Image Steganography Based Spatial and Transform Domain Techniques: A Review

Amar Y. Hussien*

Researcher, Department of Statistics, Duhok, Iraq

Email: amar.yehya85@gmail.com

Abstract

The amount of data shared online today is increasing. Data security is therefore cited as a significant problem while processing data exchanges through the Internet. Everyone needs the security of their data during communication processes. The science and art of steganography is the concealment of one audio, message, video, or image by embedding another audio, message, video, or image in its place. It is employed to protect sensitive data against malicious assaults. In order to detect the numerous methods employed with digital steganography, this study seeks to identify the primary image-based mediums. As a result, in the spatial domain of the digital medium, the LSB approach was mostly employed, whereas in the transform domain, DTC and DWT were separated as the primary techniques. Due to its simplicity and large embedding capacity, the spatial domain was the most frequently used domain in digital steganography.

Keywords: Information Security; Image Steganography; Spatial Domain; Transform Domain.

1. Introduction

In line with global trends, technology has improved to the point where the majority of people want to use the internet as their primary method of global data transfer [1]. Data can be transmitted in a variety of ways over the internet. Using the internet, the data transition is extremely straightforward, quick, and precise. However, one of the biggest issues with transferring information through the internet is the "security hazard" it poses, meaning that the private or confidential information can be stolen or hacked in a variety of ways. Data security is one of the most crucial things that must be taken into consideration during the process of transferring data, thus it becomes very necessary to do so [2].

Data security primarily refers to preventing data tampering and protecting data from unauthorized users or hackers [3]. Due to the dramatic rise in internet data transfer rates, this aspect of data security has recently attracted greater attention. Many approaches, including cryptography, steganography, and digital watermarking, have been developed to increase the security characteristics in data transfers over the internet. Steganography adds an extra layer of protection by cloaking the cipher text in an apparent invisible image or other formats, whereas cryptography conceals information by encrypting it to "cipher texts" and transferring it to the intended recipient using an unknown key [4]. Table 1 illustrates the objectives, general characteristics for information security techniques, and their drawbacks.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

Table1: Information Security Techniques Based Characteristics

Method	Requirements	Disadvantages
Cryptography	Authentication, Confidentiality, Integrity, Non-repudiation, Access control, and support services	The issue with cryptography is that it conceals the original data in ciphertext, which makes it possible for an attacker to draw attention to themselves and stop a transmission.
Watermarking	Capacity, Robustness, Security, Imperceptibility	Digital watermarking has the disadvantage that a subscriber is unable to modify certain portions of the files safely without compromising the quality.
Steganography	Capacity, Robustness, Security, Imperceptibility	The actual issue with steganography is that if the hidden message's presence is known or even suspected

Thus, "Steganography and cryptography are cousins in the spy craft family," it might be argued. Cryptography scrambles a message, rendering it unreadable. On the other hand, steganography conceals a message in order to make it invisible, which is the goal. The recipient may have doubts about the encrypted text, but there is never any doubt about steganographically hidden text [5]. Before being communicated through a public communication channel, the secret message is hidden using a cover medium (also known as a carrier) in steganography. As a result, it prevents illegal access to the message and preserves its privacy. Before using steganography to increase security and reduce the quantity of data that needs to be embedded. The covert message may be compressed or encrypted. This could reduce the carrier image's apparent artifacts (note that the carrier item can also be text, video, or audio) [6].

This study offers a large number of steganographic approaches that have lately been suggested for effectively concealing the secret data within the cover images. According to the domain utilized for embedding, picture steganography techniques may generally be divided into two major classes, which are described in the following sections as steganography methods based on the spatial domain and steganography methods based on the transform domain.

