Enhanced Data Security of Communication System Using Combined Encryption and Steganography

Haider TH. Salim ALRikabi[1(✉)], Hussein Tuama Hazim[2]
[1]Wasit University, Wasit, Iraq
[2]University of Misan, Misan, Iraq
`hdhiyab@uowasit.edu.iq`

Abstract—Data security has become a paramount necessity and more obligation in daily life. Most of our systems can be hacked, and it causes very high risks to our confidential files inside the systems. Therefore, for various security reasons, we use various methods to save as much as possible on this data, regardless of its different forms, texts, pictures, videos, etc. In this paper, we mainly rely on storing the basic image which should be protected in another image after changing its formal to composites using the DWT wavelet transform. The process of zeroing sites and storing their contents technique is used to carry the components of the main image. Then process them mathematically by using the exponential function. The result of this process is to obtain a fully encrypted image. The image required to be protected from detection and discrimination is hidden behind the encrypted image. The proposed system contains two algorithms. The first algorithm is used for encoding and hiding, but the second algorithm is designed for returning and decoding the main image to its original state with very efficiently.

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

1 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.

2   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. It provides the data being transmitted with two layers of protection and also focuses on the power of mixing methods of cryptography and steganography. In [31], They use LSB (Least Significant Bit) as a steganography method and AES, RSA, DES, 3DES, and Blowfish as cryptographic algorithms to encrypt the information that should be concealed in an image. The work in this paper demonstrates an increase in the capacity of the current steganography techniques to accommodate. In this paper, a new method which combine both of techniques is proposed to obtain better results. a method involving both these techniques to gain better results has developed. Firstly, the encrypted image should be encoded using the Rivest–Shamir–Adleman (RSA) symmetric encryption cryptography and transformed to American Standard Code for Information Interchange (ASCII) values. the received encrypted message in decimal format is changed to octal and finally to binary format. Secondly, the binary bits obtained are disguised inside any digital image using Least Significant Bits insertion to make a new image with a special key known as stego image, which is delivered to the recipient who executes inverse operations to acquire the encrypted image. Between the source and stego images, the Mean Squared Error and Peak Signal to Noise Ratio values are calculated, and the model accuracy by this technique are shown to be much better than most of the other methods.

3   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.

Fig. 1. Shows the proposed system

4   Discrete Wavelet Transform (DWT)

The suggested construction method compacts with the discrete 2-D DWT, whose mathematical procedures which definite as following:

$$x_{LL}(n_1, n_2) = \sum_{i_1=0}^{k-1}\sum_{i_2=0}^{k-1} g(i_1) \cdot g(i_2) \cdot x_{LL}^{j-1}(2n_1 - i_1)(2n_2 - i_2) \tag{1}$$

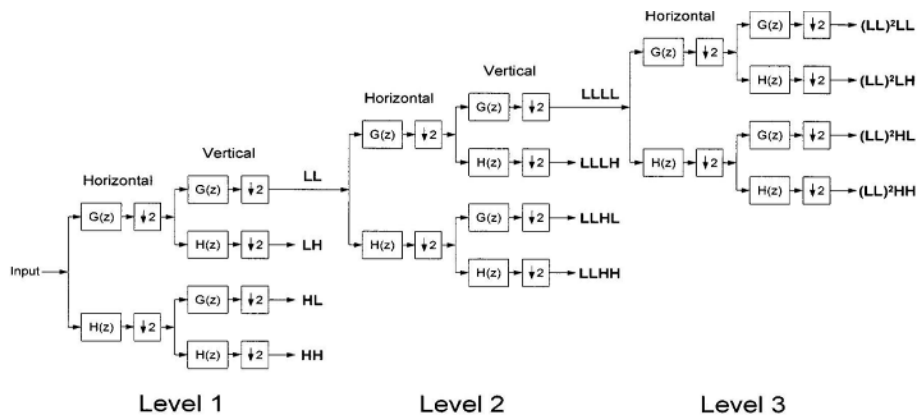$$x_{LH}(n_1,n_2) = \sum_{i_1=0}^{k-1}\sum_{i_2=0}^{k-1} g(i_1) \cdot h(i_2) \cdot x_{LL}{}^{j-1}(2n_1-i_1)(2n_2-i_2) \tag{2}$$

$$x_{HL}(n_1,n_2) = \sum_{i_1=0}^{k-1}\sum_{i_2=0}^{k-1} h(i_1) \cdot g(i_2) \cdot x_{LL}{}^{j-1}(2n_1-i_1)(2n_2-i_2) \tag{3}$$

$$x_{HH}(n_1,n_2) = \sum_{i_1=0}^{k-1}\sum_{i_2=0}^{k-1} h(i_1) \cdot h(i_2) \cdot x_{LL}{}^{j-1}(2n_1-i_1)(2n_2-i_2) \tag{4}$$

Fig. 2. Three-level Discrete Wavelet Transform

5 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').

