AUIQ Technical Engineering Science

Volume 1 | Issue 1 Article 2

2024

Video Steganography based on Sine Chaotic Map and Hamming Code

Marwa M Naji
Department of Techniques Communication Engineering, Engineering Technical College –Najaf (ETCN), AL Furat Al Awast Technical University(ATU), Kufa, Iraq, marwa.ms.etcn37@student.atu.edu.iq

Ahmad T Abdulsadda
Department of Electrical Engineering, Engineering Technical College –Najaf (ETCN), AL Furat Al Awast Technical University(ATU), Kufa, Iraq

Salim Muhsin Wadi
Department of Techniques Communication Engineering, Engineering Technical College –Najaf (ETCN), AL Furat Al Awast Technical University(ATU), Kufa, Iraq

Recommended Citation

Naji, Marwa M; Abdulsadda, Ahmad T; and Wadi, Salim Muhsin (2024) "Video Steganography based on Sine Chaotic Map and Hamming Code," *AUIQ Technical Engineering Science*: Vol. 1: Iss. 1, Article 2.
DOI: https://doi.org/10.70645/3078-3437.1001

AUIQ TECHNICAL ENGINEERING SCIENCE 2024;1:12–20

ORIGINAL STUDY

Video Steganography based on Sine Chaotic Map and Hamming Code

Marwa M Naji [a,*], Ahmad T Abdulsadda [b], Salim Muhsin Wadi [a]

[a] Department of Communication Techniques Engineering, Engineering Technical College—Najaf (ETCN), AL Furat Al Awast Technical University (ATU), Kufa, Iraq
[b] Department of Electrical Engineering, Engineering Technical College—Najaf (ETCN), AL Furat Al Awast Technical University (ATU), Kufa, Iraq

ABSTRACT

With the increase in internet usage, data exchange happens at a higher pace, but with this comes the risk of security breaches. Hackers often target data exchange, making security a top priority. To address this issue, steganography has proven to be an effective solution. It involves concealing confidential data behind seemingly innocuous cover files, making it less likely to be detected. In a recent paper, the use of Sine chaotic map was proposed as a way to enhance security. Chaotic maps are sensitive to initial values, non-linear, and non-periodic, making them ideal for encryption. The proposed method involves using a video as the cover file and an image as the secret data. The video is split into frames in YUV form, and the position of pixels is changed using the sine chaotic map. The hamming code is used to encrypt and embed the secret information in the frames, after applying the cycle shift. Using multiple encryption techniques before embedding secret data in the video increases the level of security and ensures that the information can be extracted from the stego video without any losses. The results of this method show that it is highly effective, as evidenced by the PSNR value of 78.23dB for the stego video with high value of hiding capacity and the SSIM of 0.99 between the cover video and stego video.

Keywords: Video steganograaghy, Sine chaotic map, Hamming code, Cycle shift, PSNR

1. Introduction

With the major revolution in the world of communications: messages, photos, and video sending have become a requirement of daily life for all segments of society. By increasing the internet and social media,data has been sent all over the world without interest with security level. There are various techniques to prevent highly sensitive data from being lost, tempered, or altered by hackers when it is sent across an unsafe environment [1].

Information hiding techniques are classified into watermarking and steganography. Watermarking is the technique used to hide watermarks like logos where these techniques are visible to the human visual system. On the other hand, steganography hides the secret information inside the cover medium (text, audio, image and video) which means not visible to the human visual system (it hides the existence of secret data). So, steganography protects the secret data on the cover, while, watermarking protects the intellectual property rights of the cover [2]. Steganography is not new, where it has been used for a long time in various ways, wherever it was transfer data by shaving the slave's head, invisible link waxes, and silks. The data hiding can be done in two domains: spatial and transform. In the spatial domain, the secret data embedded directly on the values cover pixels while, in the transform, the domain used transformation methods such as discrete wavelet transform (DWT), integer wavelet transform (IWT), and discrete cosine transform (DCT) (it

Received 11 May 2024; accepted 25 July 2024.
Available online 23 August 2024

* Corresponding author.
E-mail address: marwa.ms.etcn37@student.atu.edu.iq (M. M Naji).

https://doi.org/10.70645/3078-3437.1001

allows data to be hidden in(HVS) less sensitive areas, which are the high-frequency bands [HH, HL, LH, LL] where hiding in these bands provide high robustness while maintaining human visual system) [3]. Video steganography is the approach used to hide secret information in sequence of the video. The features in video steganography including high capacity and complex structure make them more preferable as cover compared with other types of covers such as image, sound, and text. The main characteristics of any steganography method are security, robustness, hiding capacity, and imperceptibility [4].

