# Robust large image steganography using LSB algorithm and 5D hyper-chaotic system

**Jinan N. Shehab[1], Hussein A. Abdulkadhim[2], Taqwa F. H. Al-Tameemi[3]**
[1,2]Department of Communication Engineering, College of Engineering, University of Diyala, Iraq
[3]Department of Computer Engineering, College of Engineering, University of Diyala, Iraq

**Article Info**

***Article history:***

Received Sep 28, 2020
Revised Dec 24, 2020
Accepted Jan 15, 2021

***Keywords:***

5D hyper-chaotic system
Color image hiding
Image cryptography
Large image steganography
LSB algorithm

**ABSTRACT**

This paper contains a robust hiding system proposed to hide and reconstruct efficiently a large size secret image based on merging encrypting and hiding. This approach deals with a video utilized as a cover of frames to hide the blocks of large image inside it. Frames are selected according to 5D hyper-chaotic algorithms and consequently change value of the pixel in the original image depends on it. Secret image will divide into many blocks and hide each block in one frame selected by 5D chaotic. This method will support and enhance the techniques of information security with less time and more capacity of transmission. The results obtained are analyzed under criteria including: Peak signal to noise ratio, Mean square error, key space and sensitivity, correlation coefficient and capacity of hiding. The results demonstrate both of the secret color image and cover video, where retaining its explicitness and properties after reconstruction in the receiver. However, the results prove stability and reliability of the proposed system under several conditions and can avoid attacks.

***Corresponding Author:***

Hussein A. Abdulkadhim
Department of Communication Engineering
College of Engineering, University of Diyala
Baqubah, Diyala 32001, Iraq
Email: hussein73@mail.ru

## 1. INTRODUCTION

Development of the computer and information technology is a new impetus for the development of computer cryptography and steganography [1, 2]. Many new applications have emerged and as technology improved, most people began to use the internet for sharing information. This information may be any format of multimedia with multiple sizes. Such information about military, banking and many government organizations are strictly confidential, while sending this information online is not always safe [2, 3]. Cryptography and steganography techniques are important tools to provide security and protect sensitive information. Encryption provides features such as data confidentiality and integrity. For example, confidentiality will be achieved through an encryption algorithm by mix private data or information so as to become unreadable to anyone other than the intended recipient. In the other hand, hiding information in a cover medium provides security so that a malicious user does not know that a hidden message exists [1, 4]. In case of large size image, which have a big amount of visual data, for example, of surrounding area or may be encrypted data or an audio hided in a large image, hiding process is a challenge task and high protection and security are required. Moreover, this image may be a satellite image with high resolution about weather, terrain and even military information. So, with the huge progress of the wireless and information technology, sending these images with high level security will represent an important challenge too [5, 6]. This paper suggests a robust method to hide a large size secret color image in a video with encryption provided by 5D hyper chaotic system. Furthermore, the secret image will, firstly, encrypted by 5D hyper-chaotic system and the result of cipher image will split into many blocks. Secondly, each block will be hide in a frame selected, also, by 5D hyper chaotic. Hiding process executed by a well-known steganographic method: least significant bit (LSB). The proposed system analyzed under different conditions such as noise and filtration to observe accuracy and robustness.

As related works, there are various methods for hiding data for both video/image frames. According to Thakur and Saikia, 2013 [7], conversion of the grayscale pixel values to the binary values and then hidden them to the higher-order coefficient value of DCT of AVI video frames have done so the hiding of information and extraction are executed effectively. Moreover, in [8], for hiding a secret image in video, the LBC method is utilized with transformation and masking- filtering tech. The paper [9] is presented low complexity algorithm for video preen coded with the high efficiency video coding standard. This paper chooses mechanisms like motion vector difference and transform coefficients of the video are extracted and modified, bypassing the need of fully decoding and re-encoding the video. The researchers in the [10] present an algorithm for multi-level reversible data hiding that is efficient for video sequence. Because the distribution of gray level of various map is Laplacian, as a result of that distribution of highest point causes into increasing in the capacity of hiding data and the quality of image. Moreover, the [3] is proposed a hiding technique for high security data and it shown when the four equal portions are cropped from selected video frame, the block of secret information are hiding in three channels by LSB technique. While in the [4], two 2-D chaotic maps are utilized as fundamental to create a steganographic algorithm where it has the ability to the encrypted sensitive data by using the chaotic maps in the image cover depended on the LSB tech. According to [11], the authors develop reversible data hiding in encrypted image (RDHEI) through divided the image into blocks that is not intersected blocks. Since each block start hiding from center pixel then moved even right or left.

By comparing with the previous works mentioned, in the present work, employing 5D chaotic system to play a great role for encrypting image and selecting frames represents an efficient and effective solution and made a quite difficult to detect secret message inside video. Furthermore, integration of 5D heyber chaotic system with LSB algorithm will produce a robust system to hide large images with high resolutions. Finally, method of this paper represents by many sections: 5D novel hyper chaotic system, LSB algorithm, embedded and constructed operation, tests and results and finally, conclusions.

