Journal of Information Systems Engineering and Management
2025, 10(17s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Steganography in Videos Captured by a Drone

Hassanain Raheem Kareem [1], Hadi Hussein Madhi [2], Mohsin Najim Sarayyih AL-Maliki [3], Ahmed Salih Al-Khaleefa [4]

[1]Physics Dep., College of Education, University of Misan , Misan ,Iraq
[2] College of Nursing, University of Misan, Misan ,Iraq
[3] Accounting., College of Management and Economics, University of Misan , Misan ,Iraq
[4] Department of Computer Technology Engineering, Technical College, Imam Ja'afar Al-Sadiq University, Maysan 10011, Iraq
* Corresponding Author: Hassanain Raheem, hassanainraheem@uomisan.edu.iq

ARTICLE INFO

Received: 06 Dec 2024

Revised: 29 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

Today, Unmanned Aerial Vehicles (UAVs), commonly known as Drones, are used to take pictures of places where it is difficult for humans to access, which represents a great advantage, but videos or photographs can likely be subsequently used by users who do not have the authorization of the owners; this represents a great vulnerability. For this reason, in this research, a technique that applies steganography to videos is proposed, implementing chaotic mathematical models to increase security, which will help to identify the devices from where the captures were made. In addition, correlation diagrams were elaborated with which it was possible to observe that the system guarantees integrity since when recovering the message, there were no losses.

Keywords: steganography, chaos, drones, authorization

1. Introduction

Current and developing technology must face the problems that are experienced today, such as the growing insecurity in many areas that generates excellent fear among people, which affects the performance of their daily and recreational activities; a viable solution that is currently being used to monitor or reach hard-to-reach places involves the use of Drones. Scenarios have also been established to know industrial safety processes to identify risk factors using drones, to minimize accidents and reduce costs [1, 2]. These devices were also used to characterize the soil cover, which allowed them to work at scales that cannot be obtained with other remote sensing products[3-6]. Drones are also highly profitable in cartography because they allow survey areas to be inspected in a very short time, but they present a low spectral resolution, so it is advisable to use digital cameras with a greater capacity [7]. Additionally, they have been used in some experiments to search for people in catastrophic situations, which is useful; however, they do not have a great impact on the assistance of victims[8]. These devices can be used in many areas, but it is of great importance to authenticate the authors of the videos or photographs that capture them; For this reason, it is necessary to establish measures to identify the owners, a technique that can be used in steganography, since it allows hiding information or binary data, within media such as text files, audio, images, videos, etc. avoiding their disclosure or making them go unnoticed[9]. Chaotic systems have behaviour that, at first glance, can be seen as if it were erroneous information, which they take advantage of to encode information[10-12] or apply steganography techniques [13].

In this research, software was developed that stores files captured from a drone on a computer or portable device; At the same time, it implements steganography using chaotic systems to hide a drone identifier within the videos or photographs, which will allow the protection of copyright or, where appropriate, will help the Secretary of Communications and Transportation SCT in the detection of the devices that capture images in unauthorized places.

2 State of the Art

2.1 Logistics Map

It is a very simple chaotic discrete system, which is solved quickly and is expressed as shown in Equation (1):

$$x1_{n+1} = b * x1_n * (1 - x1_n) \quad (1)$$

Where is a dynamic variable and represents the control parameter, which makes the system behave chaotically where $b \in [3.567,4]$.

2.2 Map Sine

It is a one-dimensional chaotic discrete system that is defined in Equation (2):

$$XS_{N+1} = c * \sin(\pi * XS_N) \quad (2)$$

where is the dynamic variable and the control parameter; the system behaves chaotically when $c \in [0.87,1]$.

2.3 Map Tent

This system is expressed in Equation 3, where is the dynamic variable and is the control parameter [13]:

$$xt_{n+1} = \begin{cases} \tau * xt_n & xt_n < 0.5 \\ \tau(1 - xt_n) & xt_n \geq 0.5 \end{cases} \quad (3)$$

3. Methodology

The software was developed that allows the communication of the client (Computer) with the server (Dron), where it is necessary to make the connection through sockets through the UDP communication protocol because it speeds up the connection established between the client and the server.