2. Steganography techniques

According to the embedding domain, image steganography algorithms can be divided into two primary classes, namely the spatial and transform domains. The embedding domain refers to the features of the cover object that are taken advantage of when messages are embedded inside of it. By adjusting image intensities using the secret data bits, the data are directly embedded into the host's pixels in a spatial domain approach. While modifying the image in an indirect manner using various transforms, the host medium's coefficients are altered in a transform domain technique [7]. Generally speaking, transform domain approaches offer greater security and are resistant to attacks than spatial techniques. Their disadvantages, however, include their high computational cost and constrained payload capacity. In contrast, spatial domain approaches are straightforward, simple to use, and sufficient in a secure setting with lossless compression. They also have a high rate of payload capacity and do not require extended execution times [8]. Table 2 shows the differences between picture steganography in the spatial and transform domains techniques in terms of embedding capacity, imperceptibility, and robustness.

Table 2: Spatial and Transform Domain Description

Technique	Description
Spatial	Simple and user-friendly; the embedding operation is executed directly within LSBs of intensity values. As a result, it is the most often used approach in digital steganography, especially in digital photos, and it has a high embedding payload. However, exceedingly fragile and vulnerable to damage from even a little alteration to the stego image, such as JPEG compression
Transform	more resistance to attacks like compression and geometric attacks than spatial domain approaches. Capacity embedding has several limitations, though. Information is embedded in the coefficients of the modified image, which necessitates additional computations.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

2.1 Spatial Domain

The idea of concealing information in the spatial realm is straightforward, and computing complexity is minimal. By simply modifying the cover-unused image's Least Significant Bits (LSBs), the secret information can be implanted. Many other types of methods have been offered for this.

(A) Least significant bit (LSB)

A popular and straightforward method for including data in an image file is known as least significant bit (LSB) insertion. This technique substitutes an M's bit for a byte's LSB. For steganography of images, sounds, and videos, this method works well. The generated image will appear to the human eye to be an exact replica of the cover object [9]. For instance, if we take into account image steganography, the letter A can be concealed in three pixels (assuming no compression). The 3-pixel original raster data (9 bytes) could be:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

In the 8 bytes that were used, only the three bits that are italicized actually change. LSB often only calls for changing half of an image's bits. The eye would not be able to detect data hidden in the least and second-least significant bits [7].

(B) Optimal Pixel Adjustment

The fundamental idea behind Optimal Pixel Adjustment (OPA) is to create the stego-image by simply integrating the secret bit into the cover picture via LSB replacement. Following the application of the best LSB approach, the new pixel values of the stego- picture are refined by applying addition or subtraction operations for the factor (2z) from the embedded pixel (where z indicates the number of hidden bits). It is interesting that the correction processes would have no effect on the least z bits for the pixel values of the stego-image [10]. As a result, the authors [10] adopted the idea of optimal pixel adjustment to improve the quality of the stego-image under settings with varying payload capacities and multiple authentication bits. Although this method produced positive results in terms of imperceptibility and embedding ability, the system's resistance to steganalysis attacks has not been addressed.

2.2. Transform Domain Techniques

This is a trickier approach to concealing data in an image. To conceal information in an image, various techniques and transformations are employed.

(A) Discrete Cosine Transform Technique (DCT)

JPEG compression makes use of DCT coefficients. It divides the image into components with varying degrees of importance. It changes a signal or image's frequency domain from the spatial domain. It can distinguish between the high-, middle-, and low-frequency components of the image. The majority of the signal energy in the low frequency sub-band is at low frequency, where the most crucial visual elements of the image are located, whereas in the high frequency sub-band, high frequency elements of the image are typically eliminated through compression and noise attacks [11]. In order to avoid affecting the image's appearance, the secret message is therefore inserted by changing the coefficients of the middle-frequency sub-band.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