## 2. THE COMPREHENSIVE THEORETICAL BASIS

### 2.1. A novel 5D hyper-chaotic system

A 5-D hyper chaotic is a special dynamical nonlinear system which has more complex properties than lower dimensional chaotic systems [12]. This novel system can be defined by the 5D independent differential equation:

$$\left.\begin{aligned} \dot{x} &= ay - bx + u + w + c\,sin(z) \\ \dot{y} &= dx - xz - y \\ \dot{z} &= xy - ez \\ u &= -fxz + gu \\ \dot{w} &= hx + i\,cos(u) \end{aligned}\right\} \qquad (1)$$

where {x, y, z, u, w}-the system states; {a, b, c, d, e, f, g, h, i}-constant values. For example, if the initial states are x(0)=-1, y(0)=0.9, z(0)=0.1, u(0)=1.3, and w(0)=0, then the 5D hyper-chaotic attractors obtained will be shown in the Figure 1.

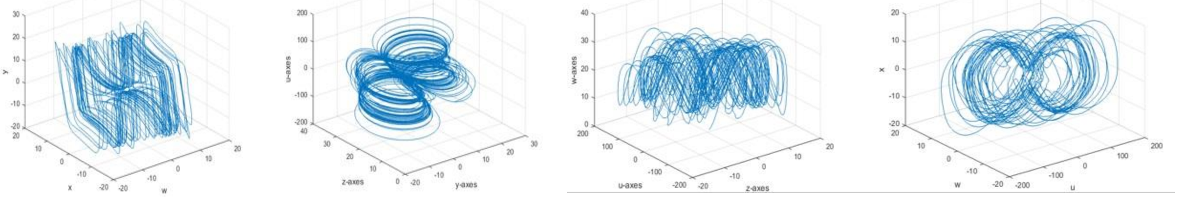


Figure 1. 5D hyper chaotic attractors

### 2.2. Least significant bit substitution method

In the field of telecommunications, LSB steganographic method is commonly used for hiding data or information inside a cover (i.e. image, audio (voice) as well as video) [13, 14]. In case of an image with 8 bits depth pixel, a tiny change in the least significant bits will be not affects or noted much. Therefore, each character of a secret message is converted to 8-bit binary sequence before hiding process and replaced with eight least significant bits of the cover image pixel [13, 15].

## 3. THE PROPOSED SYSTEM

The basic idea of the proposed system (hiding and reconstructing) is defined as a combination of the LSB with 5D hyper chaotic algorithms. According to proposed scheme of hiding operation shown in Figure 2, initially, the user should be select a cover video with resolution of, for example, (512×512×3) and provide original secret image. To demonstrate the procedure for hiding owner data, firstly, the secret image with any size will divide into 3-channels of colors (red, green, and blue). Secondly, every channel diffusion (cipher) according to the random number (key) generated by 5D hyper-chaotic system and in acceptable intervals. The resulted value of *X* will modify to integer value between (0,255) by:

$$X_i(m)=\mathrm{mod}\ (\mathrm{floor}\ (X_{i-1}(m).10^{16}), 256) \quad (2)$$

where (x, y, z, w, u) are resulted from (1) and limited between (0 and 255). Variating of the pixel according to hyper chaotic for constructing new pixel's value with the same dimension of secret image as:

Key for red color = $w_{new}$ XOR $u_{new}$ $\Longrightarrow$ New pixel = old pixel XOR key for red;
Key for green color = $z_{new}$ XOR $w_{new}$ $\Longrightarrow$ New pixel = old pixel XOR key for green;
Key for blue color = $y_{new}$ XOR $z_{new}$ $\Longrightarrow$ New pixel = old pixel XOR key for blue;

Thirdly, each channel will divide into 4-blocks (4-blocks for red, 4-blocks for green and 4-blocks for blue channels) or more, depends on the total size of image, and each block hide into one frame selected randomly by 5D chaotic system as shown in Table 1. The key of selecting frame will submit to the following relation: $Key_{frame}=X_{new}$ *XOR* $Y_{new}$. For example, if secret image divide into 4-blocks, then 12-frame will select according to the keyframe generated. Finally, convert each frame and block into binary number and hide each bit from block in the last bit of the cover frame according to LSB procedure. Then, convert back each of them from binary to decimal to produce stego-frame and consequently back into original position in video to produce stego-video. Stego-video will be ready to send through the transmission channel.

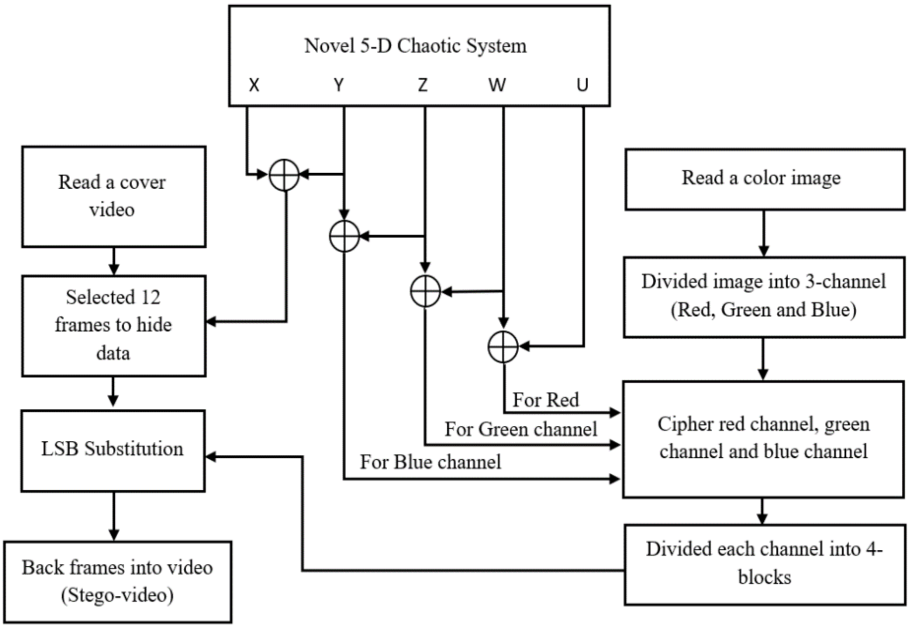
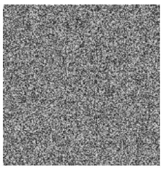
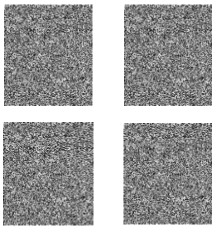
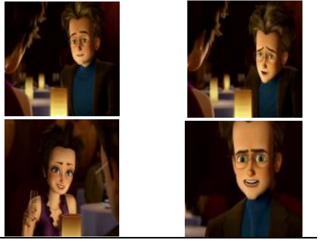