3.1 System operation

Next, the algorithms proposed in this research are explained, which allow steganography to be applied to hide any type of information in videos captured by the Drone, which are made up of frames or images, made up of pixels, which in turn are divided into 3 sub-pixels corresponding to the colours (RGB) Red, Green, and Blue; these present integer values 0 and 255 according to the intensity of the colour.

Algorithm 1. Technique to hide the message.

To hide information inside the videos, 3 chaotic orbits are generated $(orb_{log}, orb_{sin}, orb_{tent})$ solving the discrete systems of equations (1)-(3) is implemented to chaotically select the video frames, it is used to select the position of a pixel in the image[14], and finally, it allows to determine the subpixel (RGB) to modify[15]. In Figure 1, the procedure of algorithm 1 is presented, which is carried out to hide a message in the video[16-19].

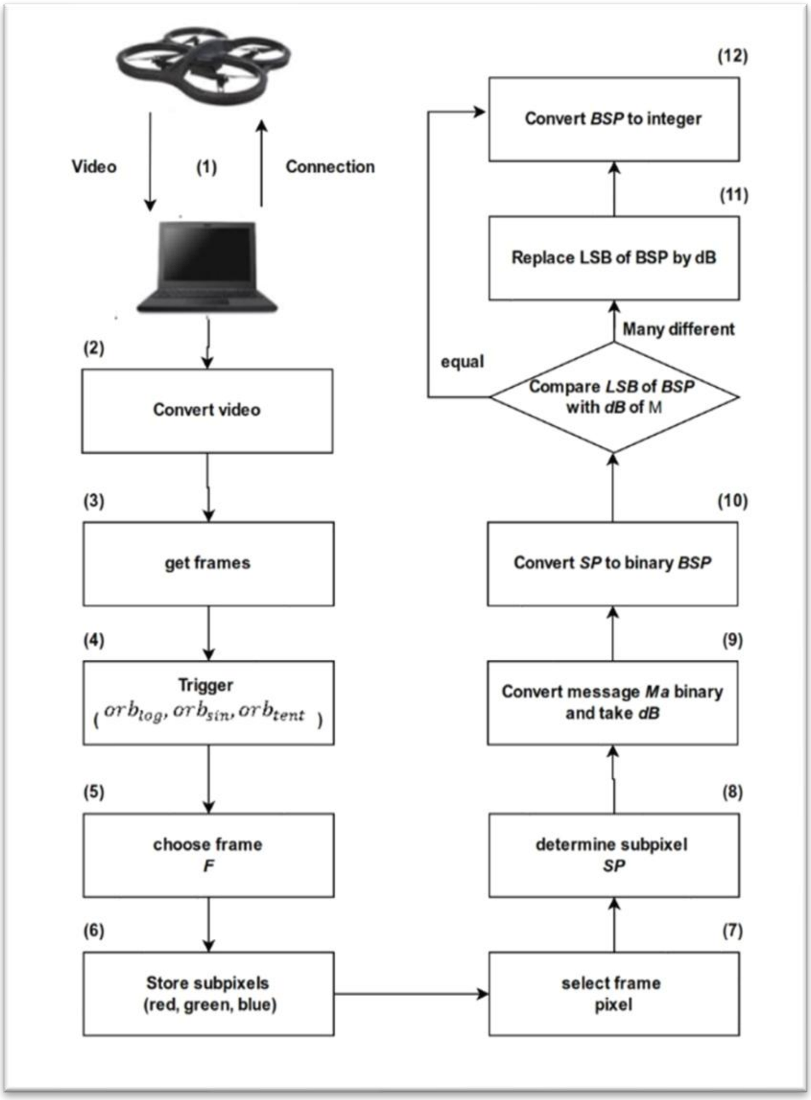

Figure. 1. Operation of algorithm 1.

Next, the entire process of Figure 1 is explained in detail:

Step 1. Make the connection with the Drone used sockets to capture the video.

Step 2. Receive the data from the Drone through the Xuggler library, which converts the video to a viewable format.

Step 3. Capture the video and split it into frames.

Step 4. Solve the chaotic mathematical models of equations (1), (2), and (3) to generate the values of the orbits ().

Step 5. Chaotically select a frame using the value.

