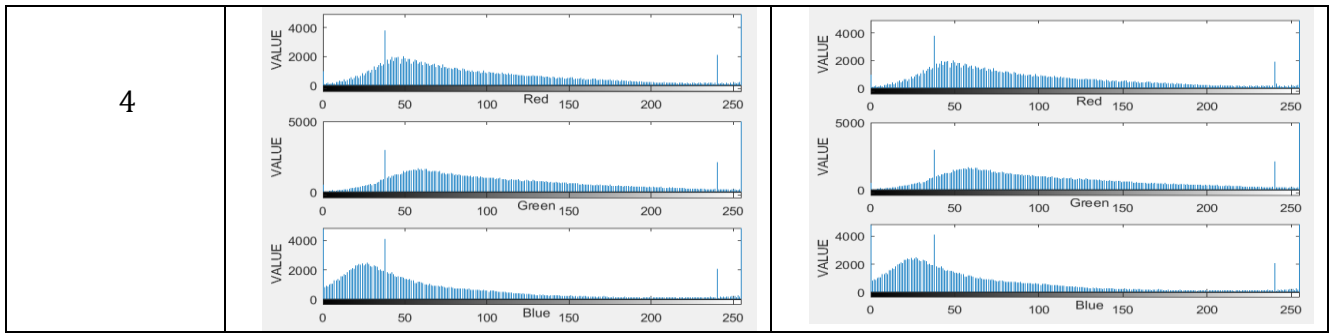
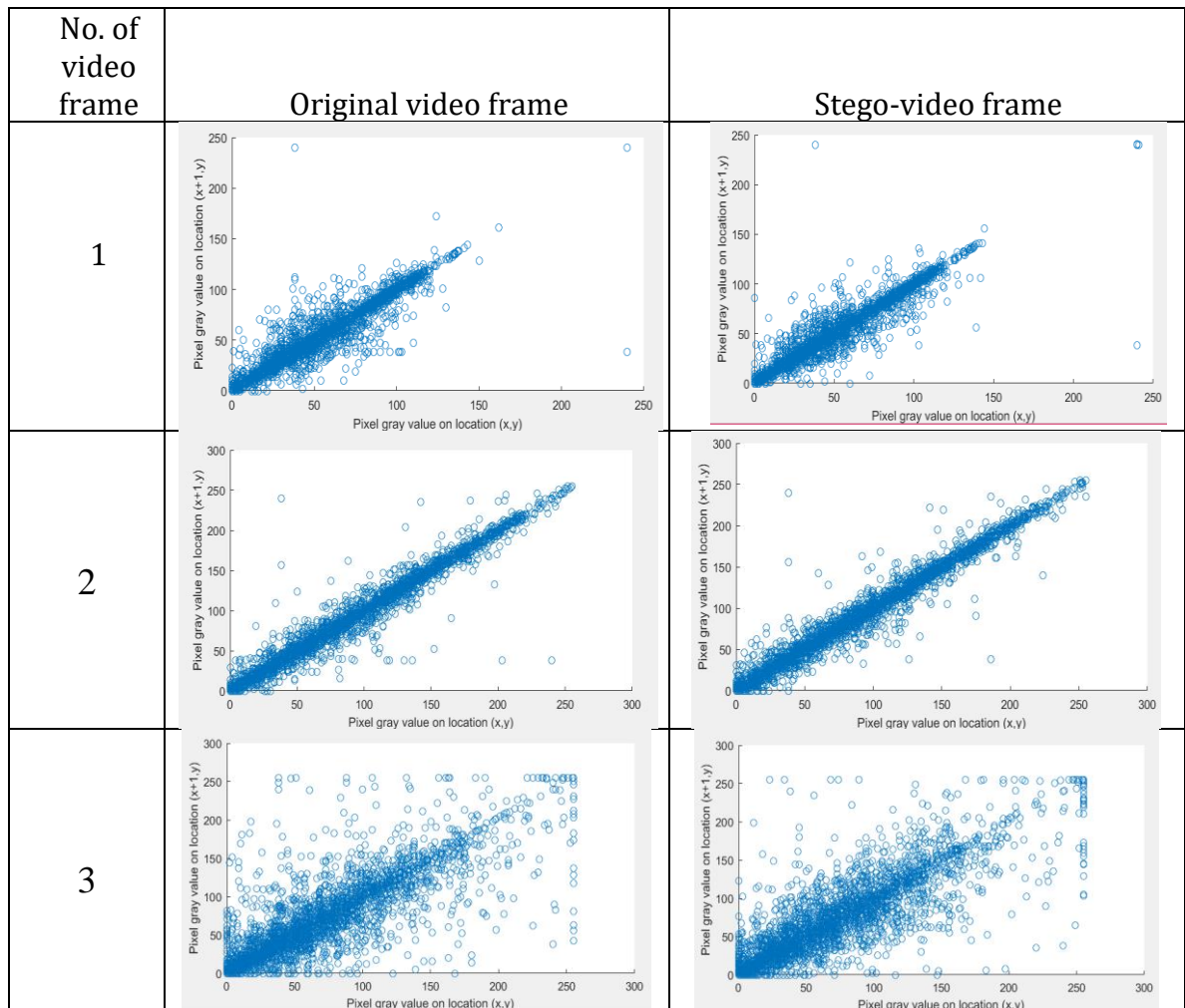
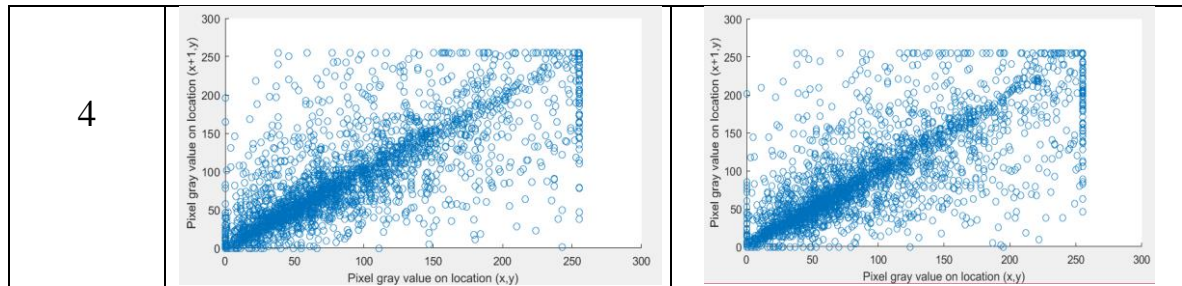


Table (4) shown the detail of correlation coefficient.