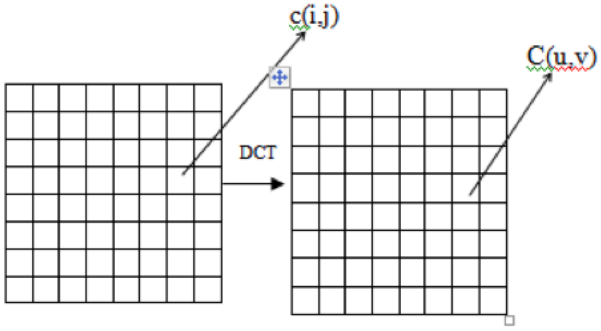

Figure 1: Discrete CosineTransform Technique (DCT) [11]

To lessen the blocking effects of image compression, the Joint Photographic Experts Group (JPEG) has adopted the (DCT) Discrete Cosine Transform as a global standard. The FDCT algorithm makes use of the qualities of energy compactness and matrix sparsity in the hesitating area to increase computed performance. The approach deconstructed the two-dimensional (2D) DCT into one pair of one-dimensional (1D) DCTs transforming it into a JPEG image with an 8 8 block volume in the spatial region. The outer results of the column and vectors of cosine functions are linearly combined to provide the 2D spatial datum, making the reverse DCT active [12].

(B) Discrete Wavelet Transform Technique (DWT)

The simplest DWT, the Haar-DWT, is the frequency domain transform that we used in this study [18][19]. Two operations make up a 2-dimensional Haar-DWT: a horizontal operation and a vertical operation. The following are detailed instructions for a 2-D Haar-DWT [12]:

Step 1: Start by horizontally scanning the pixels from left to right. Next, apply addition and subtraction operations to adjacent pixels. As seen in Figure 2, place the sum on the left and the difference on the right. Continue doing this until all rows have been processed. The original image's high-frequency portion is represented by the pixel differences, while the low-frequency portion is represented by the pixel sums (denoted by the symbol L) (denoted as symbol H).

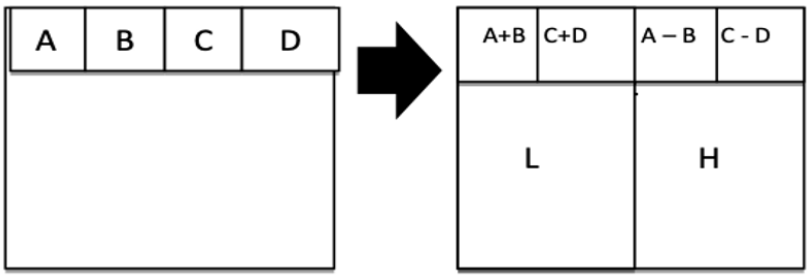

Figure 2: The First Row Operation Horizontally [12]

Step 2: Next, perform a vertical scan of the pixels from top to bottom. As shown in Figure 3, perform addition and subtraction operations on nearby pixels before storing the sum on top and the difference on the bottom. Continue doing this until all of the columns have been processed. Finally, we will have four sub-bands, each designated by the letters LL, HL, LH, and HH. Since the LL sub-band represents the low frequency part, it resembles the original image quite closely. The entire process is known as the first-order 2-D Haar-DWT.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

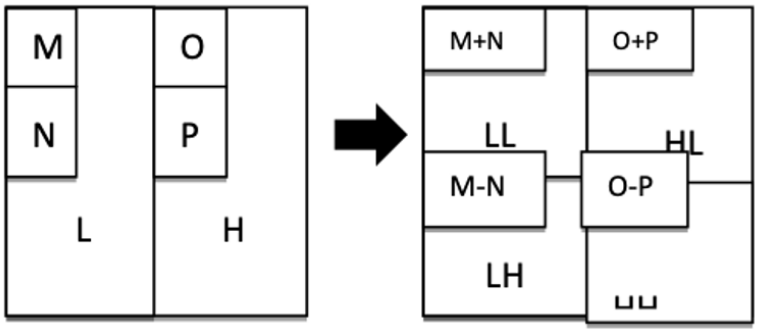

Figure 3: The First Row Operation Vertically [12]

3. Literature Survey

This kind of steganography uses the image as a cover object to conceal secret data. Images serve as a cover source in this technique because of the high bit density of their digital representation. Spatial and frequency domain images can be employed in three different ways as cover objects to conceal information.

