Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 109-118
Published by *Majmuah Enterprise*
www.majmuah.com

Comparison Of Steganographic Techniques of Spatial Domain and Frequency Domain in Digital Images

ALAA JABBAR QASIM ALMALIKI and ROSHIDI DIN
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email : *alaa_jabbar@ahsgs.uum.edu.my,roshidi@uum.edu.my* | Tel: *+60184020823 +60175981306*|

Received: September 22, 2023
Accepted: September 25, 2023
Online Published: September 26, 2023

Abstract

Steganography studies different techniques for hiding data in other objects, known as carrier objects. These carrier objects are usually digital media, such as images, videos or sound files. However, without a doubt, the most widely used media today are images due to their wide dissemination on the Internet (Zaidoon Kh Al-Ani, AA Zaidan, BB Zaidan, & Hamdan Alanazi, 2010; Anderson & Petitcolas, 1998; G. Kaur & Kochhar, 2012; Nag, Biswas, Sarkar, & Sarkar, 2010; Petitcolas, Anderson, & Kuhn, 1999). Digital images undergo certain changes in the matrix that composes them, causing the digital image to be distorted or present any change (Naji, Zaidan, Zaidan, Hameed, & Khalifa, 2009). This work evaluated steganographic techniques of Spatial Domain (DE) and Frequency Domain (DF) for the concealment of information applied in RGB, Grayscale, YCbCr and YUV colour spaces based on the imperceptibility of information in Digital images. The first technique allows hiding information in the image pixels based on the Least Significant Bit (LSB) method by altering the binarised pixel's last bit. The second technique allows for hiding information in the low frequencies of the image based on the Discrete Cosine Transform (DCT) by altering the binarized AC coefficients using the Least Significant Bit (LSB) method. Both techniques process the Digital Image and show; as a result, a new Digital Image with hidden information.

Keywords: Spatial Domain, Frequency Domain, RGB, YCbCr, YUV, steganography, DCT, Image.

1. Introduction

During the concealment of information in a carrier, such as digital images, they undergo alterations in the matrix that composes it, making evident distortions or any changes in it. The drawback presented in the process is that these Distortions are mostly visible to the human eye, making the digital image perceptible and suspicious that there is information within the digital image (Zaidoon Kh Al-Ani, AA Zaidan, BB Zaidan, & Hamdan Alanazi, 2010; Badr, Ismaial, & Khalil, 2014; Banik & Bandyopadhyay, 2015; Yahya & Yahya, 2019). The main purpose of this work is to compare steganographic techniques for hiding information in digital images in different colour spaces. The implementation of steganography in digital images is a research topic that has precedents, (M. Kaur, Kaur, & technologies, 2014) propose a method that is based on hiding information in the pixels, applying the Least Significant Bit (LSB) in a digital image of Windows Bitmap (BMP) format in Grayscale, and(Hussain, Wahab, Idris, Ho, & Jung, 2018), propose a method that is based on hiding information in the AC coefficients by applying Discrete Cosine Transform (DCT), for its robustness in compressions Join Photographic Experts Group (JPEG).The Spatial Domain (DE) steganographic technique alters the pixels of the digital image matrix in different colour spaces, and the Frequency Domain (DF) technique alters the AC coefficients obtained by the Discrete Cosine Transform (DCT). In calculating the low frequencies of images in different colour spaces, both techniques use Least Significant Bit (LSB) to insert information. In the experimental results, based on imperceptibility in digital images, a classification from 0 to 2 was assigned, where 0 is low, 1 is medium, and 2 is high, showing that DE in its RGB, Grayscale, YCbCr and YCbCr colour spaces YUV, having a classification average of 2, is better than the DF technique in its grayscale colour spaces with a classification average of 1.39, YCbCr with a classification average of 1.37, and YUV with a classification average of 1.27.

