International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 12, Issue 4 (Jul.-Aug. 2023), PP. 15-23

Enhanced Data Security of Communication System Using Combined Encryption and Steganography

Sushant Kumar Panigrahi[1] Rosalin Mangaraj[2] Debasish Pradhan[3] Lopita Bisoi[4]
[1,2,3,4] *Department of Computer Science and Engineering, Einstein Academy of Technology & Management, Bhubaneswar*

Abstract—
Data security is crucial in daily life, as systems can be hacked, posing high risks to confidential files. This paper proposes a method for storing basic images, which are protected in composites using DWT wavelet transform. The encrypted image is hidden behind the encrypted image, and the system includes two algorithms for encoding and hiding, and returning and decoding the main image to its original state efficiently.

Keywords—*encryption, discrete wavelet transform, steganography, modulated image, hidden image*

I. Introduction

Images encryption strategies are broadly utilized to overcome the issue of safe transferring for both images and messages via electronic transfer media both images and messages via electronic transfer media by utilizing the classical cryptographic processes [1–3]. However, the main problem of this method is that it is limited use remains with the huge amounts of data or high-resolution images [4, 5]. The process of hiding the board image was completed after removing the most important part of the data in the embedded image. This data was saved because it is considered as a decryption key. The fundamental indication of this research paper is to stow away and encrypt the full image interior another one [6]. At first: images should have analyzed using wavelet transform formula, where the images go through levels of (DWT). This process produced four factors conditions, (ca), (ch), (cv), and (cd). Then comes the process of clearing enough space to include target image components on embedded image components. To make the appropriate images more secretly, exponential function math was used. Decryption was mainly based on returning the last discarding values to their original positions of images, then it takes the Inverse Discrete Wavelet Transform (IDWT) to produce un-secure data. The most objective of this strategy is to hide images with 2-D and 3-D on other images to produce a single encrypted image with tall effectiveness.

II. Literature review

Some authors show that a biometric verification system which usages two individual biometric structures collective by waterline inserting with secret PIN encryption to get a non-unique ID of each person [7–9]. The converted structures and models trek over unconfident the Internet or intranet of the communication system in the client-server situation. In addition, the researchers suggested a method that composite of encryption and information hiding the use of a few characteristics of Deoxyribonucleic Acid (DNA) sequences [10–12]. The suggested system contains two parts. The first part has the confidential information encoded by using a DNA and Amino Acids-Based Show reasonable cryptograph. the second part contains the encoded information steganography assistant which secreted into some location of DNA classification. Also, the authors suggested an LSB & DCT-based steganography process for saving the information [13–17]. All the information bits are implanted by modifying the slightest noteworthy bit low frequency bits of Discrete Cosine Transform (DCT) factors which include the image segments [11, 18, 19]. In [20–22], they suggest improved protection for the data. By using encryption and steganography. The information is encrypted and hidden behind an image then transferred to the cloud afterward. The image can be downloaded whenever it seems appropriate and the data can be decoded to recover the original file. In [23], They used the RSA encryption algorithm and image steganography for data concealment, as well as the LSB approach. The Advanced Encryption Standard (AES) algorithm was adjusted and used to encode the secret message. The encrypted message was protected using this technique. In [24–27], A technique used on the advanced LSB (least significant bit) and RSA algorithm was discussed. It is less chance of an attacker being enabled to use steganalysis to recover data when matching data to an image. In [28], They suggest a new form of steganography based on gray m level modulation using image transformation, hidden key, and cryptography for true color images. Both the private key and the secret data are initially encoded using multiple encryption algorithms (bitxor processing, bit shuffling, and stego key based encoding); then encoded in the pixels of the host image. In addition, before data hiding, the input image was transposed. Objective analysis employing several image quality evaluation criteria is used to evaluate the

proposed technique, which shows promising results in terms of secret data and preservation. In [29], They suggest a new combination method of cryptanalysis and steg analysis by using an HTML file. RJDA is a method that uses LSB (least significant bit) as an algorithm for steganography and encryption/decryption. Confidentiality is one of most critical security criteria to ensure that the purpose of saving or transmitting data cannot be interpreted by any other unauthenticated person. In [30], They implement techniques that combine cryptography and steganography to encode the data as well as to conceal the image details.