Traditionally, image steganography is done using the Least Significant Bits (LSB) substitution method. Images typically have higher pixel quality, however, not all of them are utilized. The foundation of LSB techniques is the idea that small changes in pixel values would not result in noticeable alterations. The encrypted data is transformed into binary form. The least significant bits in the noisy area are found by scanning the cover image. The LSBs of the cover picture are then filled with the binary bits from the secret image.

Hamza [13] presented an LSB-based technique for image steganography. Using Blum Blum Shub and Arnold's Cat Map, the hidden logo gets mangled. Blocks of the cover image are created, and the entropy of each block is determined. The block with the highest level of entropy is chosen, and the first LSB contains one bit of the secret logo. The proposed method achieves higher security and improved imperceptibility, per the findings of its experiments. Another iteration of the LSB approach is applied to RGB images in [14]. The cover image is divided into three channels. All three planes have the hidden message encoded in them in a 2:2:4 ratio for the R, G, and B planes. Elharrouss and co. used the cover image's k-least significant bit for steganography. The authors inserted one cover image inside the other. The most important portion that could be saved in the cover image was first chosen at the sending side, and in this fashion, an entire secret image was concealed in the cover image. The authors employed the idea of region detection for decoding. An algorithm is utilized in this instance to look through the many areas where the data for the hidden image was hidden. The objective parameter was the peak signal-to-noise ratio. However, the proposed algorithm didn't work as well as anticipated.

A method of image steganography employing the Discrete Wavelet Transform (DWT) and visual cryptography was put out by Mostaghim and Boostani [16]. A secret share based on visual cryptography is created using a chaotic system. After that, a secret logo and this secret share are XORed to create a scrambled secret logo. The scrambled secret logo is encoded at the low frequency coefficients of the cover image after a DWT is applied to it. According to experimental findings, the suggested approach strengthens the security of the secret logo while presenting good imperceptibility. The usual PVD scheme incorporates a variety of additional security features with the goal of increasing the security component of the Pixel Value Differencing technique. For instance, Hussain et al. [17] suggested the use of two embedding techniques for an information hiding method that improves security. Improved Rightmost Digit Replacement (iRMDR) and Parity-Bit Pixel Value Difference are used in the corresponding methods (PBPVD). Table 3 summarises several previous studies based on data hiding in spatial and transform domains and the important issues that are processed.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

Table 3: Summary of Previous Studies in Spatial and Transform Domains

Ref	Do	Technique	Impre	Security	Capacity	Robustness	Confidentiality
[18]	Tr	Integer Wavelet Transform	High	Not approved	Secret image is smaller than cover image	Not robust	Low
[19]	Tr	DCT	High	Secure	Low	Good	Good
[20]	Tr and SP	LSB and DFT	High	Not approved	Low	Not robust	Good
[21]	Tr and SP	LSB and DWT	Low	Secure	Reasonable	Robust	Low
[22]	SP	LSB	High	Secure	High	Good	Not approved
[23]	SP	LSB	Limited	High	Reasonable	Good	Good
[24]	SP	PVD	High	Secure	High	Robust	Not approved
[25]	SP	LSB and PVD	High	High	High	Good	High
[26]	Tr	IWT	High	High	High	High	Good
[27]	Tr	DWT	Low	Not approved	Reasonable	High	High
[28]	Tr	DCT	High	Not approved	High	Good	Not approved

Ref: reference; Do: Domain; Impre: Imperceptibility; Tr: Transform; Sp: Spatial;