2. Related jobs

Previous investigations found methods to hide information in digital images; (M. Kaur et al., 2014) propose a method to hide information in grayscale digital images using Windows Bitmap (BMP). For the insertion, it used the Least Significant Bit (LSB), which consists of modifying the last bit of the binarized pixels once the binarized information has been obtained, which is to be hidden. At the end of the proposal, an application was developed where the user can select a digital image in Grayscale and enter a message to be hidden once obtained the covert digital image. It goes through 3 processes, fidelity, unaffected elements, and Signal Noise Ratio (SNR) of the covert digital image, to observe

any variation in the digital image. In the research by (Yahya & Yahya, 2019), I develop a method to hide information in digital images in greyscale, robust to Join Photographic Experts Group (JPEG) compressions. For the insertion of information in digital images, I use the Least Significant Bit (LSB) to modify the last bit of the binarized AC coefficients of the digital image, calculated by the Discrete Cosine Transform (DCT) once the encoded information has been obtained with the help of the GOLAY Linear Binary Code (23.7) that you want to hide. At the end of the proposal, an application was developed where the user can select a grayscale image and enter a message to be camouflaged. Once the covert digital image is obtained, it goes through 3 processes Join Photographic Experts Group (JPEG) compression attacks, Gaussian Noise attack and Impulsive Noise attack to see how robust it is against those attacks. In the research by (Subramanian, Santhanam, & Karunanithi, 2023), they developed a method to be able to hide information in different places of the digital colour images using graph traversal. To do this, operators, restrictions, and the elaboration of the graph according to the movement of the horse. At the end of the proposal, I developed an application where the user can select a colour digital image and entering a message to be camouflaged. Once the covert digital image is obtained, it goes through an average colour image per channel to observe the changes in the 3 RGB channels of the image.

3. Methodology

In order to identify the best technique for hiding information in digital images, using steganography to see the degree of imperceptibility, we propose to compare two techniques for hiding information in digital images. The first Spatial Domain (DE) technique is based on hiding the information in the pixels of the digital image, applying the Least Significant Bit (LSB). The second DF technique is based on hiding the information in the digital image in the AC coefficients, applying the Least Significant Bit (LSB), calculating the frequencies, and using the Discrete Cosine Transform (DCT).

3.1 Spatial Domain

The technique is based on research (Hussain et al., 2018), where information is hidden in digital images of BMP format in Grayscale. The technique uses the Least Significant Bit (LSB) to hide the information in the pixels of the digital image

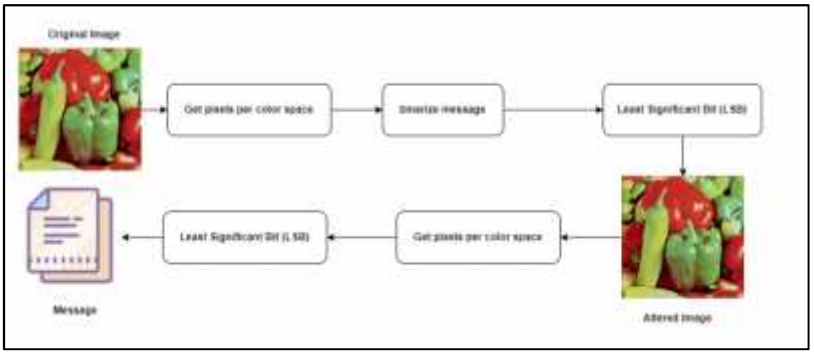


Figure 1: Illustration of the process of concealment and recovery of the message in digital images applying Spatial Domain (DE).

a. Get pixels per colour space.

The digital image is obtained, the colour space is selected, and we proceed to go through the entire matrix in order to obtain the pixels that vary from 0 to 255(Chhabra et al., 2022; Dumitrescu, Wu, & Memon, 2002; Fridrich & Long, 2000; Gupta, Shukla, Gupta, & Things, 2022).

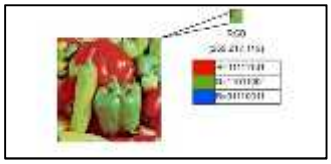


Figure 2: Illustration of obtaining pixels from the digital image in RGB.

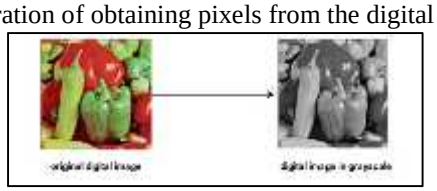


Figure 3: Illustration of conversion of the Digital Image in RGB to Gray Scale.

Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 109-118
Published by *Majmuah Enterprise*
www.majmuah.com

$$Y = A \quad (R, G, B) = \frac{R+G+B}{3} \tag{1}$$

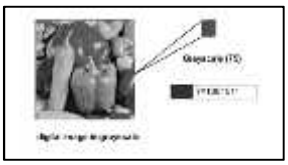


Figure 4: Illustration of obtaining pixels from the digital image in Grayscale.

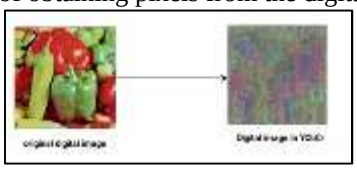


Figure 5: Illustration of obtaining pixels from the digital image in Grayscale.

$$Y = w_K * R + (1 - w_B - w_K) * G + w_B * B \tag{2}$$

$$C_b = \frac{0.5}{1 - W_B} * (B - Y) \tag{3}$$

$$C_b = \frac{0.5}{1 - w_R} * (R - Y) \tag{4}$$

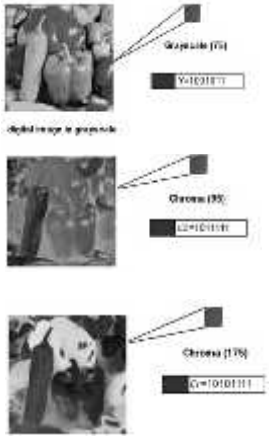


Figure 6: Illustration of obtaining pixels from the digital image in YCbCr.

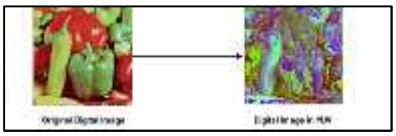


Figure 7: Illustration of conversion of the Digital Image in RGB to YUV.

$$Y = 0.299 * R + 0.587 * G + 0.114 * B \tag{5}$$

$$U = 0.492 * (B - Y) \tag{6}$$

$$V = 0.877 * (R - Y) \tag{7}$$

Figure 8: Illustration of obtaining pixels from the digital image in YUV.

b. Binarize Message

The message or phrase is broken down into characters, obtaining its decimals located in the ASCII code.

Table 1: Binarization of the phrase "hello" according to the ASCII code

Character	h	o	l	a
ASCII code	68	111	108	97
binary	0	0	0	0
	1	1	1	1
	1	1	1	1
	0	0	0	0
	1	1	1	0
	0	1	1	0
	0	1	0	0
	0	1	0	1

c. Least Significant Bit (LSB) method

The pixels are modified by applying the Least Significant Bit (LSB), which consists of changing the last bit of the pixel (Dumitrescu et al., 2002; Fridrich & Long, 2000; Havrysh, Tymchenko, & Izonin, 2022; Setiadi, 2022).

Table 2: Insertion of information applying Least Significant Bit (LSB) in a digital image in RGB.

pixels	Information	Steganographic Pixels
R=11111101	0	R=11111100
G=11011001	1	G=11011001
B=01110011	1	B=01110011
.	.	.
.	.	.
.	.	.

Table 3: Insertion of information applying Least Significant Bit (LSB) in a grayscale digital image.

pixels	Information	Steganographic Pixels
L=1001011	0	**L**=1001010
.	.	.
.	.	.
.	.	.

Table 4: Insertion of information applying Least Significant Bit (LSB) in a digital image in YCbCr

pixels	Information	Steganographic Pixels
L=1001011	0	**L**=1001010
C_b=1011111	1	C_b=1011111
C_b=10101111	1	C_b=10101111
.	.	.
.	.	.
.	.	.

Table 5: Insertion of information applying Least Significant Bit (LSB) in a digital image in YUV.

pixels	Information	Steganographic Pixels
L=1001011	0	**L**=1001010
U=10101010	1	U=10101011
V=1010000	1	V=1010001
.	.	.
.	.	.
.	.	.