III. The proposed system

The proposed system is divided into main three parts. The first part is used to analyze the images by using DWT. The second part is used to hide (embed) the analytical combinations after the zeroing process behind an image. The last part is used to encrypt the image by using a mathematical exponential function.

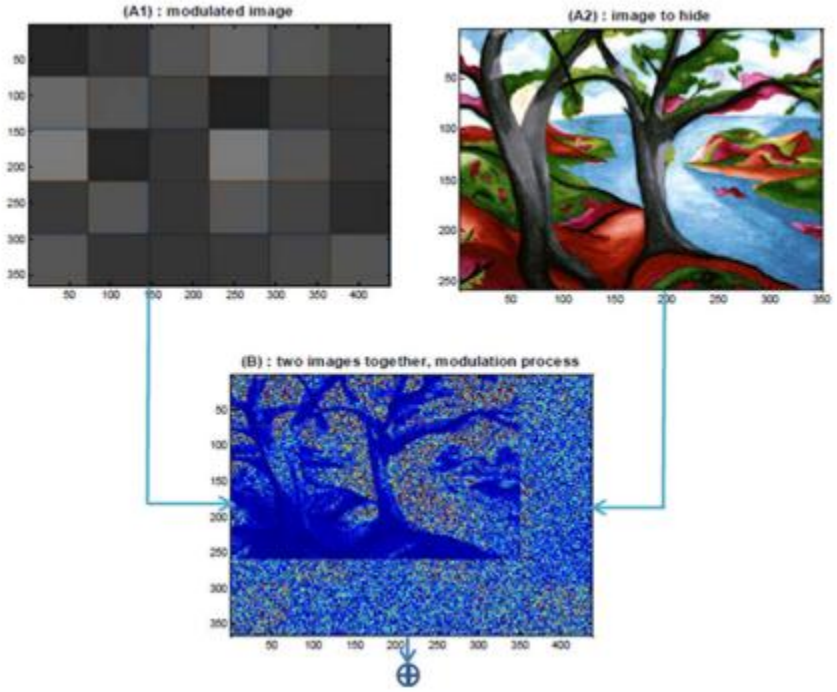
Figure 1. Shows the proposed system

IV. Algorithms and results

1- ALGORITHM (1): Encryption of 2-D image.

ALGORITHM (1): Encryption	
1.	Check the first image which has high measurements, modified image, rectangular image (365x438).
2.	Check the next image which has low measurements; image to be encoded and secreted, tree image (258x350).
3.	• Analyze "tree image", to be hidden by using wavelet disintegration for two measurements transmute law: [ca1, ch1, cv1,cd1]=dwt2(Im1,'db1'). • Decompose "squares image", (moderated image) using wavelet decomposition for two measurements transmute law: [ca2,ch2,cv2,cd2]=dwt2(Im2,'db1').

4.	Zeroing number of locations in (ca2 component) equal to the dimensions of (ca1 component), as follow: • for x=1: a [a=no. of rows of ca1] • for y=1: b [b=no. of columns of ca1] • L(c,:)=[x y]:[save locations of ca2] • V(1,c)=ca2(x,y): [save values of ca2] • ca2(x,y)=0: [do zero locations] • c=c+1 • end;end
5.	Do modulation method, as below: • for x=1: a [a=no. of rows of ca1] • for y=1: b [b=no. of columns of ca1] • if ca2(x,y)==0: • ca2(x,y)=ca1(x,y): [modulated values] • end;end;end
6.	Repeat steps 4 and 5 on (cd, ch, cv) components
7.	Using (Idwt2) to make reverse putrefaction of wavelet transform of two dimensions for the new (ca2, cd2, ch2, cv2) to get different image; new image=idwt2(ca2,cd2,ch2,cv2,'db1')
8.	Formulate (function of exponential) file at the same of new image dimensions, E= (365x438)
9.	Use math. The equation between (E and new image).
10.	Obtaining the encoded and secreted image…end