Cryptography is used to encrypt secret information by transferring it to an unknown shape using several techniques [5]. Generally, the image encryption technique is one of the famous technologies used to keep data secret [6–8]. Chaotic map techniques were one of the new techniques used in cryptography which classified into (logistic maps, sine chaotic maps, Arnold cat maps, Tent maps, Henon maps, and else) The advantages of this maps include sensitivity to the initial value,non-periodic and non linear [9].

Xing-Yuan Wang et al. (2015) proposed a novel image encryption by applying the cycle shift on the bits of pixels to scramble the secret image by the keys which were produced by a chaotic map where the simulation experiments indicate the proposed scheme is able to resist the attack [10].

Behzad Yosefnezhad Irani et al. (2019) for the encryption and scrambling processes, a novel one-dimensional chaotic map known as the chaotic coupled Sine map (CCSM) proposed in this study. The goal of the CCSM design is to make the key space more secure in comparison to simpler maps like the sine and logistic maps [11].

Milad Yousefi Valandar, et al. (2019) presented image steganography based on integer wavelet transform where to split into four regions select LL, and use a 3D sine chaotic map to increase the security and the quality [12].

Mustafa K. 2021 suggests high sensitivity and a higher level of chaotic map to (higher efficiency of Lyapunov exponent, complexity and more chaotic and the proposed algorithm gives efficient and fast encryption by using 1D-ILM and 1D-IQM to improve image encryption system and the encryption time is decreased compared with another method [13].

Donghan Li et al. (2022) presented a new exponential chaotic enhancer (one-dimensional exponential chaotic map Enhancer 1D-ECE) that solves the problem of insufficient chaos and designed the zigzag transform performed on indexes of the matrix elements after blocking and flipping and achieved to high secure and can resist the attackers [14].

In the last few years several steganography schemes that used digital multimedia as a means of transferring data, video is one of the most popular because of its wide applications in both portable storage devices and the internet. Nirmalya Kar, et al. (2017) proposed a new idea where select a video type (AVI), use NLFSR (nonlinear feedback shift register) to select a frame randomly and hide (3bits) from data in the red channel, (3bits) in the green channel and (2bits) from data in the blue channel. Among the results were quality, hidden capacity, and robustness are acceptable [15].

Widad Muhammad et al. (2020) This study aims to encrypt messages using the RSA encryption method and then hide them in video files using the LSB method. Four different types of messages with varying sizes will be tested. All messages encrypted and embedded in the video and the resultes evaluated the MSE, PSNR, and Histogram methods to determine the most accurate and secure results. By using this approach, the authenticity of messages is guaranteed, and the risk of message leakage is reduced [16]. Tanveer et al. (2021) proposed a method to hide the logo image after encrypting it by Arnold's cat map then embedded in the frames selected by the logistic map and the embedding process occurs in the middle band DCT [17].

Ashwak Alabaichi and Ammar Altamemey in 2022 this paper presents a novel technique for encrypting secret messages using DNA and a 3D chaotic map in video frames, implemented via the raster method. The proposed technique comprises of three steps. Firstly, the video frames are converted into raster to extract features from each frame. Secondly, the secret messages are encrypted using encoded forms of DNA bases, inverse/inverse complements of DNA, and 3D chaotic maps. Thirdly, the encrypted messages are hidden in the raster video frame using a secret key in the four corners of each video frame. This technique is capable of hiding large amounts of secret data due to the large size of the video frame, which accepts any message size. The outcomes of the proposed technique are efficient, robust, highly secure, and can tolerate high capacity [18].

Kumar Sudha V. proposed a video steganography method in 2022 that uses chaos to provide three layers of security. The method involves hiding sent data in the spatial domain of frames using CVF (Cover Video Frames). Private information is encrypted and randomly hidden within the CVF's encrypted spaces. The video frames are modified, and the private information is supplied by PO (Payload Owner) to provide the initial layer of defense. The second and third layers of security are provided by selecting CVFs through FS (Frame Selector) for Embedding. Another study [19].

Ahmed T Abdulsada et al. in 2022 the proposed technique begins by identifying corner points within image frames using the Shi-Tomasi technique. It then utilizes the 3-LSBs technique to conceal sensitive information within these identified corner points. Moreover, to enhance security, the proposed method encrypts the sensitive data using the AES cipher method before embedding it The proposed method outperforms those based on lack of visual imperceptibility, providing an average PSNR of 57.57 dB while maintaining high embedding capacities [20].

Mithal Hadi Jebur et al. in 2023 presented a method for hiding an image of a moving object in frames of a cover video by separating the objects from the background of the frame and using the XOR technique to embed the bits of the detected object and reserved bits [21].