Then we proceed to rebuild and convert the digital image according to its colour space, returning to its original state.

3.2. Frequency Domain

The technique is based on research (Kafri & Suleiman, 2009), where information is hidden in grayscale digital images. The technique uses the Least Significant Bit (LSB) method to hide the information, in the AC coefficients, in the calculated digital image, with the Discrete Cosine Transform (DCT)(Alyousuf, Din, Qasim, & Informatics, 2020; Din, Mahmuddin, Qasim, & Technology, 2019; Din, Qasim, & Informatics, 2019; QASSIM & SUDHAKAR, 2015; Roshidi Din, 2018).

Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 109-118
Published by *Majmuah Enterprise*
www.majmuah.com

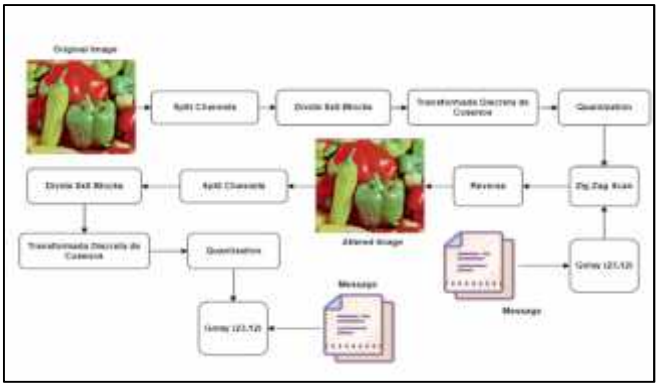


Figure 9: Illustration of the process of concealment and recovery of the message in digital images applying Frequency Domain (DF)

a. Split Channels

The digital image is selected for the colour space to be applied and proceeds to divide into the channels that make it up.

$$Y = A \quad (R, G, B) = \frac{R+G+B}{3} \tag{2}$$

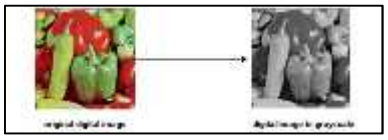


Figure 10: Convert RGB digital image to Grayscale divided into one channel.

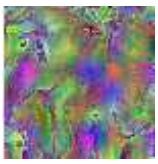
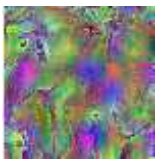
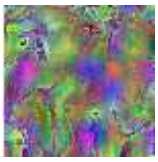
digital image	digital image in YCbCr	YCbCr divided into three channels	Equation No	Output Image
		$Y = w_R * R + (1 - w_B - w_R) * G + w_B * B$	(2)	
		$C_b = \frac{0.5}{1-W_B} * (B - Y)$	(4)	
		$C_b = \frac{0.5}{1-w_R} * (R - Y)$	(7)	

Figure 11: Convert RGB digital image to YCbCr divided into three channels.

Digital Image	digital Image in YUV	YUV Divided into Three Channels	Equation No	Output Image

Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 109-118
Published by *Majmuah Enterprise*
www.majmuah.com