Step 6. Store in the red, green, and blue vectors the integers corresponding to the subpixels that make up the frame. In the following steps, the steganography technique proposed by Maricela [20] is applied.

Step 7. Use the orbit to chaotically select the location of a pixel in the frame selected in step 5.

Step 8. Determine the SP subpixel using a where a bit of the message will be hidden.

Step 9. Convert the message to be hidden, to binary, and take a digit.

Step 10. Go to binary to generate the subpixel bits.

Step 11. Use the binary digit of, and verify if the least significant bit) should be modified, taking the following criteria: if it is equal to that of, it is left as is otherwise, the LSB of is changed (if it is 0, it is changed to 1, on the other hand, if it is 1 it is changed to 0).

Step 12. Convert from your binary value to an integer.

The process corresponding to steps 9 to 12 is shown in Figure 2.

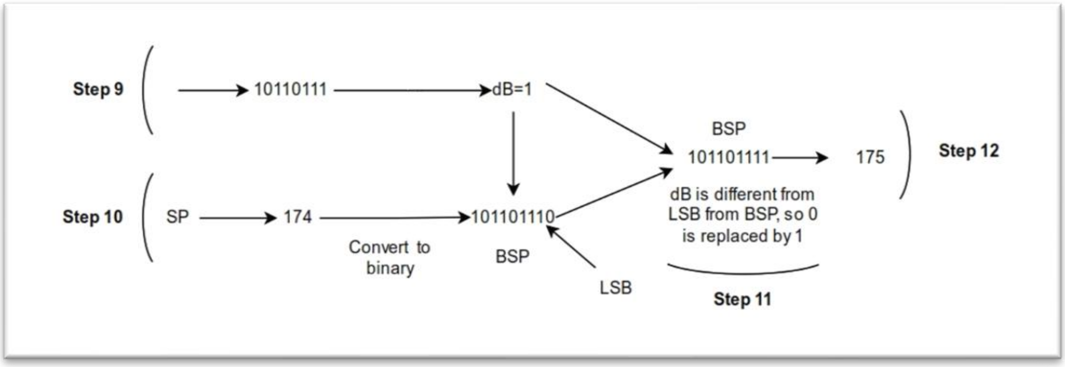

Figure. 2. Modify the LSB of the subpixel.

Steps 4 to 12 are repeated until the entire message is hidden in different frames; therefore, they are transformed into steganography. Then each RGB image is converted to its original Hexadecimal format, and the stego-video is generated[21-24].

Algorithm 2. The process to retrieve the message.

The steps to recover the stego-video message are explained below:

Step 1. Convert stego-video to frames.

Step 2. Repeat steps 4 to 7 of algorithm 1.

Step 3. Use the value generated to determine the subpixel.

Step 4. Take the del and add it to the end of. This process is shown in Figure 3.

SP		
1010111	1	**LSB**
1111000	0	
1010101	0	
1011110	1	
1000100	0	
1001111	1	
1110101	1	
0110101	1	
M=10010111		

Figure. 3. Recover the least significant bits of the subpixels.

Step 5. Repeat steps 2 to 4 until you have recovered all the original messages.

Step 6. Segment the message into 8-bit blocks and convert its value to ASCII.

4. Results

The algorithms were implemented in the Java programming language, which is multiplatform, which allows it to be executed in any operating system that the Drone runs (apply steganography locally) or in an application from a mobile device or computer. (remotely).

Figure 4 shows a chaotically taken frame from a video captured from an Ar. Drone 2.0.

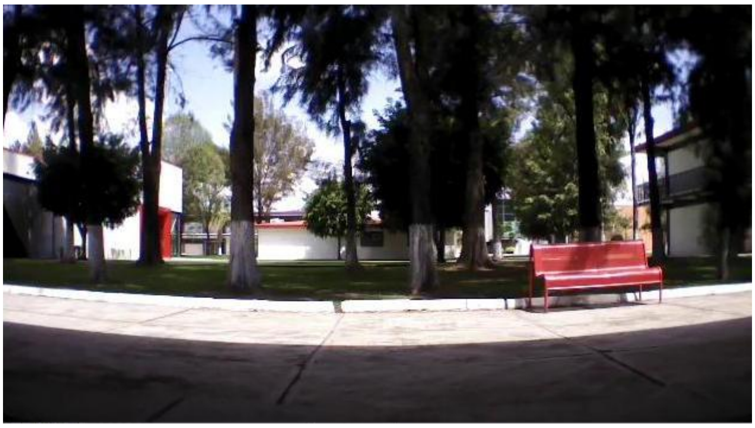

Figure. 4. Selected frame of a video.