4. Discussion

The numerous steganography approaches that have been discussed in the literature in recent years are briefly discussed in this study, along with their main categories and classification. Along with the primary types and categories of steganography techniques, this broad concept is offered. Additionally, a thorough study of the three most important steganographic system components—namely, each approach's embedding capability, imperceptibility (also known as stego-image quality), and security—has been provided. Because of this, there is a trade-off between the possibility of embedding and imperceptibility. However, it might be challenging to increase embedding capacity without sacrificing the security and quality of the stage image. Along with that, this investigation brought to light a few problems with the previously employed methods; The security level of approaches utilized in the spatial realm is minimal, to begin with. Second, techniques with weak embedding capabilities in the limited transform domain. Third, the stego-quality image is crucial and is constrained by how much embedding is possible. A thorough examination of the spatial domain was published in the prior art, with a particular emphasis on image steganography methods leveraging LSB in the context of the telemedicine field. The analysis of these methods' benefits and drawbacks in relation to the four main benchmark steganography metrics—imperceptibility, capacity, and robustness—showed that achieving satisfactory performance for each of the aforementioned parameters at the same time is difficult. Although it is clear that some of these values have been adjusted using a variety of techniques, the conflicts they cause with the other parameters persist even after optimization. Therefore, techniques for image steganography that can offer the best trade-off between these factors must be developed in order to implement telemedicine. This is necessary. The use of medical picture steganography necessitates an increased focus on other key requirements, such as privacy and authentication, in order to achieve confidentiality and security in the transfer of patient information in telemedicine applications.

It is possible to direct efforts toward the formation of a benchmark dataset that includes photos captured by a variety of source cameras and captured in a variety of image formats. In order to make steganographic images, it is also possible to construct a compilation of all of the potential algorithms. As a performance measure, hiding

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

capacity, security, and robustness have all been taken into consideration in many different ways. When the transfer, however, takes place through channels that cannot be trusted, there is a possibility that a man-in-the-middle assault could take place. Alteration of the stego picture is another possibility that exists during the transfer process. Along with other measurements, it is possible to look at both how well the planned algorithm works against these attacks and how well the attacks themselves work.

Conclusion

An extensive survey of current spatial-domain embedding techniques is presented in this review study. It explains the distinction between cryptography and information concealment. According to a graphical and tabular design, comparisons among the proposed embedding techniques that are now available in the spatial domain are discussed based on their benefits and drawbacks. This report also elaborates on numerous ideas that may help future academics continue their work on spatial-image steganography. The following represent the key difficulties in spatial-domain image steganography: maintaining imperceptibility at a higher level, providing enhanced protection for the concealed secret data, offering reliable defenses against several intruder attacks, and increasing the embedding payload. In general, if a high embedding payload is required consistently, spatial-domain steganography approaches are seen to be more suitable. The inadequate resistance against geometric attacks, such as scaling, rotation, and cropping, is the most frequently discovered weakness of spatial-domain steganography. According to the literature, adaptive embedding techniques are presumed to be successful; as a result, research may focus on implementing adaptive ways for high-quality steganography techniques.

References

[1] Beroual, Abdesselam, and Imad Fakhri Al- Shaikhli. "A Review of Steganographic Methods and Techniques." International Journal on Perceptive and Cognitive Computing 4.1 (2018): 1-6.

[2] Zebari, N. A., Zebari, D. A., Zeebaree, D. Q., & Saeed, J. N. (2021). Significant features for steganography techniques using deoxyribonucleic acid: a review. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(1), 338-347.

[3] I. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran. (2019). "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326.

[4] Z. Wang, N. Gao, X. Wang, X. Qu, and L. Li, ''SSteGAN: Self- learning steganography based on generative adversarial networks,'' in Proc. Int. Conf. Neural Inf. Process. Cham, Switzerland: Springer, 2018, pp. 253–264.

[5] X.Liao,J.Yin,S.Guo,X.Li,andA.K.Sangaiah,''MedicalJPEGimage steganography based on preserving inter-block dependencies,'' Comput. Electr. Eng., vol. 67, pp. 320–329, Apr. 2018.

[6] Zebari, D., Haron, H., & Zeebaree, S. (2017). Security issues in DNA based on data Hiding: A review. *International Journal of Applied Engineering Research*, *12*(24), 0973-4562.

