Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 42, S. 71-76, Ekim 2022

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 42, pp. 71-76, October 2022

Research Article

Data Hiding Based on Frequency Domain Image Steganography

Abdiwahab Mohamed Abdirashid[1*] , Serdar Solak [2], Aditya Kumar Sahu [3]

[1*] Department of Information Systems Engineering, Kocaeli University, 41001, Kocaeli, Turkey,(ORCID: 0000-0001-8247-7379), cabdalamoh@gmail.com
[2] Department of Information Systems Engineering, Kocaeli University, 41001, Kocaeli, Turkey,(ORCID: 0000-0003-1081-1598), serdars@kocaeli.edu.tr
[3] Amrita School of Computing, Amaravati Campus, Amrita Vishwa Vidyapeetham, Amaravati, Guntur – 522502, Andhra Pradesh, India, (ORCID: 0000-0003-4257-0688), adityasahu.cse@gmail.com

(2nd International Conference on Engineering and Applied Natural Sciences ICEANS 2022, October 15 - 18, 2022)

(**DOI:** 10.31590/ejosat.1188597)

ATIF/REFERENCE: Abdirashid, A. M., Solak, S., & Sahu, A. K. (2022). Data Hiding Based on Frequency Domain Image Steganography. *European Journal of Science and Technology*, (42), 71-76.

Abstract

The rapid development in the field of communication and technology has led to a heavy increase in the data produced in digital environment, and the need to take various active security measures has arisen in the case of robust secured data and end-to-end transmission. In line with this need, widely used methods developed are Cryptography which scrambles the data to secure the information, and Steganography techniques aiming to conceal data in digital objects so third parties cannot detect the transmitted content. Image steganography techniques can be divided into two groups: spatial domain and transform domain. Spatial domain techniques embed messages directly in the intensity of the pixels, while the transform domains also known as frequency domain images are first transformed and then the message is embedded in the image. Many practices have been offered and developed in the literature to provide secure transmission of the data. In this paper, data-hiding techniques based on frequency domain image steganography has proposed. Among these techniques, the working principle of DFT has been explained, DCT and DWT techniques performed to embed and extract secret data. As a result of the proposed methods, it has been achieved to obtain the maximum data embedding capacity in the cover image by minimizing the distortion in the stego image. It has been observed that the size and quality of the JPEG stego images have been obtained without deterioration after the data is hidden. The experimental results show successful extraction of the accurate secret message. Some good PSNR of ≈50 dB and SSIM results of the proposed methods can represent successful restoration for the same image.

Keywords: Information Security, DCT, DWT, DFT, Frequency Domain, Data Hiding.

Frekans Alanı Görüntü Steganografisine Dayalı Veri Gizleme

Öz

Internet ortamında, sağlam ve güvenli veri aktarımı söz konusu olduğunda, çeşitli aktif güvenlik önlemlerine ihtiyaç duyulmaktadır. Bu ihtiyaç doğrultusunda yaygın olarak, şifreleme ve veri gizleme teknikleri kullanılır. Şifreleme veriyi anlaşılmayacak şekilde karıştırırken, veri gizleme ise verinin varlığını anlaşılmayacak şekilde gizlemektir. Veri gizleme işleminde görüntülere veri gizlenmesi, Görüntü Steganografisi olarak bilinir. Görüntü steganografinde kullanılan teknikler uzamsal alan ve dönüşüm alanı iki grupta incelenir. Uzamsal alan teknikleri, gizlenecek bilgileri doğrudan piksellere yerleştirirken, frekans alan tekniklerinde dönüşüm işlemi gerçekleştirilir ve bilgi gizlemesi yapılır. Makalede, frekans dönüşüm alanına dayalı veri gizleme teknikleri kullanılmaktadır. Gizli verileri gömmek ve çıkarmak için DCT ve DWT teknikleri uygulanmıştır. Önerilen yöntemler sonucunda stego görüntüdeki bozulmayı en aza indirerek kapak görüntüsünde maksimum veri gömme kapasitesi elde edilmesi sağlanmıştır. Deneysel sonuçlar, gizli bilginin başarılı bir şekilde doğru olarak çıkarıldığını göstermektedir. Ayrıca önerilen yöntemlerin PSNR değeri ortalama 50 dB'in üzerinde olduğu görülmektedir.