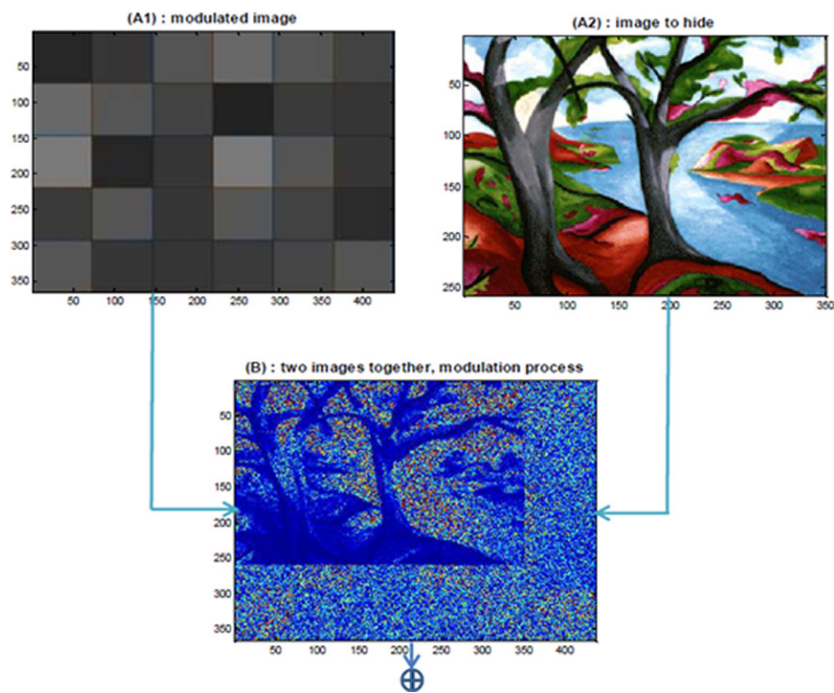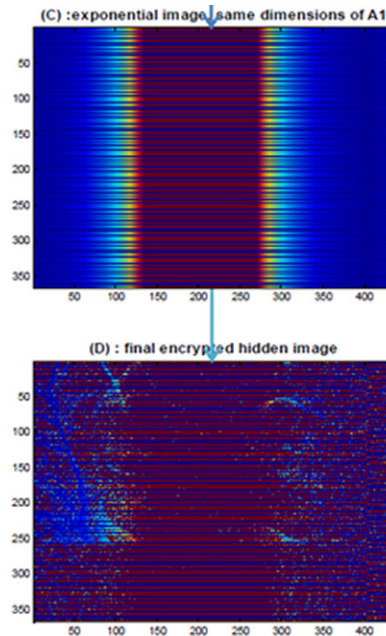| 4.	Zeroing number of locations in (ca2 component) equal to the dimensions of (ca1 component), as follow: • for x=1: a [a=no. of rows of ca1] • for y=1: b [b=no. of columns of ca1] • L(c,:)=[x y]:[save locations of ca2] • V(1,c)=ca2(x,y): [save values of ca2] • ca2(x,y)=0: [do zero locations] • c=c+1 • 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

Fig. 3. *(Continued)*

Fig. 3. Encryption of 2-D image of ALGORITHM (1)

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

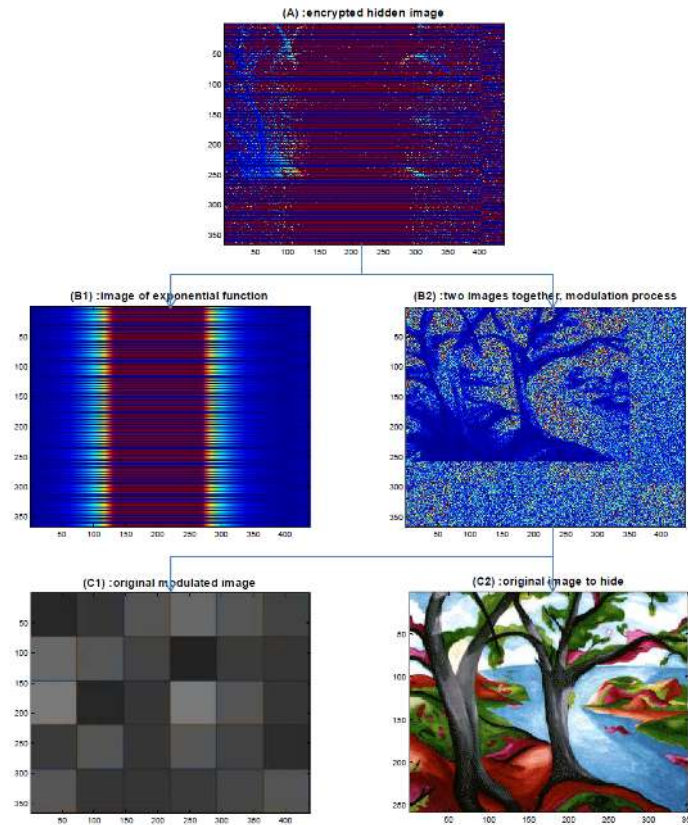Images from (A to C2) of Figure (4) show the ALGORITHM (2) experimental results.