[7] Shtayt, B. A., Zakaria, N. H., & Harun, N. H. (2021). A comprehensive review on medical image steganography based on LSB technique and potential challenges. Baghdad Sci. J, 18, 957-974.

[8] Devi S, Sahoo MN, Muhammad K, Ding W, Bakshi S. Hiding medical information in brain MR images without affecting accuracy of classifying pathological brain. Future Generation Computer Systems. 2019;99, 235-246.

[9] Zeebaree, D. Q., Abdulazeez, A. M., Hassan, O. M. S., Zebari, D. A., & Saeed, J. N. (2020). Hiding Image by Using Contourlet Transform. *Test Engineering and Management*, *83*, 16979-16990.

[10] Abduallah, W. M., & Rahma, A. M. S. (2016). A review on steganography techniques. American Academic Scientific Research Journal for Engineering, Technology, and Sciences, 24(1), 131-150.

[11] Goel, S., Rana, A., & Kaur, M. (2013). A review of comparison techniques of image steganography. Global Journal of Computer Science and Technology.

[12] S. E. Tsai, and S.M. Yang, A Fast DCT Algorithm for Watermarking in Digital Signal Processor, Mathematical Problems in Engineering, Vol. 2017, 1-7. https://doi.org/10.1155/2017/7401845

[13] Hamza YA. Highly Secure Image Steganography Approach Using Arnold's Cat Map and Maximum Image Entropy. Proceedings of the International Conference on Information and Communication Technology ICICT'19, Baghdad, Iraq, ACM. 2019:134-138.

[14] A. Singh and H. Singh, ''An improved LSB based image steganography technique for RGB images,'' in Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT), Mar. 2015, pp. 1–4

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022

[15] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An image steganography approach based on k-least significant bits (k- LSB)." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
[16] Mostaghim M, Boostani R. CVC:Chaotic visual cryptography to enhance steganography. 11th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran. IEEE. 2014: 44-48
[17] Hussain, Mehdi, et al. "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement." Signal Processing: Image Communication 50 (2017): 44-57.
[18] N. Raftari, & A. M. E. Moghadam. "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm". In Proc. of the International Conference of the Modelling Symposium (AMS), IEEE,2012, pp. 87-92.
[19] V. Sachnev, and H. J. Kim. "An improved matrix encoding scheme for JPEG steganography". In International Workshop on Digital Watermarking, Springer, vol. 7128 ,2012, pp. 3-15
[20] Khalil MI. Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. International Journal of Computer Network and Information Security. 2017;9(2), 22.
[21] Banjan N, Dalvi P. Medical Data Security using combination of Cryptography and Steganography with AES-LSB algorithm. 2018;7(7), 31–45.
[22] Babatunde AO, Taiwo AJ, Dada EG. Information Security in Health Care Centre Using Cryptography and Steganography. 2018. arXiv preprint arXiv:1803.05593.
[23] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, "Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 17799-17823, Jul. 2019.
[24] B. Santoso, "Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm," *J. Phys. Conf. Ser.*, vol. 1175, paper. 012057, Mar. 2019.
[25] S. Prasad and A. K. Pal, "Logistic Map-Based Image Steganography Scheme Using Combined LSB and PVD for Security Enhancement," *Springer Singapore*, vol. 755, pp. 203-214, 2019.
[26] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 9971-9989, Apr. 2019.
[27] A. Nevriyanto, S. Sutarno, S. D. Siswanti, and E. Erwin, "Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio," *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, vol. 17, pp. 147-152, 2019.
[28] M. K. Shyla and K. B. Shiva Kumar, "Novel Color Image Data Hiding Technique Based on DCT and Compressed Sensing Algorithm," *Springer Singapore*, vol. 545, pp. 1151-1157, 2019.

Doi : https://doi.org/10.54216/FPA.080101
Received: April 13, 2022 Accepted: July 22, 2022