Figure 5 shows the resulting steganography after hiding 511 characters in Figure 4; As can be seen, no changes visible to the human eye between the two are detected.

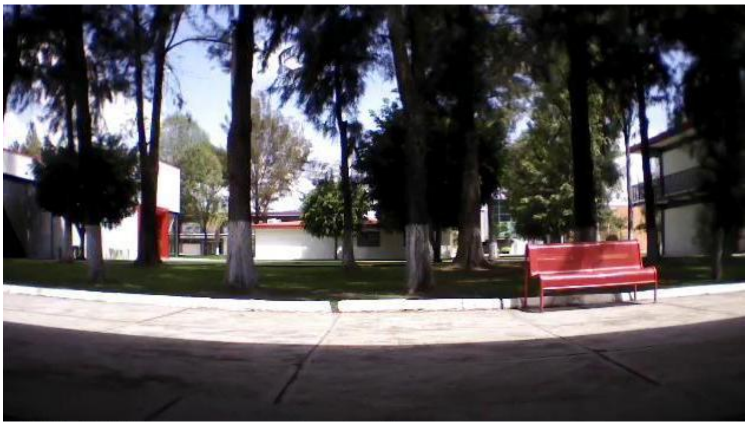

Figure. 5. Steganography with 511 hidden characters.

4.1 Correlation Diagrams

They allow evaluation of the existing relationship between two variables and results in the correlation coefficient that when it is very close to 0, there is a very little relationship, or if it is equal to 0, there is no coincidence; on the other hand, if the value is equal to 1 or -1, they are identical. To corroborate the differences between the pixels of Figure 4 and the steganography of Figure 5, the correlation diagrams shown in Figure 6 were made. In which all the R= coefficients can be observed. Based on the results, it is shown that the changes are practically imperceptible; In addition, if the attacker wishes to recover the data, he must know the keys that were used to select the positions of the pixels that were modified according to the chaotic systems.