This paper aims to conceal data in a cover medium to prevent attackers from accessing secure data. It helps protect personal photos and important data. The study combines steganography and cryptography, which involve concealing secret data in video frames after encrypting them using various techniques. The cover frames are scrambled using a chaotic map before embedding them to achieve high imperceptibility and hiding capacity. The results of parameters such as PSNR, MSE, and hiding capacity demonstrate the success of this approach by showing that increasing imperceptibility in the video and the storage capacity is high, which means the quality of the stegovideo is high. The paper is structured as follows: Section 2 presents the proposed video steganography method; Section 3 presents the experimental results and performance evaluation of the proposed algorithm; Section 4 shows the performance of the approach and comparison with other methods; and Section 5 presents the conclusions of the proposed method.

2. The proposed video steganography method

In this paper,combine steganography and cryptography where our algorithm uses an uncompressed video stream comprised of frames as still images as a cover. Initially, the video stream is divided into frames, and the color space of each frame is converted to YUV, which eliminates the relationship between Green, Blue, and Red colors. The luminance (Y) component contains brightness data, while the color parts are less sensitive to human vision. Therefore, the chrominance (color portions) can be subsampled in the video sequence, and the discarded data will not affect the image quality. To increase important data security, video frames are scrambled with a sine chaotic map to change the position of pixels for frames. The secret information used is a binary image that goes through several encryption techniques, including the Cycle Shift, and Hamming code, to embed the data inside the video frames and obtain a stego video. Finally, the information is extracted from the stego video during decoding (at receiving side).

2.1. Frames of video preprocess

This research paper employs a preprocessing technique before the embedding process of the proposed method by using a Sine chaotic map. A chaotic map is a well-known theory that has numerous applications in fields such as physics, biology, engineering, and economics. The theory's sensitivity and behavior are determined by initial conditions and control parameters. Generally, using chaotic maps helps explain how dynamical systems behave [22]. Recently, many chaotic maps, including hyper-chaotic and quantum-based maps, have been generalized. A sine chaotic map is a simple map that resembles the logistic map. This map is determined by the equation below [23]:

$$X_{n+1} = b\sin(\pi x_n) \tag{1}$$

where xn is the initial state and b control parameter then X(n + 1) represents the next state, Eq. (1) modifies by changing the value of (pi) and replacing it with a variable β as shown in Eq. (2). To increase the system's chaos and complexity and ensure a high level of security for the algorithm, For this purpose, β is set to 0.3, as shown below:

$$X_{n+1} = b\sin(\beta x_n) \tag{2}$$

where $b < 0$. Assume initial condition $x_0 = 0.1$, b varies from 0 to 4 with step size 0.02. The lyapunov exponents and bifurcation diagram of the system are shown in Fig. 5.

2.2. Encryption of secret data

In this section, explain the stages that confidential data goes through before embedding it in the cover video where encrypted by several techniques to increase the secure of the proposed method.

2.2.1. Cycle shift

This operation can be change the pixel value effectively where it is asymmetric and reversible for decryption process. Therefore, this paper used cycle shift to scramble the information of image and change the bit-level pixel values [10]. A large binary number

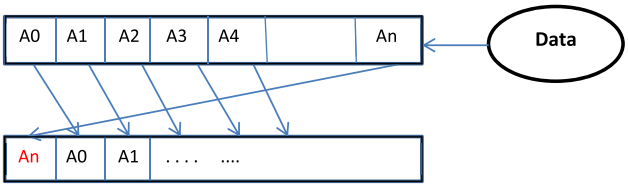


Fig. 1. Explain about cycle shift for one time.

is represented by a string A of size N and comprises of 0's and 1's, which cycly shifted. The cycle shift operation is defined as follows:

If the string A is [A0, A1, A2, ..., An], then after performing one cycle shift, the string becomes[A1, A2, A3, ... An, A0] maybe perform the shift infinite number of times.As shown figure below.

2.2.2. Hamming code

Hamming code is a well-known algorithm used for encryption and single-bit error detection and correction. The method works by adding redundancy bits to data bits to create a code word of length n bits [24]. In this research, used the hamming (7,4) code where 7 represents the codeword result, 4 bits represent the data bits, and 3 bits are added to the data, called redundancy bits. The resulting codeword transmitted is (RRDRDDD), where R refers to the redundancy bits that are calculated and arranged in locations 1, 2, 3, and 4 as shown in Fig. 2. Since Hamming codes are linear, they require two matrices: the generator matrix G for encoding used in sending part and the parity-check matrix H for decoding using in receiving part. To encode the data bits D, we multiply them(data bits) by the generator matrix and take the resultant modulo of 2. The outcome is the 7-bit codeword M, which is prepared for transmission through a busy channel. The Eq. (3) to calculate the code word.

$$M = D * G \tag{3}$$

where the generator matrix is:

$$\mathrm{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{4}$$

In the reception of the data will be received M (data + redundancy) bits in order to verify the encoded message of seven bits. It will then be multiplied by the transpose of the parity - check matrix as shown in equation below.