Novel 5-D Chaotic System
X
Y
Z
W
U
Read a cover video
Selected 12 frames to hide data
LSB Substitution
Back frames into video (Stego-video)
Read a color image
Divided image into 3-channel (Red, Green and Blue)
Cipher red channel, green channel and blue channel
Divided each channel into 4-blocks
For Red
For Green channel
For Blue channel

Figure 2. The propose system of hiding operation

Table 1. Results of the hiding process

| Original Secret image (600×600) | Red channel of the secret image | After encryption | After dividing into blocks (300×300) | 4-frames from the cover video (512×512) |
|---|---|---|---|---|
| | |  |  |  |

In the receiver side, the extraction and reconstruction operations of a secret image are simply representing the reverse of hiding process in the sender, as shown in Figure 3. The secret key (i.e. the initial conditions of x (0), y (0), z (0), w (0), u (0), (a, b, c, d, e, f, h, i) of 5-D chaotic system) must be available in the receiver. Extraction operation initializes by reading the stego-video and then generates the same keyframe to select frames from the video. Next step includes conversion operation for each pixel of selected frame to binary number (24 bits per pixel) to extract the last-bit from each pixel and convert it to the decimal number. The result of this step will produce secret block of one-color channel. Third step is the joint-process for each 4-blocks to get one channel and return each pixel value in each channel based on initial conditions and parameters of 5-D chaotic algorithm. Finally, reconstruction operation represents by joint each 3-channel to get one color block to obtain the target (i.e. secret color image).

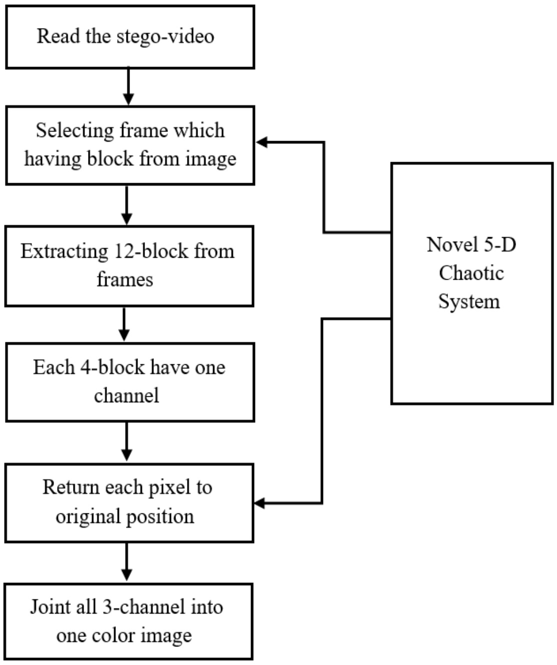

Read the stego-video
Selecting frame which having block from image
Extracting 12-block from frames
Each 4-block have one channel
Return each pixel to original position
Joint all 3-channel into one color image
Novel 5-D Chaotic System

Figure 3. The reconstruction process in the receiver

## 4. RESULTS AND DISCUSSION

In this work, AVI video with duration of 11 sec. is used for testing the proposed system. The video contains 253 frames (512×512×3). The secret message is color images with many different sizes and format. To evaluate quality of the obtained images and video (hiding and reconstructing), all results will be analyzed by:

### 4.1. MSE and PSNR

The mean square error (MSE) and peak signal-to-noise ratio (PSNR) are two metrics of error employed to evaluate image/frame quality after extraction and reconstruction. MSE gives the square error between stego-video and original image, while PSNR is define as an indicator to measure the peak error obtained from the process of extraction [16, 17]. Mathematically PSNR represented as:

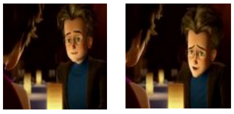
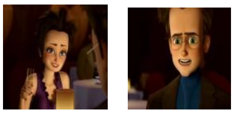
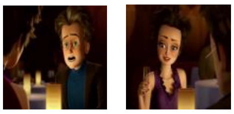
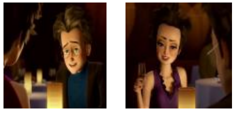
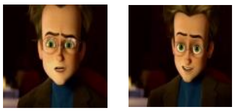
$$PSNR(dB) = 10\, log_{10} \frac{P^2}{MSE} \tag{3}$$

where $P$-max. pixel value; the cumulative Errors are estimated by:

$$MSE = \frac{1}{RC} \sum_{i=0}^{R-1} \sum_{j=0}^{C-1} [X_{i,j} - \hat{X}_{i,j}]^2 \tag{4}$$

where $R$, $C$ are the number of pixels in each row & column respectively; $i$, $j$ -row and column numbers, $X_{i,j}$ −original image and \ $\hat{X}_{i,j}$ −stego-image/frame. The results of test are shown in the Table 2. Clearly note the variance in PSNR values when using different size of color image like (100×100, 200×200, 300×300, 400×400, 500×500, 600×600). Moreover, it is observed that the ability to hide a massive amount of information with high accuracy instead of sending an image in each frame. The maximum size obtained when decreasing of PSNR and effects on the image's content.

Table 2. Analysis by using PSNR

| Cover frames (512×512) (12-frames selected from cover video) | Secret image (4-blocks red, 4-blocks green and 4-blocks blue channel) | Extraction of secret blocks | Size of secret block | PSNR (dB) | | | |
|---|---|---|---|---|---|---|---|
| | | | | Block1 | Block2 | Block3 | Block4 |
|  | | | 100×100 | 67.133 | 67.240 | 67.020 | 67.325 |
| | | | 200×200 | 61.132 | 61.212 | 61.212 | 61.244 |
| | | | 300×300 | 57.784 | 57.664 | 57.677 | 58.178 |
|  | | | 400×400 | 55.534 | 55.674 | 55.250 | 55.499 |
| | | | 500×500 | 53.084 | 53.089 | 53.133 | 53.321 |
| | | | 600×600 | 51.635 | 51.575 | 51.598 | 51.594 |
|  | | | 100×100 | 66.951 | 67.067 | 66.757 | 66.947 |
| | | | 200×200 | 60.879 | 61.034 | 60.745 | 60.959 |
| | | | 300×300 | 57.833 | 57.629 | 58.225 | 58.270 |
| | | | 400×400 | 54.998 | 55.006 | 55.361 | 55.273 |
| | | | 500×500 | 53.101 | 53.152 | 52.860 | 52.935 |
| | | | 600×600 | 51.436 | 51.562 | 51.403 | 51.436 |
|  | | | 100×100 | 66.801 | 67.064 | 66.698 | 66.829 |
| | | | 200×200 | 60.836 | 61.016 | 60.662 | 60.735 |
| | | | 300×300 | 57.484 | 57.726 | 57.642 | 57.702 |
|  | | | 400×400 | 54.967 | 55.214 | 55.472 | 55.537 |
| | | | 500×500 | 52.930 | 53.166 | 52.879 | 52.922 |
| | | | 600×600 | 51.337 | 51.567 | 51.417 | 51.519 |

### 4.2. Signal to noise ratio

The presented method is also evaluated according to the similarity between cover frame (original) and stego-frame. Highest value of signal to noise ratio (SNR) indicates a minimum variance among original and stego-frames [18]:

$$SNR = 10\, log_{10} \frac{1/N \sum_{i=0}^{N} xi^2}{MSE}$$

### 4.3. Correlation coefficient and capacity of hiding

Digital image correlation is full-field image analysis methods based on grey value of digital images which can be determine the contour and the displacements of an object under load in three dimensions [12]. The correlation coefficient has a unit value (i.e. N.Corr.=1) if the two images are absolutely identical, while N.Corr.=0 if they are completely uncorrelated. Correlation number is also used to measures the similarity level between these two covers (before and after hiding the secret message) and between two images (original secret image and cipher image). Pearson's correlation coefficient is commonly employed in statistical analysis, pattern recognition, and image processing [13]. Consider Z1 and Z2 are two images, then the correlation coefficient estimated by the following expression:

$$\text{N. Corr.} = \frac{\sum(X_i - X_j)(Y_i - Y_j)}{\sqrt{(X_i - X_j)^2}\sqrt{(Y_i - Y_j)^2}}$$

where $X_i$ is the intensity of the i<sup>th</sup> pixel in Z1, $Y_i$ is the intensity of the i<sup>th</sup> pixel in Z2, $X_j$ is the mean intensity of Z1 and $Y_j$ is the mean intensity of Z2. Let us the multiple secret images 200x200 (4-blocks 100x100) for only the red channel of each image and cover frame (512x512), then the results of PSNR, SNR and $N.Corr.$ obtained are shown in Table 3.

The term called "Capacity of hiding" refers to the amount of information that hidden in the cover medium without effects on its original characteristics [19]. In Table 4 reflected the results of hiding secret image with multiple sizes and 4-blocks in the cover video. Analysis results shows that increasing of the capacity of hiding for the whole channel image/block in one frame (i.e. related to the size of hiding) will reduce the PSNR and SNR values and consequently change slowly the intensity ratio of cover frame. In other words, the sizes of secret block and cover frame are change in one forward direction for the hiding and reconstructing operations to reduce the detection factor. Moreover, it is to keep on the correlation value between pixels of the frame approximately unity. This lead to raise the difficulty level of detection by attackers and provide the impression of no hidden information.