Anahtar Kelimeler: Bilgi Güvenliği, DCT, DWT, DFT, Frekans Uzayı, Veri Gizleme.

* Corresponding Author: cabdalamoh@gmail.com

1. Introduction

The field of information security research has been challenged by security issues in online data transmission and communication to develop techniques to prevent any third-party interception during communication over the internet [1]. One of the methods to ensure the security of digital data is using steganography, cryptography, and digital watermarking. Steganography is hiding information in digital cover objects and protecting embedded content by hiding the existence of valuable data [2]. Methods of digital watermarking are used to protect the ownership or copyright of original content [3]. Many steganographic techniques have been proposed to provide secure data exchange through an open communication channel. These approaches are mainly hosted under two domains: In spatial domain techniques [4] [5], and frequency domain techniques. In the spatial domain data hiding, and replacement is directly applied to the pixels of the image, LSB [6]is the commonly used method in the spatial domain [7]. Whereas in the frequency domain the cover image is transformed from spatial to frequency by applying DCT, DWT, and DFT methods [8]. The generated image after applying steganographic algorithms is called Stego-image. This paper proposes data hiding in digital images by using steganographic techniques based on frequency domains. Digital steganography [9] is classified into image, audio, and video. In this paperwork, image steganography techniques [10] are preferred to achieve a maximum level of data embedding capacity [11]. Images comprise square pixels in the type of RGB color, bilevel, and greyscale images. RGB-colored images consist of red, green, and blue which represents 8-bit pixel for each color channel in a total of 24-bit pixel. Greyscale images contain Black and White color tones in which each pixel represents 8 bits.

Pixel intensity in images is between 0 to 255 as shown in **Figure 1.**

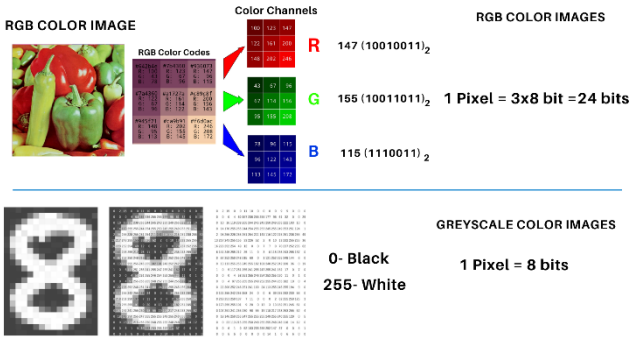

Figure 1 Color Spaces in Digital Images

The method implemented is DCT which will give us a very sharp data transition because of its high frequency. Data Embedding process is first transformed the cover image using frequency- oriented mechanism like discrete cosine transform domain (DCT), then secret data is embedded by modifying some frequency coefficients. The rest of this paper is organized as follows. Section II literarure survey of the proposed methoda is explained, in Section 3 Proposed Method is explained, in Section 4 Experimental results are discussed, and last Section 5 provides the Conclusion of the paper.

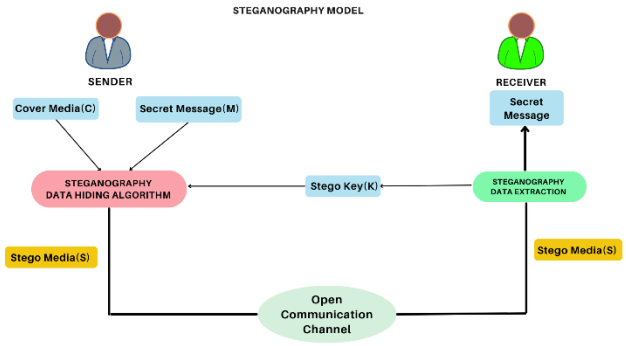

Figure 2 Steganography model

1.1. Discrete Fourier Transform Domain(DFT)

In Fourier transform, DFT the secret image to be sent is converted into its ASCII format according to the length of secret data. The cover image with the size M×N is represented as a two-dimensional function of f(x,y) in the spatial domain is also subjected to two dimensional Discrete Fourier Transform. The DFT consists of both real and imaginary coefficients. Therefore, the secret image is embedded into the real coefficients of the DFT-converted cover image. Once the embedding process is done, the cover image is converted to its spatial domain by applying inverse DFT to obtain the stego image. The receiver side can extract the ASCII values of the embedded secret image from real coefficients of the cover image by applying DFT.