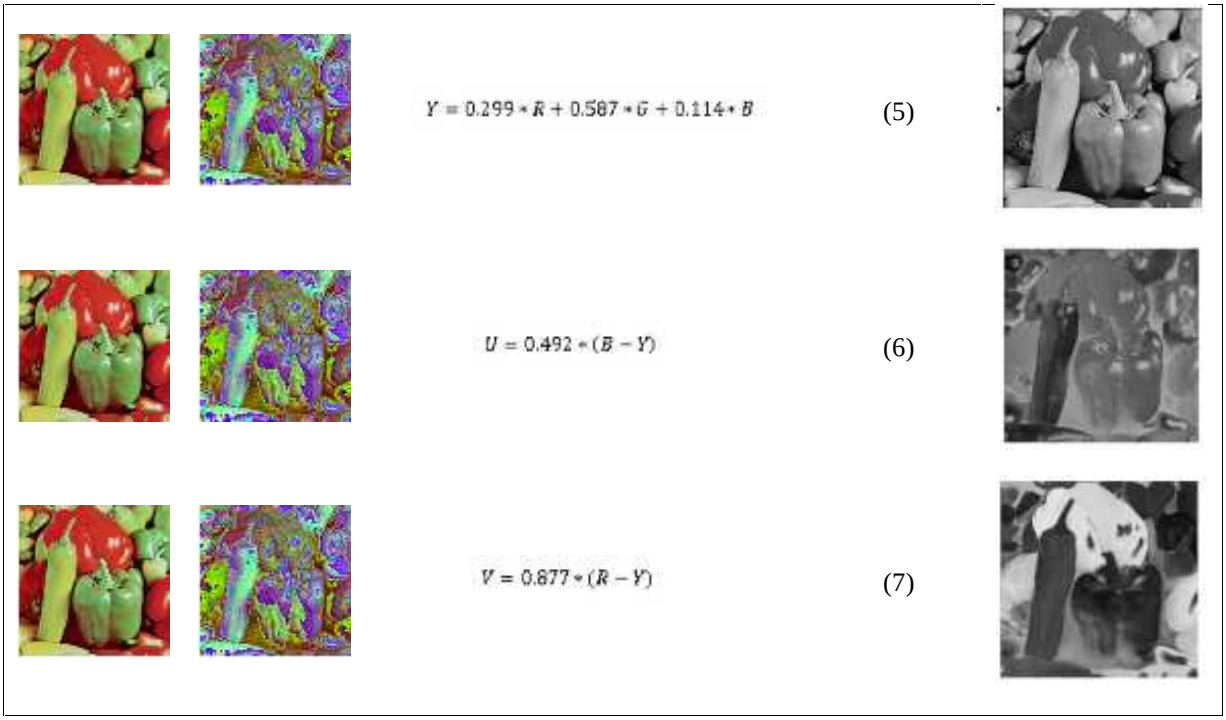


Figure 12: Convert RGB digital image into YUV divided into three channels.

b. Divide 8x8 Blocks

The digital image is divided into sub-images or 8x8 blocks. It is done in order to avoid loss of quality during image processing.

$A = (a_{ij})_{m}$, where $m = n$

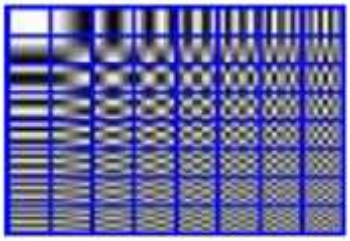


Figure 13: Dividing the Digital Image into 8x8 Blocks.

c. Discrete Cosine Transform (DCT)

The pixels of the 8x8 blocks of the digital image of each channel are calculated.

$$S(u,v) = \frac{2}{N} C(u)\, C(v) \sum_{X}^{N} \sum_{Y}^{N} S(x,y) \cos\left(\frac{\pi\ (2x+1)}{2N}\right)\cos\left(\frac{\pi\ (2x+1)}{2N}\right) \quad (8)$$

S(u,v) is the value of the coefficient of row "u" and column "v", where their values vary from 0 to 7. To obtain the value of the coefficient, we proceed to see the coefficients C(u) and C(v) taking these values. When u and/or v are equal to zero, its value of C(u,v) cs√(1/N) And when they are greater than zero and less than N-1, their value cs√(1/N) Where N is equal to 8, the sums of x and y go through the matrices from 0 to 7, in order to obtain the value S (x, y), which represents the pixel, and proceed to calculate the cosines, in order to obtain the value of the coefficient, this process is repeated for all the pixels(Alaa Jabbar & Farah Qasim Ahmed, 2021).

d. Quantization

In this phase, the greatest number of zeros possible is obtained to greatly reduce the amount of information in the high-frequency components and is done by applying this formula:

$$C = r \qquad \left(\frac{F}{E}\right) \quad (9)$$

FB=8x8 block frequency , ES=JPEG Standard Element

Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 109-118
Published by *Majmuah Enterprise*
www.majmuah.com

$$B = \sum_{i=0}^{m-1}\sum_{i=0}^{n-1} b_{i,} \; ; \text{ where } 9 < b_{i,} \leq 121$$