Table 3. Some results of analysis for the cover frame

| The secret image (block size 200×200) | Stego-video (to hide red channel) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PSNR | | | | SNR | | | | N.Corr. | | | |
| | Block1 | Block2 | Block3 | Block4 | Block1 | Block2 | Block3 | Block4 | B1 | B2 | B3 | B4 |
| Lena.bmp | 61.132 | 61.1399 | 61.1200 | 61.1229 | 48.3477 | 48.8805 | 49.0276 | 48.7911 | 1 | 1 | 1 | 1 |
| Monaliza.jpg | 61.0048 | 61 | 61.0303 | 60.9709 | 48.2081 | 48.7406 | 48.938 | 48.639 | 1 | 1 | 1 | 1 |
| Babbon.png | 61.0472 | 61.0400 | 61.0674 | 61.1153 | 48.2504 | 48.7806 | 48.9751 | 48.7835 | 1 | 1 | 1 | 1 |
| Airplane.jpg | 61.3277 | 61.3060 | 61.2490 | 61.4148 | 48.5309 | 49.0466 | 49.1567 | 49.0830 | 1 | 1 | 1 | 1 |

Table 4. Some results of analysis hiding block (for frame)

| Dimension of the secret image (Lena.bmp) | | For one frame to hide one block (red channel) | | | |
|---|---|---|---|---|---|
| All size of the image | One block from secret red channel in color image | Capacity (%) | PSNR (dB) | SNR | N.Corr. |
| 100×100 | 50×50 | 0.9536 | 67.1249 | 54.3281 | 1 |
| 200×200 | 100×100 | 3.8146 | 61.1445 | 48.3477 | 1 |
| 300×300 | 150×150 | 8.5831 | 57.5965 | 44.7998 | 1 |
| 400×400 | 200×200 | 15.2588 | 55.1422 | 42.3455 | 0.9999 |
| 500×500 | 250×250 | 23.8419 | 53.1453 | 40.3485 | 0.9999 |
| 600×600 | 300×300 | 34.3323 | 51.5475 | 38.7507 | 0.9999 |

### 4.4. Entropy of information

Entropy of a source provides an idea of self-information, i.e. information obtained via a random process about itself, where it represents trait characteristic of randomness. Let $p(x)$ stands for the information source, the formula for computing the entropy of information illustrated in the following equation [12]:

$$Entropy = -\sum_{i=0}^{n-1} p(x_i)\,.log_2 p(x_i)$$

In Table 5, some results of entropy of information hidden with the correlation coefficient of diagonal, horizontal and vertical of the cipher color image. Analysis results show that the difference in entropy level between original and cipher image is large because of distribution of data in the cipher image is uniformly distributed. Additionally, the correlation coefficient among them approximately zero, i.e. there is no relation between pixels in the original & cipher. In this case, attackers will not detect the original image.

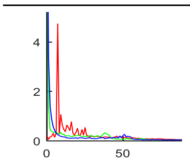
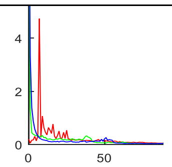
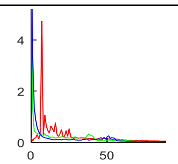
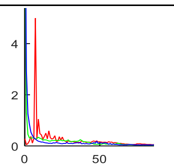
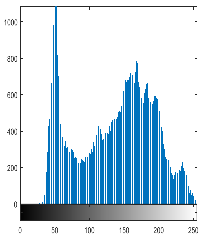
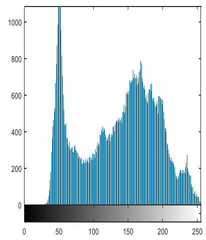
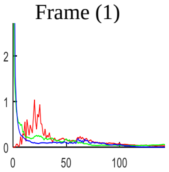
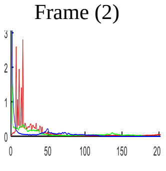
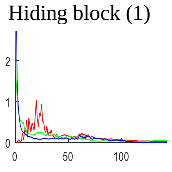
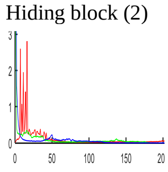
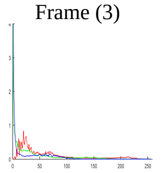
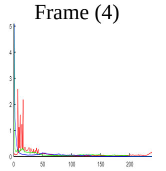
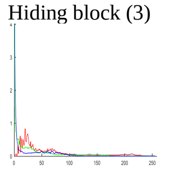
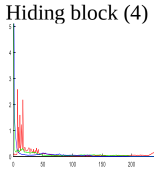
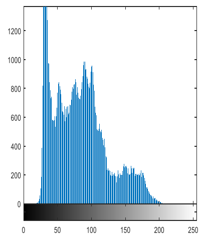
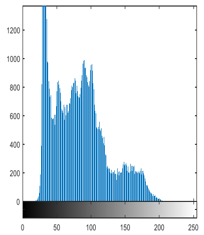
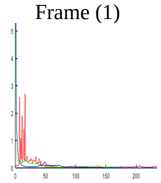
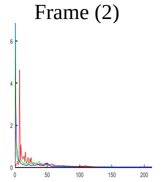
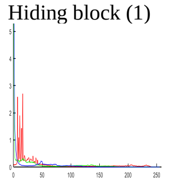
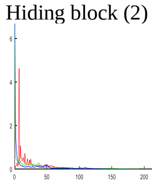
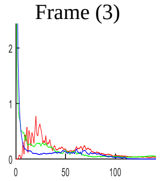
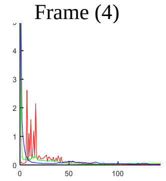
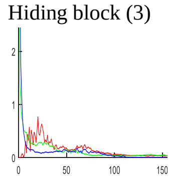
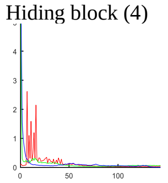
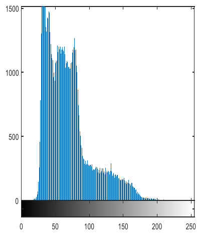
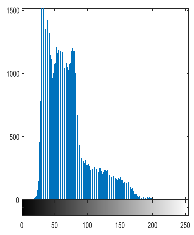
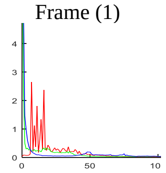
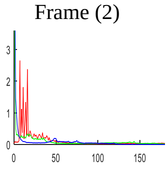
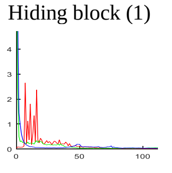
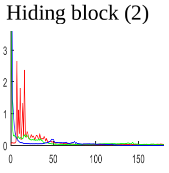
Table 5. Some results of entropy of information and correlation coefficient for color cipher image