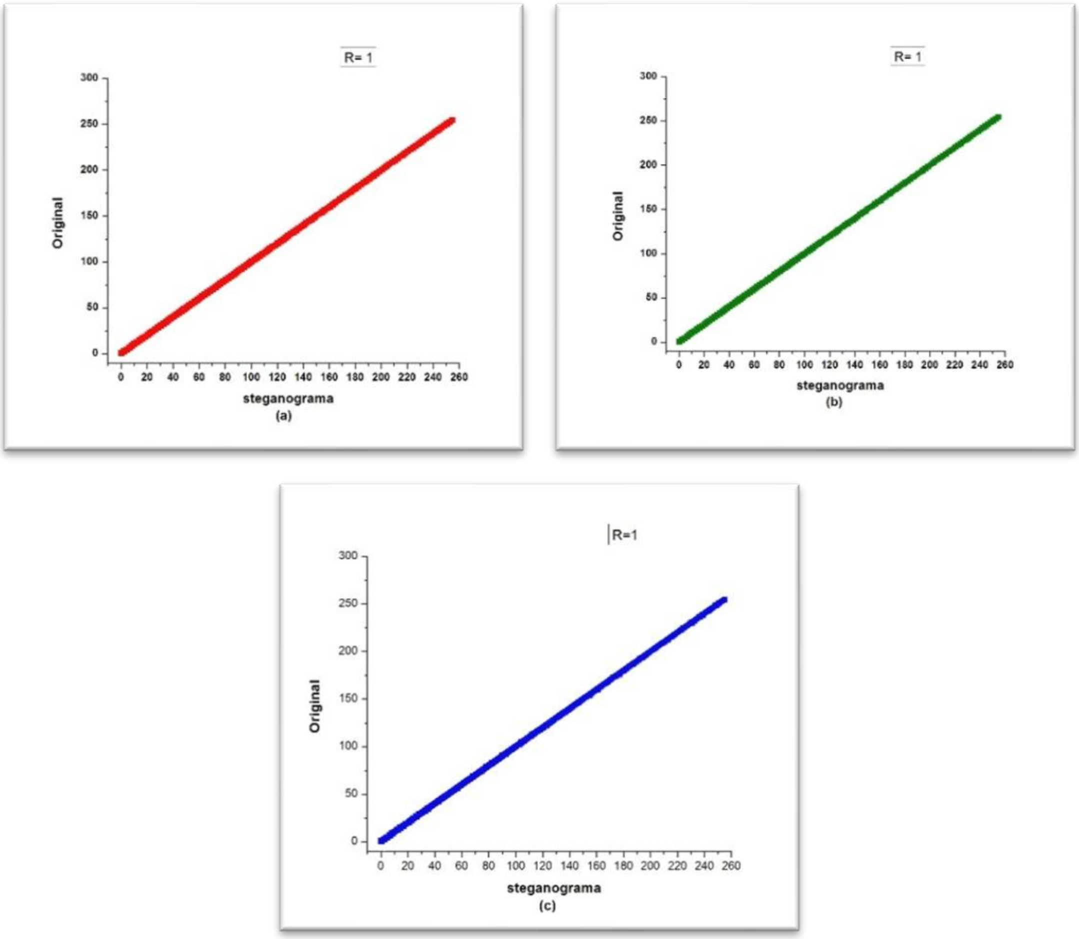

Figure. 6. Correlation of Figures 4 vs. 5, with respect to color intensity: (a) red, (b) green, and (c) blue.

The data recovered from the steganography and the original message were also compared to verify if there were any loss of information. The diagram is shown in Figure 7, which presents a coefficient. Therefore, there is no loss at the time of retrieving the hidden message.

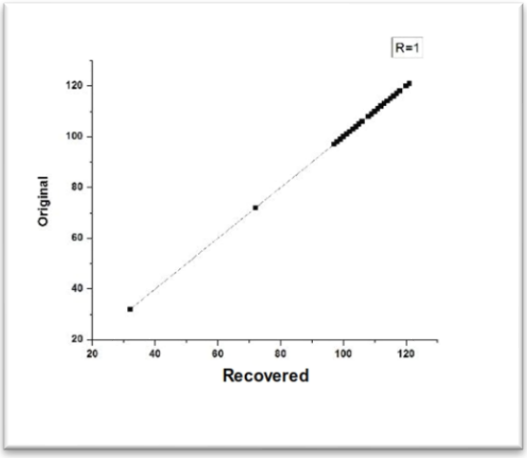

Figure. 7. Correlation original message recovered.

4.2 Histograms

Figure 8 shows the histograms of the RGB colors of both the original image and the steganography, with which it is possible to identify the frequency and distribution of the pixels in the images.