DFT [12] is applied in the image according to the partition of the sine and cosine frequency components. 2D Fourier transform's mathematical function *f(x, y)* is shown Equation below.

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}.\sum_{y=0}^{N-1} f(x,y).e^{-j2\pi.\left(\frac{ux}{M}+\frac{vy}{N}\right)} (1)$$

u, v are frequency parameters in the DFT domain.

$$F(x,y) = \sum_{u=0}^{M-1}.\sum_{v=0}^{N-1} f(u,v).e^{-j2\pi.\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (2)$$

x, y are the spatial variables in the image.

1.2. Discrete Wavelet Transform Domain(DWT)

Wavelet transform transforms an image from spatial to transform domain. The Haar-DWT(HDWT) [13] is widely used and it is the easiest transformation. The operation of 2D-DWT consists of the construction of scanning images horizontally and vertically. The procedure of these operations is explained as follows:

Step 1: First pixels of the image is scanned from left to right in the horizontal direction. The addition and subtraction operations are applied to the neighboring pixels. Next is to store the sum on the left blocks and the difference on the right, this operation is illustrated in Hata! Başvuru kaynağı bulunamadı.. This process is repeated until all the scanned rows are processed. The mentioned pixel summation is denoted as a low-frequency (L) and pixel differences as a high-frequency band (H).

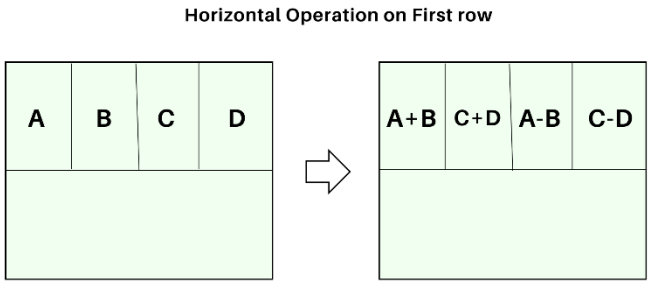

Figure 3 DWT Horizontal Scan on the first row

Step 2: Pixels are scanned from top to bottom in a vertical direction. Addition and subtraction operations are performed on adjacent pixels. Next is to store the sum on top and the difference on the bottom. This operation is repeated until all columns are processed as illustrated in **Figure 4**.

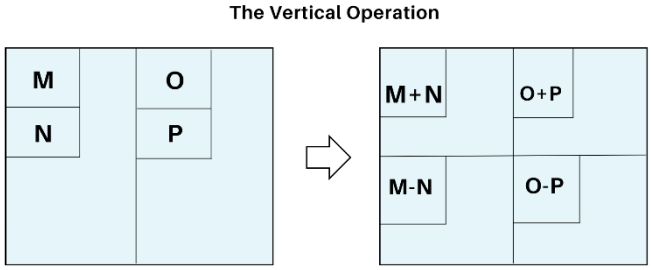

Figure 4 DWT Vertical scan operation

The sub-bands LL denotes a low-frequency block and it is very similar to the original image, any modification made to this sub-band could be captured by the intruders' attention, other sub-bands are Middle-level frequency(HL, LH), and high-frequency(HH). Modifications done to the HH sub-band can not be noticed by observers, it is imperceptible to the human visual system. Wavelet transformation provides both spatial and frequency embedding. **Figure 5** shows the Barbara image with 4-Level DWT.

Figure 5 Barbara Image 4-Level DWT

1.2.1. Data Hiding Algorithm Process with DWT in Image Steganography

1. Read cover Image (C).
2. Read secret message (S)
3. The secret message is converted to binary format.
4. The cover image is divided into 4 × 4 blocks.
5. Apply 2D- Haar DCT to get Low-frequency(LL),
6. Middle-level frequency(HL, LH), and high frequency(HH) sub-bands.
7. Apply LSB to each sub-band to replace secret data.
8. Calculate the inverse of 2D-HDWT for each 4 × 4 block.
9. Stego image(S) is finally produced.