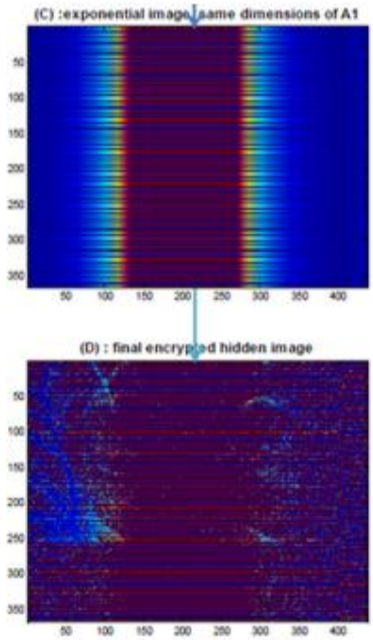


Figure 3: . Encryption of 2-D image

2- ALGORITHM (2): Decryption of two dimensions' image.

ALGORITHM (2): Decryption	
1.	Make the inversing process of math. to obtain a modulated image (365x438)
2.	Decompose "new image" with wavelet decomposition law for two dimensions converting : [ca2,ch2,cv2,cd2]=dwt2(new image,'db1').
3.	Separate the modulated values (ca1) from (ca2) and zeroing these locations, as follow: • for x=1:a [a=no. of rows of ca1] • for y=1:b [b=no. of columns of ca1] • if ca2(x,y)=ca1(x,y) • ca2(x,y)=0 • end;end;end
4.	Recover the original protected values of old (ca2), as following: • for x=1:a [a=no. of rows of ca1] • for y=1:b [b=no. of columns of ca1] • if L(c,:)=[x y]; [L, saved locations of old ca2]. • ca2 (x,y)=V(1,c); [retrieve old values of ca2 which saved earlier]. • c=c+1; • end;end;end
5.	Repeat step 4 for all other components to retrieve old (ch2, cv2, and cd2)
6.	Using (Idwt2) to make inverse decomposition of wavelet transform of two dimensions for old (four components ca2, cd2, ch2, cv2) and (ca1,cd1,ch1,cv1) Squares image=idwt2(ca2,cd2,ch2,cv2,'db1') Tree image=idwt2(ca1,cd1,ch1,cv1,'db1')
7.	Recover the main images…end

Images from (A to C2) of Figure (3) show the ALGORITHM (2) experimental results.