$$\mathrm{S} = \mathrm{M}^{*} H^{T} \tag{5}$$

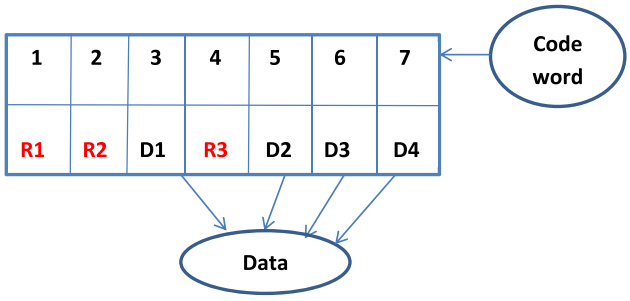


Fig. 2. The codeword contain from the Data bits and redundancy bits.

where the parity-check matrix:

$$H^{T} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \tag{6}$$

The end product is a three-bit syndrome vector S (s1, s2, s3), all of which must be zeros (000) in order for the message to be error-free. If not, any modification to the message while it is being transmitted will cause one or more of the message's pieces to be flipped; after that, it requires a procedure for fixing errors.

2.3. Embedding process

The proposed method involves hiding data within a video. Secret data is first encrypted using techniques such as the RSA technique, cycle shift, and Hamming code as mentioned in the previous section. The encrypted data obtained from the Hamming code, which is a 7-bit code word, is then hidden within the least significant bits (LSB) of selected pixels from frames Y, U, and V. Three bits are hidden in frame Y, two bits in frame U and two bits in frame V. The frames are then unscrambled from Sine chaotic map and combined to obtain the stego video, as shown in the Fig. 3.

2.4. Extraction process

The proposed method for extracting information from a stego video involves several steps. First, the stego video is split into frames in the RGB format. Next, the frames are converted into the Y, U, and V format and encrypted using the sine chaotic map with a specific key. Then, the Hamming code on the message is decoded, and a cyclic shift is applied to