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Figure 14: JPEG Standard Matrix

$$C = \sum_{i=0}^{m-1}\sum_{i=0}^{n-1} c_{i,} \; ; \text{ where } 16 < c_{i,} \leq 99$$

$$\begin{bmatrix} 17 & 18 & 24 & 47 & 66 & 99 & 99 & 99 \\ 18 & 21 & 26 & 66 & 99 & 99 & 99 & 99 \\ 24 & 26 & 56 & 99 & 99 & 99 & 69 & 56 \\ 47 & 66 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \end{bmatrix}$$

Figure 15: Matrix JPEG colour

The same process is carried out for the Chrominance using the Matrix of Fig. 15.

e. Information Coding

The message is broken down into characters, and the decimal that corresponds to it is located in the ASCII code to binarize. Then the binary information goes through an encoder, applying a Code GOLAY Linear Binary (23,7).

f. Zig Zag Scan

Order the AC coefficients of each 8x8 luminance block. Then it begins to modify the first 8 AC coefficients of each 8x8 block, with the Least Significant Bit (LSB) method inserting the encoded information.

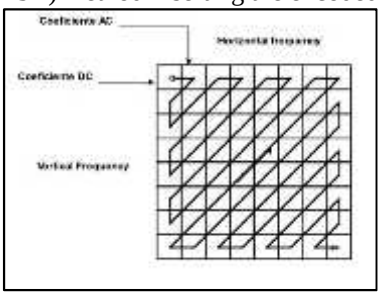


Figure 16: Zig-Zag arrangement

g. Reverse

After sorting the AC coefficients, they are restored to their original position. Afterwards, the quantization is carried out, the frequencies of the 8x8 block of luminance are multiplied by the Standard JPEG matrix. It also proceeds for the chrominance by the colour JPEG matrix. Then we use the Inverse Discrete Cosine Transform (IDCT) to return their values from before.

$$S(u,v) = \frac{2}{N}\sum_{X=0}^{N-1}\sum_{Y=0}^{N-1} C(u)\,C(v)S(x,y)\cos\left(\frac{\pi\ (2x+1)}{2N}\right)\cos\left(\frac{\pi\ (2x+1)}{2N}\right) \quad (10)$$

S(u,v) is the value of the pixel of the row "u" and the column "v", where their values vary from 0 to 7. To obtain the coefficient's value, we see the coefficients C(u) and C(v) taking these values. When u and/or v are equal to zero, its value of C(u,v) cs√(1/N) And when they are greater than zero and less than N-1, their value cs√(1/N) Where N is equal to 8, the sums of x and y go through the matrices from 0 to 7, to obtain the value S (x, y), which represents the

coefficient, and proceed to calculate the cosines, to obtain the value of the pixels, this process is repeated for all coefficients. Then we rebuild the Digital Image and convert it to its original appearance depending on the colour space.

h. Recover Information

The recovery process must be applied to steps a, b, c, d, e and f. It extracts information from the AC coefficients, applying Least Significant Bit (LSB). Once the information is recovered, it is decoded with the GOLAY Linear Binary Code (23.7). Once the bits have been decoded, are grouped into bytes to convert them into decimals, and consult the ASCII code to reconstruct the message. Once the covert digital images of both techniques have been obtained, they will go through certain processes to confirm the degree of imperceptibility.

4.Experiments

To evaluate the 2 techniques, a digital image repository composed of 30,607 digital images was used, of which 41 were evaluated for each technique.

a. Information Coding

$$EA = \sum_{i=1}^{N} \sum_{j=1}^{N} 1(X_i, Y_j) \quad (11)$$

This measurement results from the elements affected in the digital image by hiding a message in the different colour spaces.

Table 6: Number of Affected Elements in the Spatial Domain (DE)

Number of elements affected in the Spatial Domain (DE)			
color space	**No**	**Half**	**Standard deviation**
Grayscale	41	1469873,63	921047,537
RGB	41	5256,29	22159,799
YCbCr	41	611693,24	373020,174
YUV	41	581420,73	377593,917

Table 7: Number of Affected Elements in the Frequency Domain (DF).