1.2.2. Data Extraction Process with DWT in Image Steganography

1. Read the stego image (S).
2. Divide the stego image into 4 × 4 blocks.
3. Extract coefficients in the transform domain by using 2D- HDWT for each 4 blocks.
4. Apply LSB to extract the secret message from the pixels.
5. Extract the secret message.

2.Literature Survey

Many steganography techniques based on transform domain techniques have been found in the literature. Ramadhan J. Mstafa *et al* [14] have proposed video steganography based on DCT-DWT techniques. Their method focused on offering complete security criteria such as robustness, imperceptibility, and so on. First, they applied multiple object tracking (MOT) algorithm to allocate specific regions of interest (ROI) in the Cover video, then secret data is embedded in the chosen region by using DCT and DWT coefficients. They achieved high-security results and the algorithm is resistant to any possible attacks. Rufeng Chu *et al* [15] proposed DCT -based image steganography technique which takes advantage of the discrete cosine coefficients between the adjacent pixel blocks. They achieved good-quality images and the method is resistant to possible attacks. Abdelhafiz MM. *et al* [16] proposed a hybrid method based on the steganography domain and encrypted domain together. The method used left the most significant-bit (LMSB) areas in the image to hide the secret data in the quantized DCT coefficients. Evaluations show good results based on the quality measures and applied some steg attacks. Mohamed Hamidi *et al* [17] proposed a watermarking method a hybrid frequency domain consisting of DCT and DFT both together. They applied Arnold transform (AT) to enhance the security of their algorithm. They achieved robustness and imperceptibility compared with similar methods. Shakir, H.R. *et al* [18] proposed a crypto-stego based method that combined AES encryption, Wavelet transform in steganography, and chaotic pixel shuffling.

3. Proposed Method

The proposed method is aiming high embedding capacity without compromising the original visual quality of the reconstructed stego image and preventing any possible distortion. JPEG-format greyscale color images with the size of (512 × 512) are used for the experiment. JPEG images are maintained by converting the RGB color model to JPEG-YCbCr color space. The luminance channel is represented as (Y), whereas CbCr channels are representing the chrominance components of the color space. The proposed method uses a (Y) channel to embed secret data because it is an ideal space for data hiding and it provides a simple reconstruction of the original image. After choosing the luminance channel(Y) we divide it into 8 × 8 non-

overlapping blocks and apply DCT on each pixel blocks, next quantization is applied on the obtained DCT pixel blocks then standard JPEG quantization is utilized as shown in **Table 1**

The embedding and extraction process has shown in **Figure 6** in detail.

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

Table 1 JPEG Standard Quantization Table

3.1. DataHiding Algorithm process with DCT in Image Steganography

1. Read the Cover Image(C)
2. Read secret message(M)
3. Convert secret messages into binary.
4. Divide the selected channel(Y) of the Cover Image(C) into 8×8 non-overlapping blocks.
5. Apply and calculate DCT for each block.
6. Quantize each DCT block using the standard JPEG quantization **Table 1**
7. Embed the secret message(M) by swapping with calculated each DCT coefficient.
8. Stego image(S) is finally produced.

Below the DCT mathematical function is shown in Eq. (3), and Eq. (4) inverse DCT which is used to reconstruct the frequency-transformed image into the spatial domain:

$$C(u,v) = f(x,y)\sum_{x=0}^{N-1}.\sum_{y=0}^{N-1}\alpha(u)\cdot\alpha(v)\cdot cos\left[\frac{(2x+1)\cdot u\cdot\pi}{2N}\right]cos\left[\frac{(2y+1)\cdot v\cdot\pi}{2N}\right] (3)$$

$$For\ u,v\ =\ 0,1,2,3,\ldots\ldots\ldots,N-1$$

IDCT(inverse DCT) function: (4)

$$f(x,y) = C(u,v)\sum_{x=0}^{N-1}.\sum_{y=0}^{N-1}\alpha(u)\cdot\alpha(v)\cdot cos\left[\frac{(2x+1)\cdot u\cdot\pi}{2N}\right]cos\left[\frac{(2y+1)\cdot v\cdot\pi}{2N}\right]$$