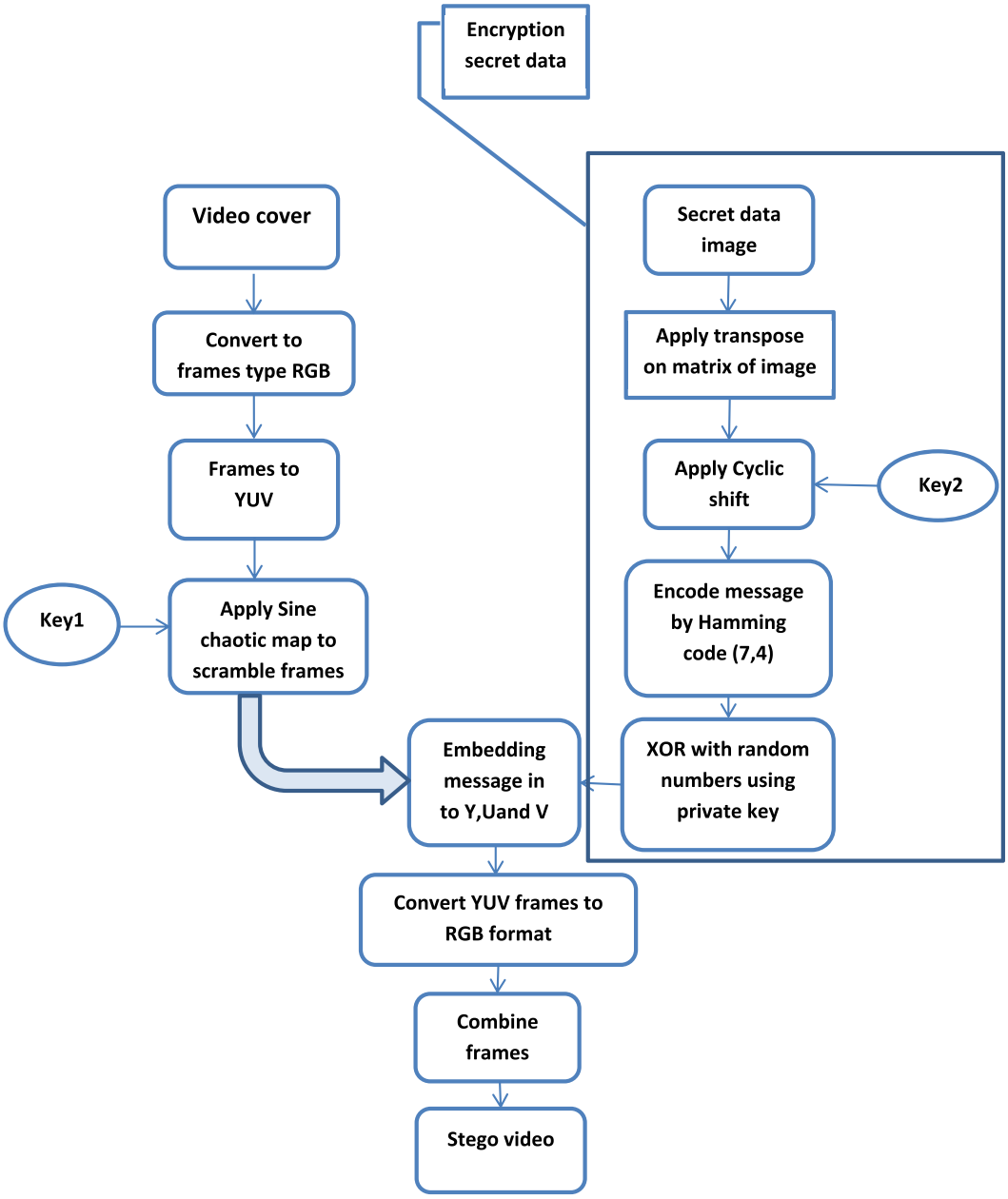


Fig. 3. Flow chart of the embedding process.

the pixels of the image using another specific key. The final step is to extract the image from the stego video. Fig. 4 shows all the steps required to extract the message.

3. Experimental results

In this section, will evaluate the performance of the suggested algorithm in terms of impercibility,hiding ratio, payload and histogram analysis. To implement the presented method, used a personal laptop with 8 GB RAM, a solid-state drive (SSD), and Windows 10 Pro. The simulation language used was MATLAB 2021A software. will verify the impercibility performance by calculating its parameters such as PSNR, SSIM,MSE as shown below.

3.1. Imperceptibility

One of the important factors used to measure the hiding algorithms performance was stego quality. The imperceptibility was used to measure the stego video quality after concealing the secure data within

Table 1. The PSNR value in (dB) for cover video's channels(YUV).

Cover video	PSNR (Y)	PSNR (U)	PSNR (V)
Akiyo	76.32	75.64	76.64
News	71.87	72.53	74.65
Foreman	78.23	77.05	78.01
Bridge far	77.42	78.22	78.43

through several factors such as PSNR, SSIM, and MSE as shown in below.

3.1.1. Peak Signal to Noise Ratio (PSNR) and (MSE)

The simplest and most widely used indicator of perceptual similarity between original video frames and stego video frames is the peak signal to noise ratio, which is calculated by the Eq. (7) below and measure in decibels [25], Where max f_c is the maximum value of the cover video frames,and MSE is the mean square error is calculated by comparing each byte in the stego and cover files. It measures the squared difference between the evaluated and appraised attributes defined by the Eq. (8) below; Where vc is the cover video frame,and vs is the stego video frame, while $M * N$ is the size of the cover video frame. The Table 1 demonstrated the values of peak signal to noise ratio for several videos.

$$\text{PSNR} = 10 \log_{10} \left(\frac{\max fc^2}{MSE} \right) \tag{7}$$

$$\text{MSE} = \frac{1}{M * N} \sum_{i=1}^{m} \sum_{j=1}^{n} [vc(i, j) - vs(i, j)]^2 \tag{8}$$

3.1.2. The Structural Similarity (SSIM)

This approach used to measure the similarity between the cover video frame before embedding and the stego video frame, and used to contrast the structure and brightness of the cover video and stego video frames [25]. The SSIM is calculated by the Eq. (9):

$$\text{SSIM} = \frac{(2\mu x\mu y + c1)(2\sigma xy + c2)}{(\mu x^2 + \mu y^2 + c1)(\sigma x^2 + \sigma y^2 + c2)} \tag{9}$$

where C1 and C2 are the factors that stabilize the division when the denominator is weak and $\sigma x, \sigma y$ are the main intensities of x and y. μx, μy are the averages of x and y. The variances of x and y are σx^2 and σy^2, σxy is the co-variance of x and y, sequentially.

3.2. Hiding ratio and payload

The percentage of space in the cover frame that can be used to embed secret data is known as the hiding ratio, In other words, the hiding ratio is measured as the ratio of secret data to the size of the carrier data and The higher the hiding ratio, the more secret data you can hide within the carrier data. The hiding ratio can be computed using the following formula:

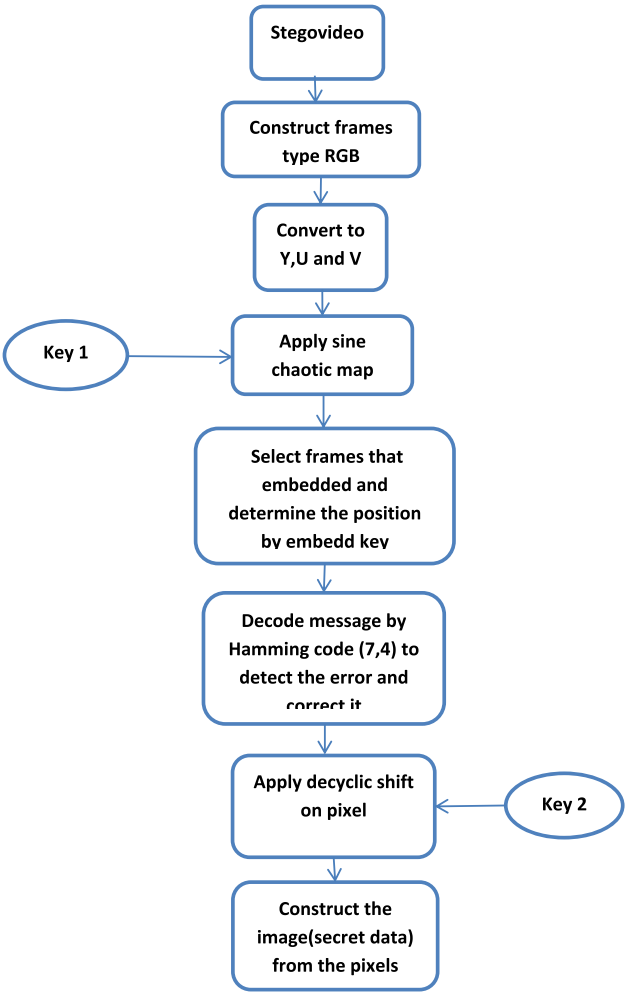


Fig. 4. Extraction of the secret data (image).

$$\text{HR} = \frac{\text{size of secret data}}{\text{size of cover video}} \tag{10}$$

And The maximum number of bits allotted for encoding the secret data within the cover frame is represented by the payload, which is determined in terms of bits per pixel using the Eq. (11) that follows (bpp) [26]. Where $\|S\|$ indicates how many secret bits are going to be inserted into the cover frame. The height and width of the cover frames are M and N

$$P = \frac{\|S\|}{M * N} \tag{11}$$

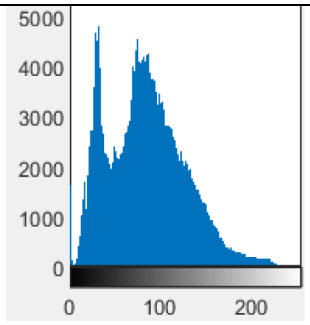
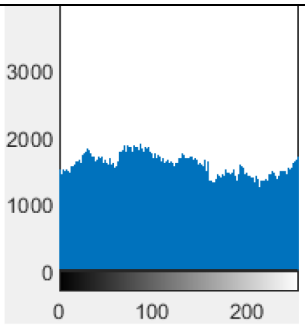
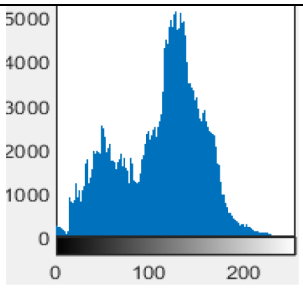
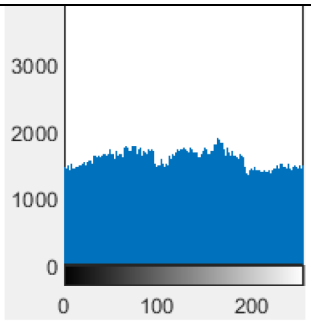
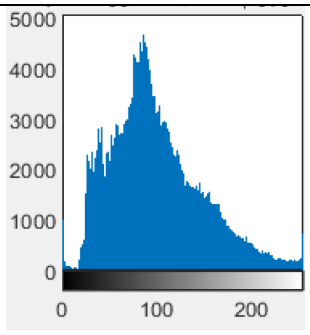
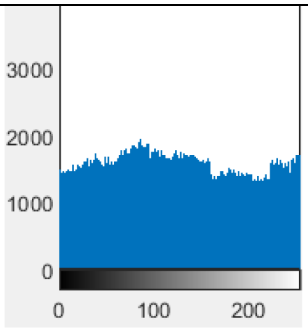
Cover video frames		Histogram of the cover frame before scrambling	Histogram of the cover after scrambling
RGB color frame size of (640x480)	Y		
	U		
	V		

Fig. 5. The histogram analysis for the cover frames.

3.3. Histogram analysis

One popular tool for examining video frame pixels is the histogram, which shows the intensity value range for each video frame used in video steganography to calculate the destruction of color channels by looking at the intensity of the frames' pixels and also shows the statistical information of video frames after the embedding process .in this section we represent the histogram for every channels of cover video frames after and before scrambling with sine chaotic map [27] as showen in Fig. 5.