Number of affected elements in the Frequency Domain (DF)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**1431408,32**	**910779,247**
YCbCr	**41**	**1172631,63**	**745480,934**
YUV	**41**	**1172213,02**	**738650,686**

Tables 6 and 7 show that between colour spaces in both techniques, the one with the least affected elements is in table 6. The Domain Spatial (SD) in RGB has fewer elements affected, with a standard deviation of 22159.799 compared to the other colour spaces.

b. Number of Wrong Characters

$$C = \sum_{i=0}^{n} c(X_i) \quad (12)$$

This measurement results from the erroneous characters when retrieving the message from the disguised digital image.

Table 8: Number of erroneous characters in the Spatial Domain (DE)

Number of elements affected in the Spatial Domain (DE)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**0**	**0**
RGB	**41**	**0**	**0**
YCbCr	**41**	**57,46**	**187,379**
YUV	**41**	**28,63**	**75,635**

Table 9: Number of erroneous characters in the Frequency Domain (DF)

Number of affected elements in the Frequency Domain (DF)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**58,59**	**244,958**
YCbCr	**41**	**80,20**	**251,858**
YUV	**41**	**122,10**	**291,112**

Tables 8 and 9 show that between the colour space in both techniques, the one with the least affected elements is in table 8. The Spatial Domain (DE) in Grayscale and RGB has fewer erroneous characters with a standard deviation from 0.

c. Visual Detection

The results of the Visual Detection of the digital images were classified by the degree of imperceptibility through the human eye.

Table 10: Classification by degree of imperceptibility in the Spatial Domain (DE)

Number of elements affected in the Spatial Domain (DE)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**2.00**	**0**
RGB	**41**	**2.00**	**0**
YCbCr	**41**	**2.00**	**0**
YUV	**41**	**2.00**	**0**

Table 11: Classification by degree of imperceptibility in the Frequency Domain (DF)

Number of affected elements in the Frequency Domain (DF)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**1,39**	**0.771**
YCbCr	**41**	**1,37**	**0.829**
YUV	**41**	**1.27**	**0.837**

Tables 10 and 11 show that among the colour spaces in both techniques, the one with the highest degree of imperceptibility with values between 0 and 2, where 0 is low, 1 is medium, and 2 is high, is table 10. The Spatial Domain (DE), in all the applied colour spaces, has an average classification of 2, thus being the highest degree of imperceptibility.

5. Image Fidelity

$$F = 1 - \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(\mathbb{I}(m,n) - \mathbb{I}(m,n))^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\mathbb{I}(m,n)^2} \quad (13)$$

This measure results from the fidelity of the digital image by camouflaging a message, altering the appearance of the digital image.

Table 12: Percentage of fidelity of the digital image in the Spatial Domain (DE)

Number of elements affected in the Spatial Domain (DE)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**90,7463**	**8,14855**
RGB	**41**	**99,9985**	**,00358**
YCbCr	**41**	**99,9473**	**,26387**
YUV	**41**	**99,9485**	**,26390**

Table 12: Percentage of fidelity of the digital image in the Frequency Domain (DF)

Number of affected elements in the Frequency Domain (DF)			
colour space	**No**	**Half**	**Standard deviation**
Grayscale	**41**	**90,0978**	**8,20693**
YCbCr	**41**	**97,1361**	**10,74432**
YUV	**41**	**96,6239**	**11,03911**

In tables 12 and 13, it can be seen that between colour spaces in both techniques, the one with the highest percentage of fidelity in digital images is Table 12. In the Spatial Domain (DE), it can be considered that applied in RGB, YCbCr and YUV colour spaces, its fidelity is greater than 99%, behaving in a stable manner. On the other hand, in the grayscale, it is considered stable, despite the fact that its fidelity is 90.75%.

6.Conclusions

After the tests were carried out, it was determined that the most efficient technique in the degree of imperceptibility - which does not vary the appearance of the image in a large amount despite the modification of its pixels - is the Spatial Domain (DE) technique, which obtained a fidelity in grey scale of 90.75%, and in RGB, YCbCr and YUV not less than 99%; and achieved a Class 2 imperceptibility rating in all applied colour spaces. In the future, the use of steganography in other digital carriers, such as audio and video, will be explored to see the degree of auditory and visual perception.