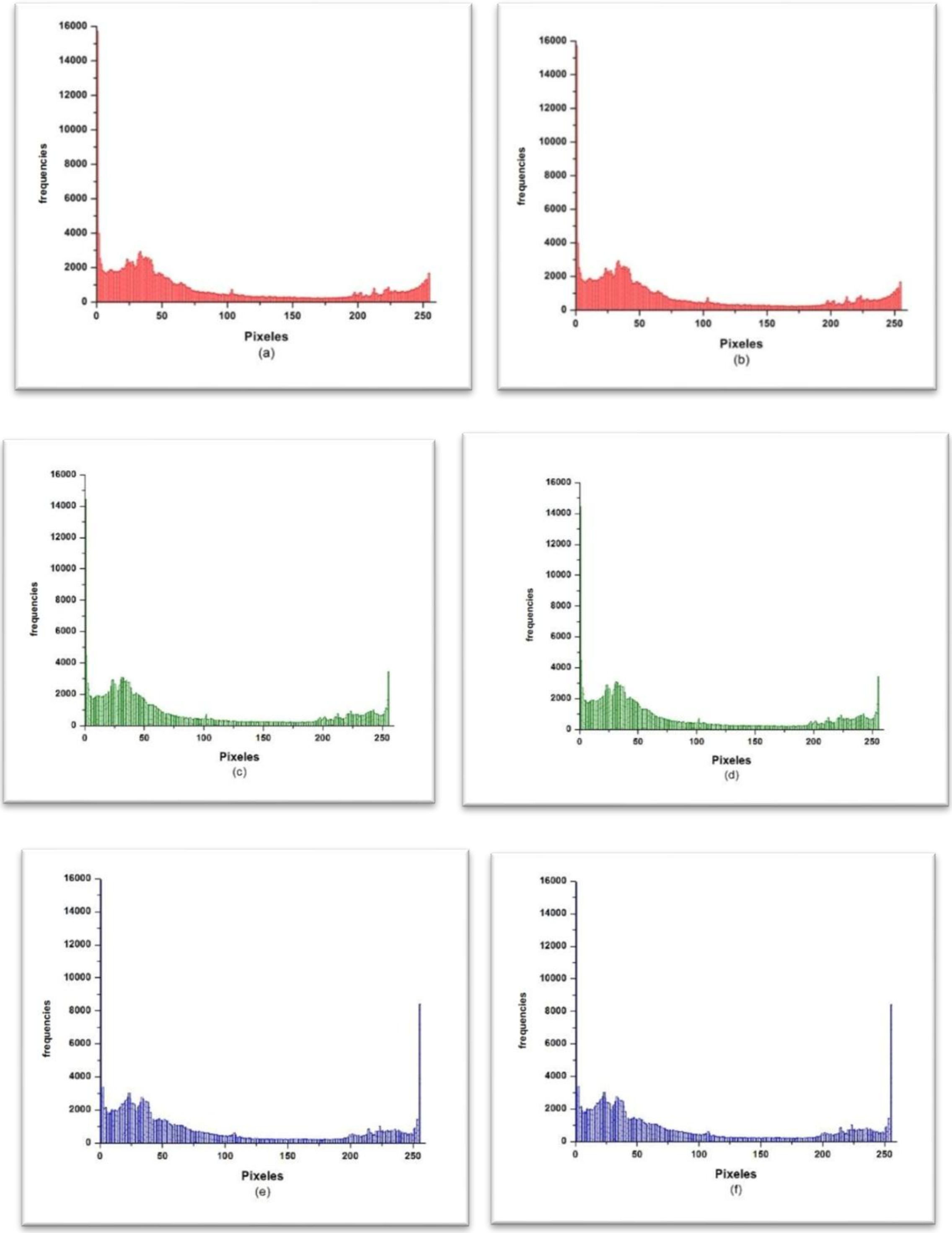

Figure. 8. Histograms: (a), (c), and (e) pixels of the original image; (b), (d), and (f) correspond to the steganography.

4.3 Statistical analysis

To detect if there are differences between the original image and the steganography, contrast, energy, and homogeneity tests were carried out according to the RGB colors that make them up, and it was detected that no alterations were shown between the images. The results can be seen in Table 1.

Pixels	Contrast	Energy	Homogeneity	Image
Red	1.5123e+10	8.5840e-06	1.1952e-04	**Original**
Green	1.4619e+10	8.7948e-06	1.2401e-04	
Blue	1.4313e+10	8.7636e-06	1.2068e-04	
Red	1.5123e+10	8.5840e-06	1.1952e-04	**steganography**
Green	1.4619e+10	8.7948e-06	1.2401e-04	
Blue	1.4313e+10	8.7636e-06	1.2068e-04	

Table 1. Statistical analysis.

5. Conclusions

An application was developed in Java for the management of Parrot's Ar.drone 2.0 or that implements sockets using the UDP protocol with ports 5554, 5555, and 5556. It allows capturing videos and then applying steganography, hiding a message in chaotically selected frames. The system was also used on a Raspberry, which can be attached to a weight-bearing drone.

The system provides reliability by taking advantage of the properties of chaotic mathematical models, such as high sensitivity to initial parameters and conditions, which are used as keys to hide the message. Therefore, only users who have knowledge of them can retrieve it. In addition, it was designed to use any mathematical model and not for a specific one; that is, any other that generates chaos can be implemented; the only requirement is that three orbits must be generated to apply steganography in videos.