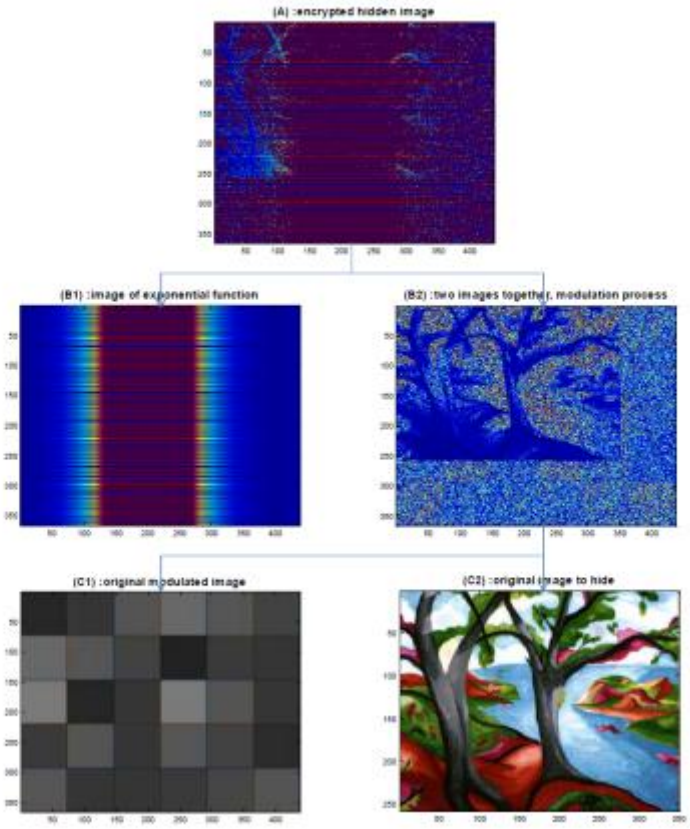


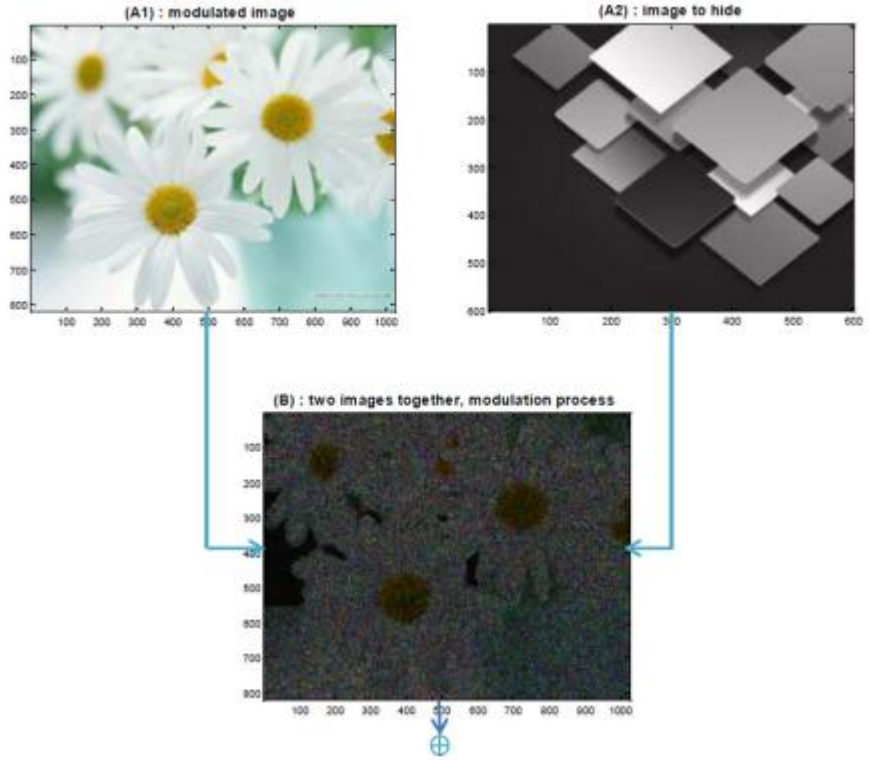
Figure 3. Decryption of 2-D image

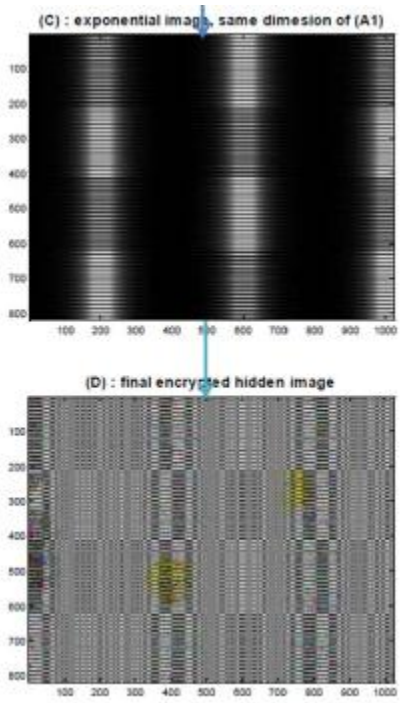
3- ALGORITHM (3): Encryption of 3-D image.

	ALGORITHM (3): Encryption
1.	Check the first image which has high dimensions, modulated image, geometric image (819x1024x3).
2.	Check the second image which has low measurements; image to be encoded and secreted, pyramid image (600x600x3).
3.	• Decompose "flowers image", (modified image) using wavelet putrefaction for two measurements modify law: [ca1,ch1,cv1,cd1]=dwt2(Im1,'db1'). • Decompose "geometric image", (image to hide) using wavelet decomposition for two dimensions transform law: [ca2,ch2,cv2,cd2]=dwt2(Im2,'db1').
4.	Zeroing number of locations in (ca1 component) equal to the dimensions of (ca2 component), as follow: • for k=1:3 [3- dimensions] • for x=1:a [a=no. of rows of ca2] • for y=1:b [b=no. of columns of ca2] • L(C,:)=[x y k]:[save locations of ca1] • V(1,C)=ca1(x,y,k): [save values of ca1] • ca1(x,y,k)=0: [do zero locations] • C=C+1 • end;end;end