7. Conclusion

This article is offer the outcomes of the proposed system to conceal secret text into video media uses magic square to found location in each video frames. The proposed system has a good level of efficiency, robustness, capacity and high security without sensitive by attackers, through applying a collection of evaluated like as PSNR, MSE, Entropy, and correlation coefficient is good. The secret text is hidden. When conceal secret text, the PSNR are decreases, but the MSE are increases, and ranges of correlation coefficient among the 0 and 1, the ratio is good. And the capacity of system when hid 960 bit in video the ratio is 0.0044, hide 1920 bit in video the ratio is 0.0089, and hide 2880 bit in video the ratio is 0.013 this indicate system when hide number of bits in text is small denote the high security, when the number of bits in text is big denote low security, and also the histogram between the original frame and stego frame is similar, the attackers not detected existence secret message, this denote the proposed system is good.

References

- [1] T. Vandana, S. Monjul, Hiding Secret Image in Video, International Conference on Intelligent Systems and Signal Processing (ISSP), 2013 IEEE, pp 150-153.
- [2] D. A. Baharathi, P. Anitha, and S. M. Kiran, High-Security Data Hiding in Videos Using Multi Frame, Image Cropping, and LSB Algorithm, International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 3(3), 2017, pp 693-698.
- [3] S. Vaishali, T. Roshani, and G.Rajesh babu, Implementation on Hiding Data and Image in Audio Video Using Anti Forensics Technique, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3(9), 2015, pp 8159-8164. DOI: 10.15680/IJIRCCE.2015.0309037
- [4] B. Youssef, Video shot boundary detection and key-frame extraction using mathematical models, book, 2017.
- [5] E. Hassan, S. Wessam M., and A. Yasmine, New Video Encryption Schemes Based on Chaotic Maps, Image processing, IET, 14(2), October 2019, pp 1-16. DOI: 10.1049/iet-ipr.2018.5250
- [6] R. Vinay D, and J. Ananda Babu, A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS, I. J. Computer Network and Information Security, 2, 2021, pp 53-65. DOI: 10.5815/ijcnis.2021.02.05

[7] Z. Bin, Li. Xuelong, and Lu. Xiaoqiang, Video Captioning with Tube Features, Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), 13-19 July 2018, pp 1177-1183.

[8] G. Michael, and Ridiculously, Fast Shot Boundary Detection with Fully Convolutional Neural Networks, In 2018 International Conference on Content-Based Multimedia Indexing, CBMI 2018, La Rochelle, France, September 4-6, 2018, pp1-4. DOI: 10.1109/CBMI.2018.8516556

[9] Wu. Zuxuan, Y. Ting, Yanwei Fu, and Yu. Gang Jiang, Deep Learning for Video Classification and Captioning, Book, 22 Feb 2018, pp 3-400. arXiv:1609.06782v2 [cs.CV].

[10] O. Ismaeel, and I. Al-Farraji, New Technique of Steganography Based on Locations of LSB, International Journal of Information Research and Review, Vol. 04 (01), January 2017, pp.3549-3553.

[11] A. Kumar Sahu, and M. Sahu, Digital Image Steganography Techniques In Spatial Domain: A Study, International Journal of Pharmacy & Technology, Vol. 8 (4), Dec. 2016, pp 5205-5217.

[12] S. Pund-Dange, and C. G Desai, Data Hiding Technique Using Catalan-lucas Number Sequence, Indian Journal of Science and Technology, vol. 10 (4), 2017: pp 1-6.

[13] S. Aditya Kumar, and S. Monalisa, Multi-Bit Data Hiding Scheme for Compressing Secret Messages, Appl Sci, Vol. 5(4), 2015: pp 1033-1049.

[14] A. ALabaichi, K. Maisa'a Abid Ali Al-Dabbas, and S. Adnan, Image Steganography Using Least Significant Bit and Secret Map Techniques, International Journal of Electrical and Computer Engineering (TTECE). 2020 February ;10(1): pp 935-946.

[15] A. Aung M., LSB Based Image Steganography for Information Security System, International Journal of Trend in Scientific Research and Development (IJTSRD). 2018; 3(1): pp 394-400.

[16] Hashim M. H, Rahim M. S. M, Johi F. A, Taha M. S, Hamad H. S., Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats, (IJET).2018; 7 (4): pp 3505-3514.

[17] K. Maisa'a AA. Hide Secret Messages in Raster Images for Transmission to Satellites using a 2-D Wavelet Packet, Iraq journal of Science (IJS). 2018;59(2B): pp 922-933. DOI:10.24996/ijs.2018.59.2B.14

[18] Maisa'a Abid Ali K., and Shatha Habeeb Jaafer, Concealed Secret Letter Using a 2D Wavelet-Packet, Second International Conference Mathematic and Sciences June 31 August 6- 2018AIP Conference Proceedings 2086, 030007 (2019), 02 April 2019, pp 030007-1- 030007-4.