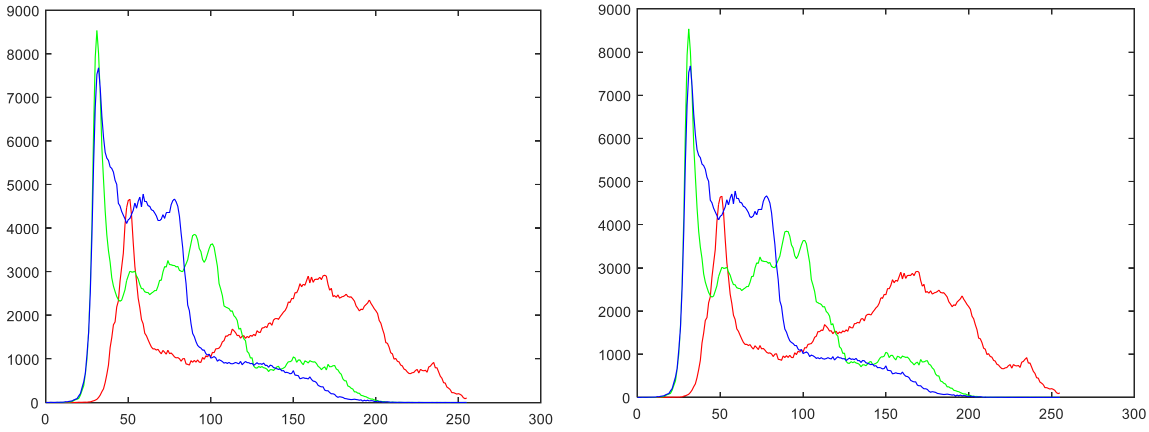
| Dimension of the secret image (Lena.bmp) | | For cipher color image | | | |
|---|---|---|---|---|---|
| All size of the image | One block from secret red channel in color image | Entropy | N.Corr. | | |
| | | | Diagonal | Horizontal | Vertical |
| 100×100 | 50×50 | 7.9941 | 0.00153 | 0.00079 | 0.00361 |
| 200×200 | 100×100 | 7.9987 | 0.00114 | 0.000130 | 0.00117 |
| 300×300 | 150×150 | 7.9993 | 0.00081 | 0.00080 | 0.00249 |
| 400×400 | 200×200 | 7.9996 | 0.00096 | 0.0009 | 0.0009 |
| 500×500 | 250×250 | 7.9997 | 0.00038 | 0.0008 | 0.0003 |
| 600×600 | 300×300 | 7.9998 | 0.000745 | 0.0053 | 0.0087 |

## 4.5. Histogram analyzer

Histogram analysis for the cover and stego-frame and original & reconstruction color image are used to verify the statistical properties which are not changed by varying one bit in some pixels [16, 20]. Table 6 contains results of the histogram analysis for this purpose. Result shows that histogram analysis for the original images before hiding are the same as it after reconstruction. Practically, there is no difference noted between the original and reconstructed image as shown for each channel. Figure 4 represents some results of histogram analysis for the secret image before and after construction operation. Simply note that no errors appear between two cases.

Table 6. Histogram for the cover & stego frames and hiding blocks

| Cover frame (512×512) | | Stego-frame (512×512) | | Secret image | Extraction secret image |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| Frame (1) | Frame (2) | Hiding block (1) | Hiding block (2) | | |
|  |  |  |  | | |
| Frame (3) | Frame (4) | Hiding block (3) | Hiding block (4) | Red channel | |
|  |  |  |  |  |  |
| Frame (1) | Frame (2) | Hiding block (1) | Hiding block (2) | | |
|  |  |  |  | | |
| Frame (3) | Frame (4) | Hiding block (3) | Hiding block (4) | Green channel | |
|  |  |  |  |  |  |
| Frame (1) | Frame (2) | Hiding block (1) | Hiding block (2) | | |
|  |  |  |  | | |
| Frame (3) | Frame (4) | Hiding block (3) | Hiding block (4) | Blue channel | |