5.	Make modulation process, as follow: • for k=1:3 [3- dimensions] • for x=1:a [a=no. of rows of ca2] • for y=1:b [b=no. of columns of ca2] • if ca1(x,y,k)==0: • ca1(x,y,k)=ca2(x,y,k): [modulated values] • end;end;end;end
6.	Repeat steps 4 and 5 on (cd, ch, cv) components
7.	Using (Idwt2) to make opposite decomposition of wavelet transform of two dimensions for the new (ca1, cd1, ch1, cv1) to get different image; new image=idwt2(ca1,cd1,ch1,cv1,'db1')
8.	Make (function of exponential) file of the same dimensions as of new image, E= (819x1024x3)
9.	Create mathematical Equation between E and new image.
10.	Obtaining encoded and secreted image…end

Images from (A1 to D) of Figure (5) display the experimental results of ALGORITHM (3)





4- ALGORITHM (4): Decryption of three-dimension image.

ALGORITHM (4): Decryption	
1.	Make inverse of mathematical Process to obtain image (819x1024x3)
2.	Decompose "new image" using wavelet decomposition for two measurements transform law: [ca1,ch1,cv1,cd1]=dwt2(new image,'db1').
3.	Separate the modulated values of (ca2) from (ca1) and zeroing these locations, as follow: • for k=1:3 [3- dimensions] • for x=1:a [a=no. of rows of ca2] • for y=1:b [b=no. of columns of ca2] • if ca1(x,y,k)=ca2(x,y,k) • ca1(x,y,k)=0 • end;end;end;end
4.	Recover the main protected values of old (ca1), as follows: • for k=1:3 [3- dimensions] • for x=1:a [a=no. of rows of ca2] • for y=1:b [b=no. of columns of ca2] • if L(C,:)=[x y k]; [L, saved locations of old ca1]. • ca1 (x,y,k)=V(1,C); [retrieve old values of ca1 which saved earlier]. • C=C+1; • end;end;end;end
5.	Repeat step 4 for all other components to retrieve old (ch1, cv1, and cd1)