3.4. Chaotic behaviour

3.4.1. Lyapunov exponent and bifurication diagram

Lyapunov exponent and bifurication diagram show the chaotic behavior of the presented map where the LE is give the average rate of separation between trajectories that begin from two very near initial states,when LE is positive that mean a dynamical system is chaotic and the larger value of LE prove the map more complex behavior but the negative value of LE indicate to the dynamical system is stable .bifurication diagram accurately characterizes the system's

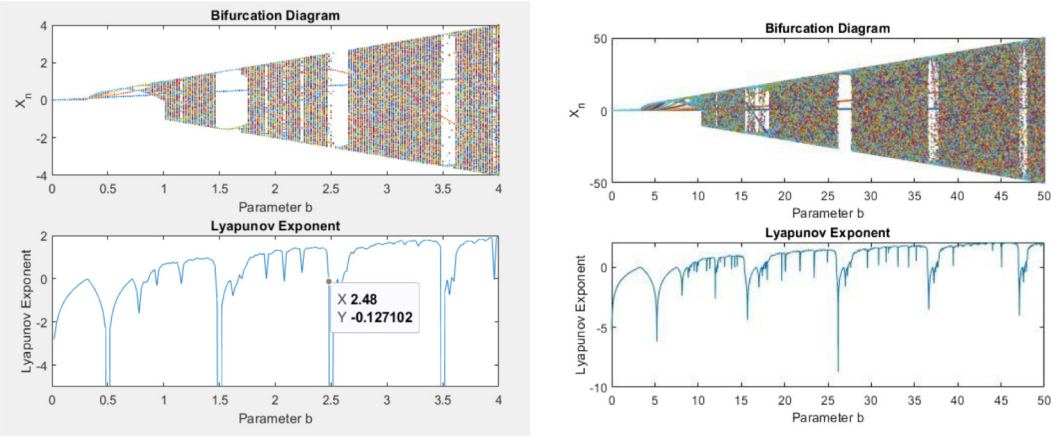


Fig. 6. Chaotic behaviors of the sine chaotic (bifurication diagram and lyapunov exponent) a) sine chaiotic b) Modify sine chaiotic.

Table 2. Comparison of the PSNR and SSIM value between the proposed method and other methodes.

Method	PSNR(dB)	MSE	SSIM
[12]	53.7294	–	0.999
[19]	52.28 to 62.05	–	–
[29]	34.81	–	0.96
[25]	61.44	–	–
[30]	32.79	–	0.920
Proposed method	78.2375	0.00097	0.9974

Table 3. Comparison of the payload and hiding ratio (HR) between the proposed method and other methodes.

Method	Payload	HR
[29]	0.45	–
[19]	2.25	28.25
[27]	2	25%
Proposed method	0.072	0.99

chaotic state and calculated by the Eq. (12) [28].

$$\lambda = \lim_{n\to\infty}\left(\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f^{'}(xi)\right|\right) \tag{12}$$

4. Comparison with other approaches

This section explains the results obtained from the proposed method. It compares it with other methods explaining the values for PSNR, MSE, and SSIM which give high values from other methods so improved the impercibility for the stego video is higher as illustrated in Tables 2 and 3 and the hiding ratio for the cover video is large where can embed a large amount of data in video.and the similarity between the cover video and stego video is large.

5. Conclusion

In this paper, discuss the importance of data security in the context of the increasing use of the internet. With the growing exchange of data, the risk of data breaches has become a major concern. To address this issue, steganography has emerged as an effective solution. Steganography involves concealing confidential data behind an apparently harmless cover file, making its presence difficult to detect. A recent paper proposed the use of the Sine chaotic map as a way to enhance security. Chaotic maps are sensitive to initial values, non-linear, and non-periodic, making them ideal for encryption. The proposed method involves using a video as the cover file and an image as the secret data. The video is split into frames in YUV form, and the position of pixels is changed using the sine chaotic map. The hamming code is used to encrypt and embed the secret information in the frames, after applying the cycle shift. Using multiple encryption techniques before embedding secret data in the video increases the level of security and ensures that the information can be extracted from the stego video without any losses. The results of this method show that imperceptibility increased with hiding capacity increased too, as evidenced by the PSNR value of 78.23dB for the stego video and the SSIM of 0.99 between the cover video and stego video then the hiding capacity equal to (0.99).

Acknowledgments

We are grateful to the College of Communication Technical Engineering Najaf of the University Al Furat Al-Awsat Technical for providing resources that enhanced the quality of my research.

Conflicts of interest

The author declares no conflict of interest.