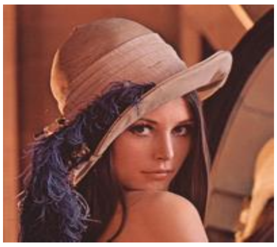
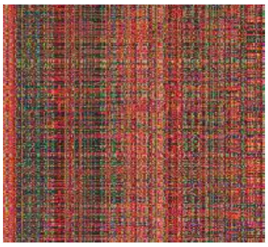
(a) (b)

Figure 4. Histogram of the secret image, (a) Histogram of secret image at transmitter, (b) Histogram of secret image after reconstruction

### 4.6. Key space and sensitivity

The first term “key space” is defined as the total number of different generated keys which used in the encoding process [16, 20]. The second term “The key sensitivity “is defined as a minimum amount of changing at the encoded image/picture resulted from a little variation in the secret (detection) key [12, 16]. For the first term, the possible size of key (β) in bits is designed to $10^{80}$ for the presents work and the probability of detecting key has 2β times to find the correct key. However, both the initial condition and parameters are enough combined to avoid the exhaustive search. For the second term, in order to rise degree of the key sensitivity (z) of the proposed system, the minimum significant sensitive illustrated to $10^{-16}$ which mean only using the exact key can retrieve the secret block as illustrated in Table 7.

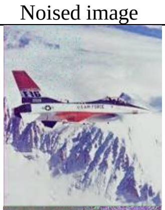
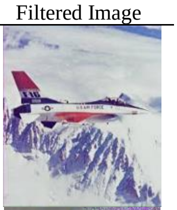
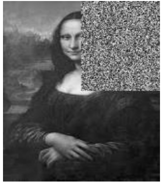
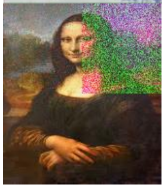
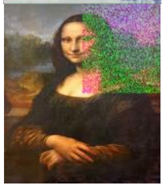
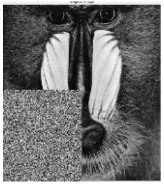
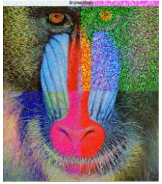
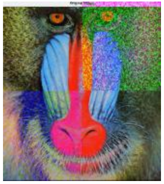
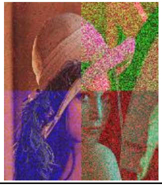
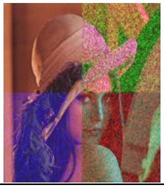
Table 7. High sensitivity of the detection key

| Original secret image | Reconstruction by the key z= **0.7** | Reconstruction by wrong key z= **0.70000000000001** |
|---|---|---|
| |  |  |

### 4.7. Noise test and filtration

In the channel of information, the noise is any degradation in the image signal caused by external disturbance such as: Wireless transmission, Satellite transmission and Network cable transmission [21-23]. Therefore, filtering of an image corrupted by noise is a significant area of image restoration [23-25] and depending on the type of disturbance in the signal [25-28]. For testing the proposed system against different types of noise (white noise, salt and pepper noise.) and filtration process, let us adding such noise to the frame and then use, as example, the median filter, as shown in Table 8. The process of reconstruction target blocks shows that if one frame effected by noise, then it will change one block of one-color channel from the secret color image. Of course, this is better than if the whole color image is hidden with a frame. Moreover, random selection of the cover frames depends on the key generated by 5D chaotic system will provide minimum probability of damage produced by noise. Also, filtration process will support block retrieving process and consequently reconstruct secret image with better status of contrast. Finally, through the results above can be processed frame before pulling the block to get a better result if the image was processed after the withdrawal of the frame.

Table 8. Reconstruction process for the secret image under noise and filtration

| Red channel | Green channel | Blue channel | Noised image | Filtered Image |
|---|---|---|---|---|
| | | |  |  |
| |  | |  |  |
| | |  |  |  |
| | | |  |  |

## 5. CONCLUSION

This paper presents a robust system proposed for hiding a large color image with different sizes in a cover video based on the LSB steganography technique and utilizing of diffusion key produced by the 5-D chaotic system. The secret image splitted into three color channels and diffused each of them. Each channel divided into four blocks or more based on dimensions of image. This work will enhance the security of secret image/picture and sturdiness of undetectability. Also, the idea of hiding blocks will produce high-level security, more transmission capacity of information and more accuracy. Moreover, the utilize of different image/pictures in hiding led to the slightly verity in results and that depended on the intensity of the data content and color gradations. According to the obtaining results from PSNR, SNR, correlation, capacity of information and histogram tests, the stego-video was hiding with minimum remarkable damage and degeneration. Large space and high sensitivity of the secret key will enhance difficulty of detection by attackers and present extra security for the base of steganography techniques and cryptography. Finally, selection of cover frame by 5D chaotic system and increasing of block numbers will relatively improve secret image under noise condition.

## REFERENCES

[1] Ashwak ALabaichi, Maisa'a Abid Ali K. Al-Dabbas, and Adnan Salih, “Image steganography using least significant bit and secret map techniques,” *International Journal of Electrical and Computer Engineering*, vol. 10, no.1, pp. 935-946, Feb. 2020.

[2] Roshidi Din and Alaa Jabbar Qasim, “Steganography analysis techniques applied to audio and image files,” *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1297-1302, Dec. 2019.

[3] Bharathi D. A, Anitha P., and Kiran S. M., “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, no. 3, pp. 693-698, 2017.