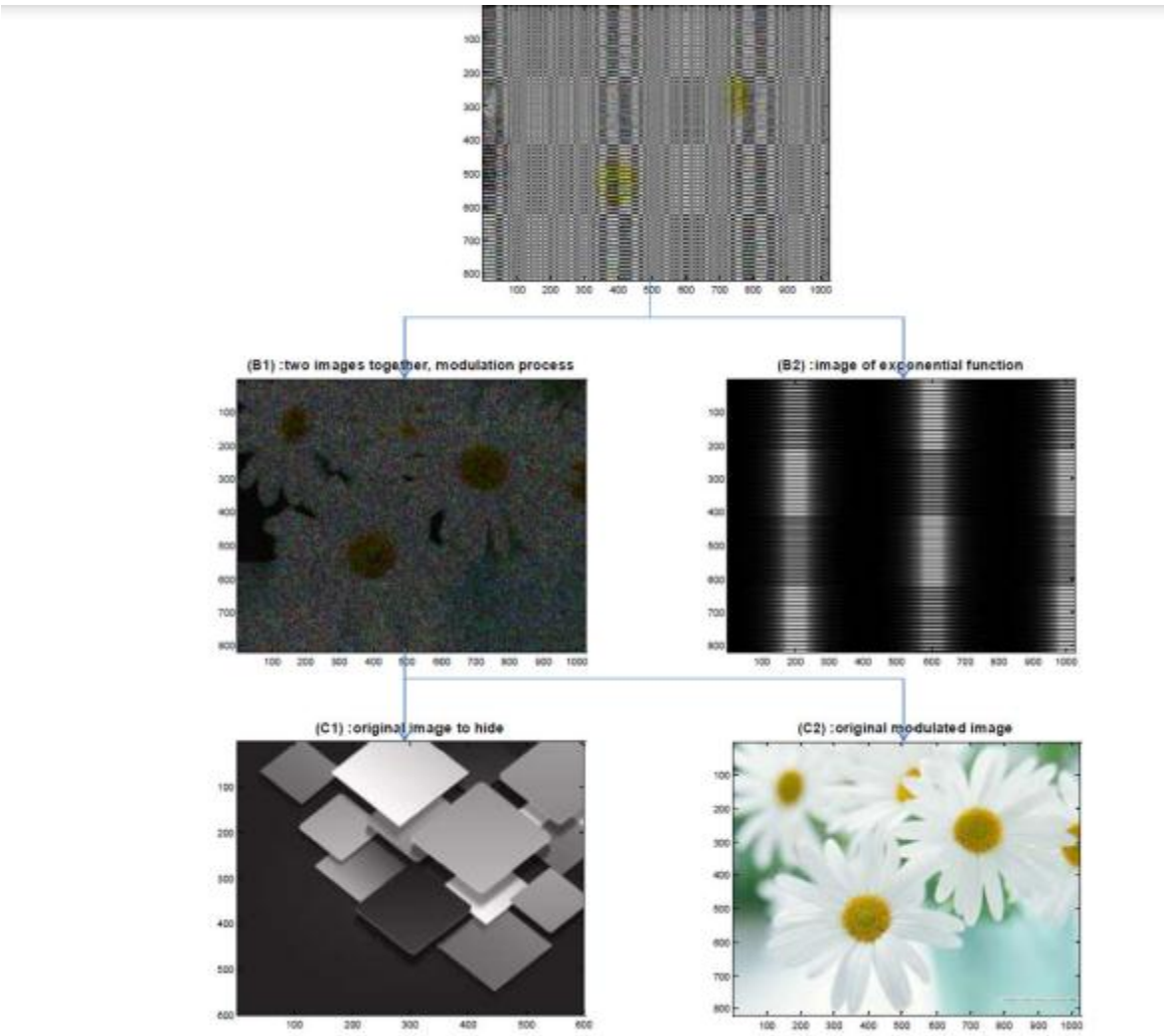


Figure 6. The decryption of the 3-D image

Tables 1 shows the feature measurements used to show the method efficiency and to compare status Before and after the hiding and encryption activities. correlation and entropy measurements for the two-dimensional and three-dimensional images were used, as follows:

Table 1. Quality measurements used for 2-D and 3-D data

	Signal	Correlation	Entropy
First state 2-D	Modulated image (squares image)	–0.0007402	3.9231
	Hidden image (tree image)		5.7006
	Combined encrypted hidden image 1.	–0.0007402	1.0427
Second state 3-D	Modulated image (sunflower image)	0.0004278	6.7425
	Hidden image (geometric image)		6.5511
	Mixed encrypted hidden image 2.	0.0004278	1.0087

V. Conclusions

The technology data is fully relying on web services. This paper deals with security difficulties and how can be stopped. The cryptography and Steganography the method is used to secure data. Table I shows that that the closing of the main characteristics of the images involved in the encryption process resulted from the encrypted image with less entropy, and it is noted that the correlation values closed to zero, indicating the quality of the method, i.e., closer result to zero better quality of the method. After eliminating the protection and decrypting, the resulting images show that it is exactly the same as the main image. The approach used in this paper will assist to create a confident construction for data security.

References

[1]. M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," rchives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15–43, 2020. https://doi. org/10.1007/s11831-018-9298-8

[2]. I. J. Kadhim, P. Premaratne, P. J. Vial, and B. J. N. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326, 2019. https://doi.org/10.1016/j.neucom.2018.06.075

[3]. F. Yepes-Calderon, S. Bluml, S. Erberich, and M. D. Nelson, "Improving the picture archiving and communication system: towards one-click clinical quantifying applications," Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, vol. 7, no. 2, pp. 154–161, 2019. https://doi.org/10.1080/21681163.2018.1466199

[4]. D. Hörl, F. R. Rusak, F. Preusser, P. Tillberg, N. Randel, R. K. Chhetri, A. Cardona, P. J. Keller, H. Harz, and H. J. N. M. Leonhardt, "BigStitcher: reconstructing high-resolution image datasets of cleared and expanded samples," Nature Methods, vol. 16, no. 9, pp. 870–874, 2019. https://doi.org/10.1038/s41592-019-0501-0