References

Al-Ani, Z. K., Zaidan, A., Zaidan, B., & Alanazi, H. (2010). Overview: Main fundamentals for steganography. *arXiv preprint arXiv:1003.4086*.

Al-Ani, Z. K., Zaidan, A., Zaidan, B., & Alanazi, H. (2010). Overview: Main fundamentals for steganography.

Alaa Jabbar, Q., & Farah Qasim Ahmed, A. (2021). History of Image Digital Formats Using in Information Technology. *QALAAI ZANIST JOURNAL, 6*(2), 1098-1112. doi:10.25212/lfu.qzj.6.2.41

Alyousuf, F. Q. A., Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2020). Analysis review on spatial and transform domain technique in digital steganography. *9*(2), 573-581.

Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. *IEEE Journal on selected areas in communications, 16*(4), 474-481.

Badr, S. M., Ismaial, G., & Khalil, A. H. (2014). A review on steganalysis techniques: from image format point of view. *102*(4).

Banik, B. G., & Bandyopadhyay, S. K. (2015). Review on steganography in digital media. *4*(2), 265-274.

Chhabra, A., Woeden, T., Singh, D., Rakhra, M., Dahiya, O., & Gupta, A. (2022). *Image Steganalysis with Image decoder using LSB and MSB Technique.* Paper presented at the 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM).

Din, R., Mahmuddin, M., Qasim, A. J. J. I. J. o. E., & Technology. (2019). Review on steganography methods in multi-media domain. *8*(1.7), 288-292.

Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2019). Steganography analysis techniques applied to audio and image files. *8*(4), 1297–1302.

Dumitrescu, S., Wu, X., & Memon, N. (2002). *On steganalysis of random LSB embedding in continuous-tone images.* Paper presented at the Proceedings. International conference on image processing.

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

Gupta, A., Shukla, H., Gupta, M. J. N. J. f. A. I., & Things, I. o. (2022). A secure image steganography using X86 assembly LSB. *1*(1), 38-47.

Havrysh, B., Tymchenko, O., & Izonin, I. (2022). *Modification of the LSB Implementation Method of Digital Watermarks.* Paper presented at the The International Conference on Artificial Intelligence and Logistics Engineering.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K.-H. (2018). Image steganography in spatial domain: A survey. *65*, 46-66.

Kafri, N. M., & Suleiman, H. Y. (2009). *Bit-4 of frequency domain-DCT steganography technique.* Paper presented at the 2009 First International Conference on Networked Digital Technologies.

Kaur, G., & Kochhar, A. (2012). A steganography implementation based on LSB & DCT. *International Journal for Science and Emerging Technologies with Latest Trends, 4*(1), 35-41.

Kaur, M., Kaur, G. J. I. j. o. c. s., & technologies, i. (2014). Review of various steganalysis techniques. *5*(2), 1744-1747.

Nag, A., Biswas, S., Sarkar, D., & Sarkar, P. P. (2010). A novel technique for image steganography based on Block-DCT and Huffman Encoding. *arXiv preprint arXiv:1006.1186*.

Naji, A., Zaidan, A., Zaidan, B., Hameed, S. A., & Khalifa, O. O. (2009). Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography. *International Journal of Computer Science and Network Security.[On-line], 9*(5), 294-300.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

QASSIM, A. J., & SUDHAKAR, Y. (2015). Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm.

Roshidi Din, O. G., Alaa Jabbar Qasim. (2018). Analytical Review on Graphical Formats Used in Image Steganographic Compression. *Indonesian Journal of Electrical Engineering and Computer Science, Vol 12, No 2*, pp. 441~446. doi: 10.11591

Setiadi. (2022). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection.

Subramanian, P., Santhanam, S., & Karunanithi, H. (2023). *Image steganography using reversible data hiding approach.* Paper presented at the AIP Conference Proceedings.

Yahya, A., & Yahya, A. J. S. t. f. d. i. (2019). Steganography techniques. 9-42.