[4] A. H. S. Abdelgader , R. A. Aboughalia, and O. A. S. Alkishriwo, “Combined image encryption and steganography algorithm in the spatial domain,” *First Conference for Engineering Sciences and Technology (CEST-2018)*, 2018.

[5] C. Periyasamy, “Satellite image compression based on SPIHT algorithm,” *Indonesian Journal of Electrical Engineering and Informatics*, vol. 5, no. 4, pp. 366-368, Dec. 2017.

[6] A. Kumar and K. Pooja ,“Steganography-a data hiding technique,” *International Journal of Computer Applications*, vol. 9, no.7, pp. 19-23, Nov. 2010.

[7] V. Thakur and M. Saikia, “Hiding secret image in video,” *International Conference on Intelligent Systems and Signal Processing (ISSP)*, pp 150-153, 2013, doi: 10.1109/ISSP.2013.6526892.

[8] K. S. Jenifer, G. Yogaraj, and K. Rajalakshmi, “LSB approach for video steganography to embed images,” *International Journal of Computer Science and Information Technologies*, vol. 5, no. 1, pp. 319-322, 2014.

[9] S. Acharya, P. Srimany, S. Kundu, and J. G. Dastidar, “Data hiding in video using triangularization LSB technique,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 4, no. 3, pp. 44-47, 2015.

[10] K-L. Chung, W-J. Yang, T-C. Chang, and H-Y. M. Mushtaq, “Efficient Multilevel Reversible Data Hiding For Vedio Sequence Using Temporal And Spatial Approch,” *Proceedings of 2009 APSIPA Annual Summit and Conference*, pp. 573-582, 2009.

[11] A. Mohammadi and M. Nakhkash, “Reversible data hiding in encrypted images using local difference of neighboring pixels,” *arXiv preprint arXiv:1907.05123*, 2019.

[12] S. A. Mehdi, K. K. Jabbar, and F. H. Abbood, “Image encryption based on the novel 5D hyper-chaotic system via improved AES algorithm,” *International Journal of Civil Engineering and Technology*, vol. 9, no. 10, pp. 1841-1855, Oct. 2018.

[13] H. Gupta and S. Chaturvedi, “Video data hiding through LSB substitution technique,” *International Journal of Engineering and Science*, vol.2, no. 10, pp. 32-39, April 2013.

[14] S. A. Nie, G. Sulong, R. Ali, and A. Abel, “The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image,” *International Journal of Electrical and Computer Engineering*, vol. 9, no. 6, pp. 5218-5226, Dec. 2019.

[15] A. M. Aaref, “Video steganography using LSB substitution and sobel edge detection,” *Diyala Journal of Engineering Sciences*, vol. 11, no. 2, pp. 67-73, June 2018.

[16] J. N. Shehab and H. A. Abdulkadhim, “Image steganography based on least significant bit (LSB) and 4-dimensional Lu and Liu chaotic system,” *2018 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 274-279, 2018, doi: 10.1109/ICOASE.2018.8548864.

[17] S. Pramanik, R. P. Singh, and R. Ghosh, “A new encrypted method in image steganography,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 3, pp. 1412-1419, June 2019.

[18] Asawari S. Shinde and Archana B. Patankar, “Image steganography: hiding audio signal in image using discrete wavelet transform,” *International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017)*, vol. 5, no. 3, pp. 331-334, 2017.

[19] M. Shrivastava, R. Ranjanand, and S. Kumari, “Video steganography using pixel intensity value and LSB technique,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 2, pp. 287-290, Feb. 2015.

[20] H. A. Abdulkadhim, J. N. Shehab, and A. N. Albu-rghaif, “audio security based on LSB steganography and 4-D Lü system,” *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, pp. 203-208, 2018, doi: 10.1109/SCEE.2018.8684213.

[21] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, “A combination of inverted LSB, RSA, and arnold transformation to get secure and imperceptible image steganography,” *Journal of ICT Research and Applications*, vol. 12, no. 2, pp. 103-122, 2018.

[22] A. Odat, M. Otair, and F. Shehadeh, “Image denoising by comprehensive median filter,” *International Journal of Applied Engineering Research*, vol. 10, no. 15, pp 36016-36022, 2015.

[23] J. Liu, C-H. Wu, Y. Wang, Q. Xu, Y. Zhou, H. Huang, C. Wang, S. Cai, Y. Ding, H. Fan, and J. Wang, “Learning raw image denoising with Bayer pattern unification and Bayer preserving augmentation,” *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 2070-2077, 2019.

[24] F. H. Mohammed Sediq Al-Kadei, “Two-level hiding an encrypted image,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 961-969, May 2020.

[25] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, “Text in image hiding using developed LSB and random method,” *International Journal of Electrical and Computer Engineering*, vol.8, no.4, pp. 2091-2097, August 2018.

[26] C. A. Sari, G. Ardiansyah , D. R. I. M. Setiadi, and E. H. Rachmawanto, “An improved security and message capacity using AES and Huffman coding on image steganography,” *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 5, pp.2400-2409, Oct. 2019.

[27] Z. N. Al-kateeb and M. Jader, “Encryption and hiding text using DNA coding and hyperchaotic system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, pp. 766-774, August 2020.

[28] O. F. Abdel Wahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, “Hiding data in images using steganography techniques with compression algorithms,” *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol.17, no.3, pp.1168-1175, June 2019.