[5]. C. Shorten and T. Khoshgoftaar, "A survey on image data augmentation for deep learning," ournal of Big Data, vol. 6, no. 1, p. 60, 2019. https://doi.org/10.1186/s40537-019-0197-0

[6]. A. Roy, P. André, D. Arzoumanian, M.-A. Miville-Deschênes, V. Könyves, N. Schneider, S. Pezzuto, P. Palmeirim, and A. Kirk, "How the power spectrum of dust continuum images may hide the presence of a characteristic filament width," Astronomy & Astrophysics, vol. 626, p. A76, 2019. https://doi.org/10.1051/0004-6361/201832869

[7]. M. S. Houston, D. M. Stange, and J. P. Aronson, "Ad Hoc Item Geo Temporal Location and Allocation Apparatuses, Methods and Systems," U.S. Patent Application, ed: Google Patents, 2018.

[8]. I. J. Cox, G. Doërr, and T. Furon, "Watermarking is not cryptography," in International Workshop on Digital Watermarking, 2006, pp. 1–15: Springer. https://doi.org/10.1007/11922841_1

[9]. M. S. Subhedar and V. Mankar, "Current status and key issues in image steganography: A survey," Computer science review, vol. 13, pp. 95–113, 2014. https://doi.org/10.1016/j. cosrev.2014.09.001

[10]. N. Chakravarthy, A. Spanias, L. D. Iasemidis, and K. Tsakalis, "Autoregressive modeling and feature analysis of DNA sequences," EURASIP Journal on Advances in Signal Processing, vol. 2004, no. 1, p. 952689, 2004. https://doi.org/10.1155/S111086570430925X

[11]. L. Wei, S. Luan, L. A. E. Nagai, R. Su, and Q. J. B. Zou, "Exploring sequence-based features for the improved prediction of DNA N4-methylcytosine sites in multiple species," Bioinformatics, vol. 35, no. 8, pp. 1326–1333, 2019. https://doi.org/10.1093/bioinformatics/bty824

[12]. I. A. Aljazaery, A. A. Ali, and H. Abdulridha, "Classification of electroencephalograph (EEG) signals using quantum neural network," Signal Processing: An International Journal (SPIJ), vol. 4, no. 6, p. 329, 2011.

[13]. O. F. AbdelWahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, A. A. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," Telkomnika, vol. 17, no. 3, pp. 1168–1175, 2019. https://doi.org/10.12928/telkomnika.v17i3.12230

[14]. I. A. Aljazaery, H. T. S. Alrikabi, and M. Aziz, "Combination of Hiding and Encryption for Data Security," International Journal of Interactive Mobile Technologies (iJIM),vol. 14, no. 9, p. 35, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[15]. M. Kharrazi, H. T. Sencar, and N. Memon, "Performance study of common image steganography and steganalysis techniques," Journal of Electronic Imaging, vol. 15, no. 4, p. 041104, 2006. https://doi.org/10.1117/1.2400672

[16]. H. T. Alrikabi, A. H. M. Alaidi, A. S. Abdalrada, and F. Abed, "Analysis the Efficient Energy Prediction for 5G Wireless Communication Technologies," International Journal of Emerging Technologies in Learning, vol. 14, no. 08, pp. 23–37, 2019. https://doi.org/10.3991/ijet. v14i08.10485

[17]. M. Al-dabag, H. S. ALRikabi, and R. Al-Nima, "Anticipating Atrial Fibrillation Signal Using Efficient Algorithm," International Journal of Online and Biomedical Engineering (iJOE), vol. 17, no. 2, pp. 106–120, 2021. https://doi.org/10.3991/ijoe.v17i02.19183

[18]. B. Yang, M. Schmucker, W. Funk, C. Busch, and S. Sun, "Integer DCT-based reversible watermarking for images using companding technique," in Security, steganography, and watermarking of multimedia contents VI, 2004, vol. 5306, pp. 405–415: International Society for Optics and Photonics. https://doi.org/10.1117/12.527216