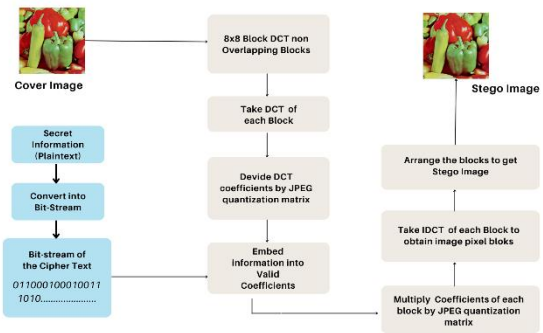

Figure 6 Embedding process of DCT in Image Steganography

3.2. Extraction Algorithm Process with DCT in Image Steganography

1. Read the Stego Image(S)
2. Separate the Stego image into 8× 8 blocks of pixels.
3. Apply DCT for each Pixel block.
4. Use a quantization table **Hata! Başvuru kaynağı bulunamadı.** to compress each block.
5. Calculate LSB for each DC coefficient.
6. Convert each bit into character and extract the secret message.

4. Experimental Results and Evaluations

Commonly used performance evaluation metrics [19] in data hiding techniques such as PSNR, MSE, and SSIM are given in this experiment as it's calculated in **Table 2 ,** and the equations below are used to calculate these values:

$$MSE = \frac{1}{m*n}\sum_0^{m-1}\sum_0^{n-1}\left(X'_{i,j} - X''_{i,j}\right)^2 \quad (5)$$

$$PSNR = 10 * log_{10}\left(\frac{max^2}{MSE}\right) \quad (6)$$

$$SSIM(x,y) = \frac{(2\mu x\mu y + c1)(2\sigma xy + c2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \quad (7)$$

Images 512 × 512	PSNR(dB)		SSIM		MSE	
	DCT	**DWT**	**DCT**	**DWT**	**DCT**	**DWT**
Lena	49.97	36.89	0.98	0.92	0.82	0.42
Peppers	36.26	37.2	0.95	0.7	0.69	0.49
Mandrill	48.67	47.54	0.92	0.96	0.93	0.68

Table 2 Method Evaluation Metrics

4.1. Histogram and Visual Quality Difference

The histograms of the proposed method are shown in the figures **Figure 7, Figure 8, Figure 9** below. It has been observed that there is no difference between both cover image and stego image after applying high JPEG compression and maximum data embedding.