It is proposed to implement the technique explained in this investigation to hide an identifier in the videos captured by the Drone locally or remotely, which would allow the Ministry of Communications and Transportation to determine from which device the videos were captured. The system guarantees the integrity of the hidden message verified through correlation diagrams, which compare the original message vs. the retrieved one. The proposed system can be used in different areas in which images are included, such as medicine, radiology, and photogeology.

Reference

[1] Alyousuf, F.Q.A., et al., *Analysis review on spatial and transform domain technique in digital steganography*. 2020. **9**(2): p. 573-581.

[2] Qasim, A.J. and F.Q.A.J.Q.Z.S.J. Alyousuf, *History of Image Digital Formats Using in Information Technology*. 2021. **6**(2): p. 1098-1112.

[3] Roshidi Din, O.G., Alaa Jabbar Qasim, *Analytical Review on Graphical Formats Used in Image Steganographic Compression*. Indonesian Journal of Electrical Engineering and Computer Science, 2018. **Vol 12, No 2**: p. pp. 441~446.

[4] Zaidan, B., et al., *Stego-Image Vs Stego-Analysis System*. International Journal of Computer and Electrical Engineering, 2009. **1**(5): p. 572.

[5] QASSIM, A.J. and Y. SUDHAKAR, *Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm*. 2015.

[6] Tayel, M., H. Shawky, and A.E.-D.S. Hafez. *A new chaos steganography algorithm for hiding multimedia data*. in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*. 2012. IEEE.

[7] Qasim, A.J., et al., *Review on techniques and file formats of image compression*. 2020. **9**(2): p. 602–610.

[8] Altaay, A.A.J., S.B. Sahib, and M. Zamani. *An introduction to image steganography techniques*. in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. 2012. IEEE.

[9] Chae, J.J. and B. Manjunath. *Data hiding in video*. in *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*. 1999. IEEE.

[10] Al-Frajat, A., et al., *Hiding data in video file: An overview*. J. Appl. Sci, 2010. **10**(15): p. 1644-1649.

[11] Jalab, H., A. Zaidan, and B. Zaidan, *Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation*. arXiv preprint arXiv:0912.3986, 2009.

[12] Bhattacharyya, S., *A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier*. Journal of global research in computer science, 2011. **2**(4).

[13] Kareem, Hassanain Raheem, Hadi Hussein Madhi, and Keyan Abdul-Aziz Mutlaq. "Hiding encrypted text in image steganography." Periodicals of Engineering and Natural Sciences (PEN) 8.2 (2020): 703-707..

[14] Madhi, H.H., et al., *Pixel steganography method for grayscale image steganography on colour images*. 2021. **9**(3): p. 615-624.

[15] Kareem, H.R., et al., *Hiding encrypted text in image steganography*. 2020. **8**(2): p. 703-707.

[16] Zhang, T. and X. Ping. *A fast and effective steganalytic technique against JSteg-like algorithms*. in *Proceedings of the 2003 ACM symposium on Applied computing*. 2003.

[17] Boehm, B.J.a.p.a., *Stegexpose-A tool for detecting LSB steganography*. 2014.

[18] Sumathi, C., T. Santanam, and G.J.a.p.a. Umamaheswari, *A study of various steganographic techniques used for information hiding*. 2014.

[19] Meghanathan, N., L.J.I.J.o.N.S. Nayak, and I. Application, *Steganalysis algorithms for detecting the hidden information in image, audio and video cover media*. 2010. **2**(1): p. 43-55.

[20] Jiménez-Rodríguez, M., et al., *Steganography applied in the origin claim of pictures captured by drones based on chaos*. 2018. **38**(2): p. 61-69.

[21] Patidar, V., et al., *A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption*. 2011. **284**(19): p. 4331-4339.

[22] Lerch-Hostalot, D., D.J.C. Megias, and security, *LSB matching steganalysis based on patterns of pixel differences and random embedding*. 2013. **32**: p. 192-206.

[23] Chhikara, R. and L.J.I.J.E.I.T. Singh, *A review on digital image Steganalysis techniques categorised by features extracted*. 2013. **3**(4).

[24] Fridrich, J. and M. Long. *Steganalysis of LSB encoding in color images*. in *2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532)*. 2000. IEEE.