References

1. A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–52, 2010.
2. P. Pareek and N. Monica, "An overview of steganography: data hiding technique," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 1. pp. 87–89, 2020.
3. M. Y. Valandar, P. Ayubi, M. J. Barani, and B. Y. Irani, "A chaotic video steganography technique for carrying different types of secret messages," *Journal of Information Security and Applications*, vol. 66, pp. 103160, 2022.
4. J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: recent advances and challenges," *Multimedia Tools and Applications*, pp. 1–43, 2023, doi: https://doi.org/10.1007/s11042-023-14844-w.
5. A. Gupta and N. K. Walia, "Cryptography algorithms: a review," *International Journal of Engineering Development and Research*, vol. 2, no. 2, p. 146, 2014.
6. A. A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," *Optik*, vol. 261, p. 169122, 2022.
7. U. Zia, M. McCartney, B. Scotney, J. Martinez, M. Abu-Tair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, 2022.
8. K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps," *Pattern Recognition Letters*. vol. 152, pp. 356–64, 2021.
9. R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Annals of Data Science*, vol. 11, no. 1, pp. 1–26, 2024.
10. X. Y. Wang, S. X. Gu, and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, pp. 126–34, 2015.
11. B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled Sine map," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2693–721, 2019.
12. M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 9971–89, 2019.
13. M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. M. Al-Jubari, "Designing 1D chaotic maps for fast chaotic image encryption," *Electronics*, vol. 10, no. 17, p. 2116, 2021.
14. D. Li, J. Li, and X. Di, "A novel exponential one-dimensional chaotic map enhancer and its application in an image encryption scheme using modified ZigZag transform," *Journal of Information Security and Applications*, vol. 69, p. 103304, 2022.
15. N. Kar, M. A. Aman, K. Mandal, and B. Bhattacharya, "Chaos-based video steganography," In: *2017 8th International Conference on Information Technology (ICIT)* 2017 May 17 (pp. 482–487). IEEE.
16. W. Muhammad, D. H. Sulaksono, and S. Agustini, "Message security using Rivest-Shamir-Adleman cryptography and least significant bit steganography with video platform," *International Journal of Artificial Intelligence & Robotics (IJAIR)*, vol. 2, no. 2, pp. 52–61, 2020.
17. T. J. Siddiqui and A. Khare, "Chaos-based video steganography method in discrete cosine transform domain," *International Journal of Image and Graphics*, vol. 21, no. 2, p. 2150015, 2021.
18. M. AA. Khoder, A. Alabaichi, and A. A. Altameemi, "Steganography encryption secret message in video raster using DNA and chaotic map," *Iraqi Journal of Science*, vol. 63, no. 22, pp. 5534–5548, 2022.
19. D. Kumar and V. K. Sudha, "Efficient three layer secured adaptive video steganography method using chaotic dynamic systems".
20. A. Taha, F. A. Hameed, and S. Wadi, "Video steganography using a hybrid scheme," *NeuroQuantology*, vol. 20, no. 8, pp. 8764–8784, 2022.
21. M. H. Jebur, F. A. Joda, and M. A. Naser, "Video steganography technique based on enhanced moving objects detection method," *Journal of University of Babylon for Pure and Applied Sciences*, vol. 31, no. 2, pp. 270–95, 2023.
22. N. Kar, M. D. AAA. Aman, K. Mandal, and B. Bhattacharya, "Chaos-based video steganography," *2017 8th International Conference on Information Technology (ICIT)*. IEEE, 2017.
23. C. Dong, K. Rajagopal, S. He, S. Jafari, and K. Sun, "Chaotification of sine-series maps based on the internal perturbation model," *Results in Physics*, vol. 31, p. 105010, 2021.
24. A. K. Singh, "Error detection and correction by hamming code," In: *2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*, pp. 35–37. IEEE, 2016.
25. R. J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, "A new video steganography scheme based on Shi-Tomasi corner detector," *IEEE Access*, vol. 8, pp. 161825–161837, 2020.
26. R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "Video steganography techniques: taxonomy, challenges, and future directions," *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2017.
27. R. Ranjithkumar, D. Ganeshkumar, and S. Senthamilarasu, "Efficient and secure data hiding in video sequence with three layer security: an approach using chaos," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13865–13878, 2021, doi: https://doi.org/10.1007/s11042-020-10324-7.
28. S. A. Al Nahian, Z. Hosen, and P. Ahmed, "An elementary study of chaotic behaviors in 1-D maps," *Journal of Applied Mathematics and Physics*, vol. 7, no. 5, pp. 1149–1173, 2019.
29. J. Vivek and B. Gadgay, "Video steganography using chaos encryption algorithm with high efficiency video coding for data hiding," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 5, 2021.
30. S. Mumthas and A. Lijiya, "Transform domain video steganography using RSA, random DNA encryption and huffman encoding," in *7th International Conference on Advances in Computing & Communications*, ICACC-2017, 22–24 August 2017, Cochin, India.