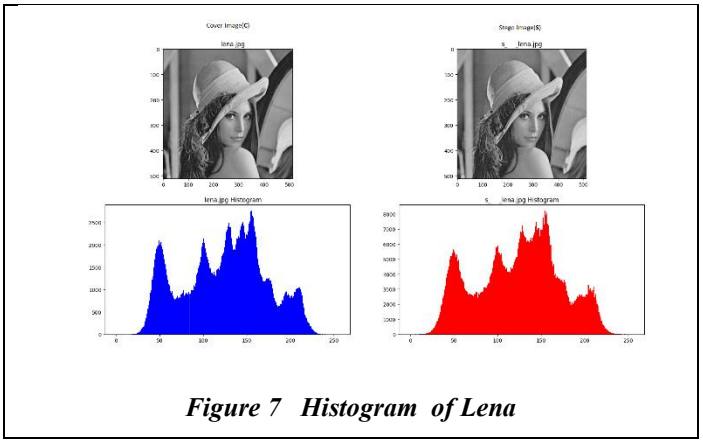

Figure 7 Histogram of Lena

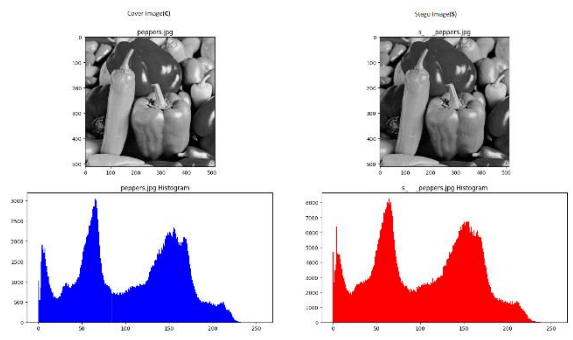

Figure 8 Histogram of Peppers

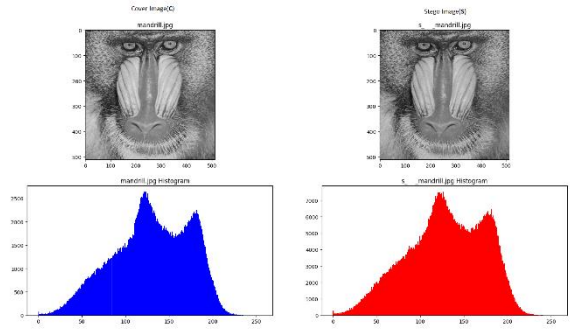

Figure 9 Histogram of Mandrill

5. Conclusions

This paper proposed secure data hiding algorithms based on frequency domain in image steganograğhy. The methods are evaluated according to the criteria of imperceptibility, payload capacity, and robustness. Some applied objective performance measurement metrics are PSNR, MSE, and SSIM. Among the proposed frequency domain steganography algorithms, DCT is the one with the best results and strong robustness. DCT is the most widely used technique in signal processing and linear transformation in data compression, it has strong energy compaction and is capable of achieving high-quality maximum data compression ratios. Thus DCT is the recommended method to apply for better data hiding in the frequency domain. The proposed method is also evaluated under subjective measurements, it has been observed that there was no visible difference when the quality of the stego image compared with the original cover image. Most of the time, due to the JPEG high compression method applied by the DCT algorithm to the image, block artifacts or quality degradation may occur in the image, and it can be said that our algorithm prevents this issue.

References

[1] «Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. Open Computer Science, 10(1), 296-342».

[2] «Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), 26-34».

[3] «Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). Digital watermarking and steganography. Morgan kaufmann».

[4] «Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66».

[5] «SOLAK, S., & ALTINIŞIK, U. (2021). Image Steganography-Based GUI Design to Hide Agricultural Data. Gazi University Journal of Science, 34(3), 748-763».

[6] «Sahu, A. K., & Swain, G. (2019). A novel multi stego-image based data hiding method for gray scale image. Pertanika Journal of Science & Technology, 27(2), 753-768».

[7] «Solak, S., "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms," in IEEE Access, vol. 8, pp. 166513-166524, 2020, doi: 10.1109/ACCESS.2020.3023197».

[8] «Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital Image Steganography: A Literature Survey. Information Sciences».

[9] «Uzun, M., Solak, S. (2022), GÖRÜNTÜ STEGANOGRAFİSİNDE YAYGIN KULLANILAN VERİ GİZLEME TEKNİKLERİNİN İNCELENMESİ. Mühendislik Bilimleri ve Tasarım Dergisi, 10(3), 816-830».

[10] «Solak, S., & Altınışık, U. (2019). Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3. Journal of Electronic Imaging, 28(4), 043025».

[11] «Sahu, A. K., & Swain, G. (2019). A novel multi stego-image based data hiding method for gray scale image. Pertanika Journal of Science & Technology, 27(2), 753-768».

[12] «Liao, X., Li, K., & Yin, J. (2017). Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform. Multimedia Tools and Applications, 76(20), 20739-20753».

[13] *Chan, Y. K., Chen, W. T., Yu, S. S., Ho, Y. A., Tsai, C. S., & Chu, Y. P. (2009). A HDWT-based reversible data hiding method. Journal of Systems and Software, 82(3), 411-421.*

[14] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017). A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE access, 5, 5354-5365.

[15] Chu, R., You, X., Kong, X., & Ba, X. (2004, May). A DCT-based image steganographic method resisting statistical attacks. In 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing (Vol. 5, pp. V-953). IEEE.

[16] Abdel-Aziz, M. M., Hosny, K. M., & Lashin, N. A. (2021). Improved data hiding method for securing color images. Multimedia Tools and Applications, 80(8), 12641-12670.

[17] «Hamidi, M., Haziti, M. E., Cherifi, H., & Hassouni, M. E. (2018). Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform.

Multimedia Tools and Applications, 77(20), 27181-27214».

[18] «Shakir, H. R. (2019). An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling. Multimedia Tools and Applications, 78(18), 26073-26087».

[19] «Konyar, M. Z., & Solak, S. (2021). Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. Journal of Information Security and Applications, 63, 103037».