Fig. 4. 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).
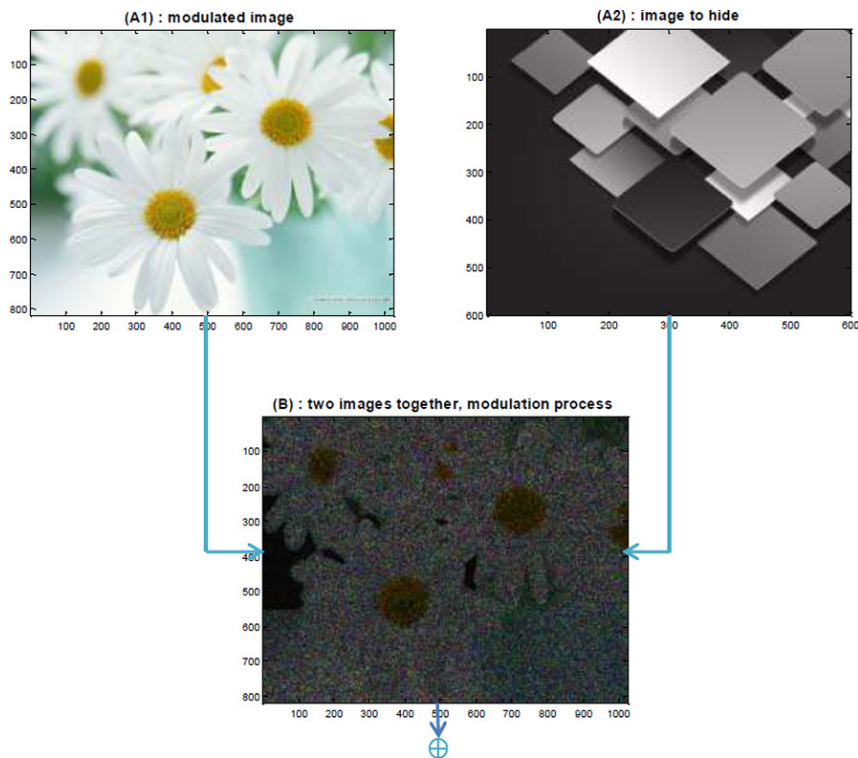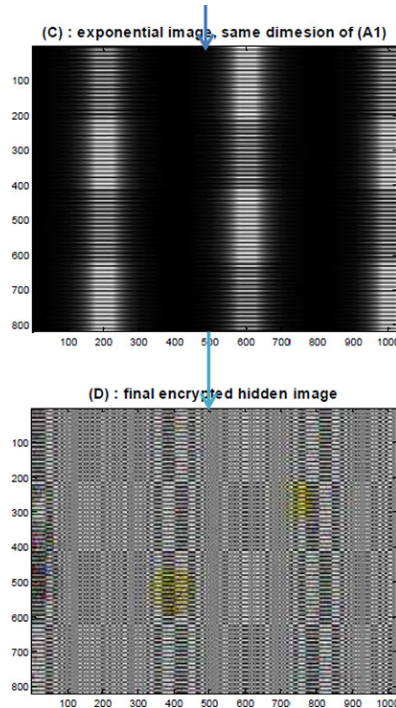

Fig. 5. *(Continued)*

Fig. 5. Encryption of 3-D image

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)

6.	Using (Idwt2) to make inverse decomposition of wavelet transform of two dimensions for old (ca2, cd2, ch2, cv2) and (ca1,cd1,ch1,cv1) geometric image=idwt2(ca2,cd2,ch2,cv2,'db1') flowers image=idwt2(ca1,cd1,ch1,cv1,'db1')
7.	Recover the images to the original …end

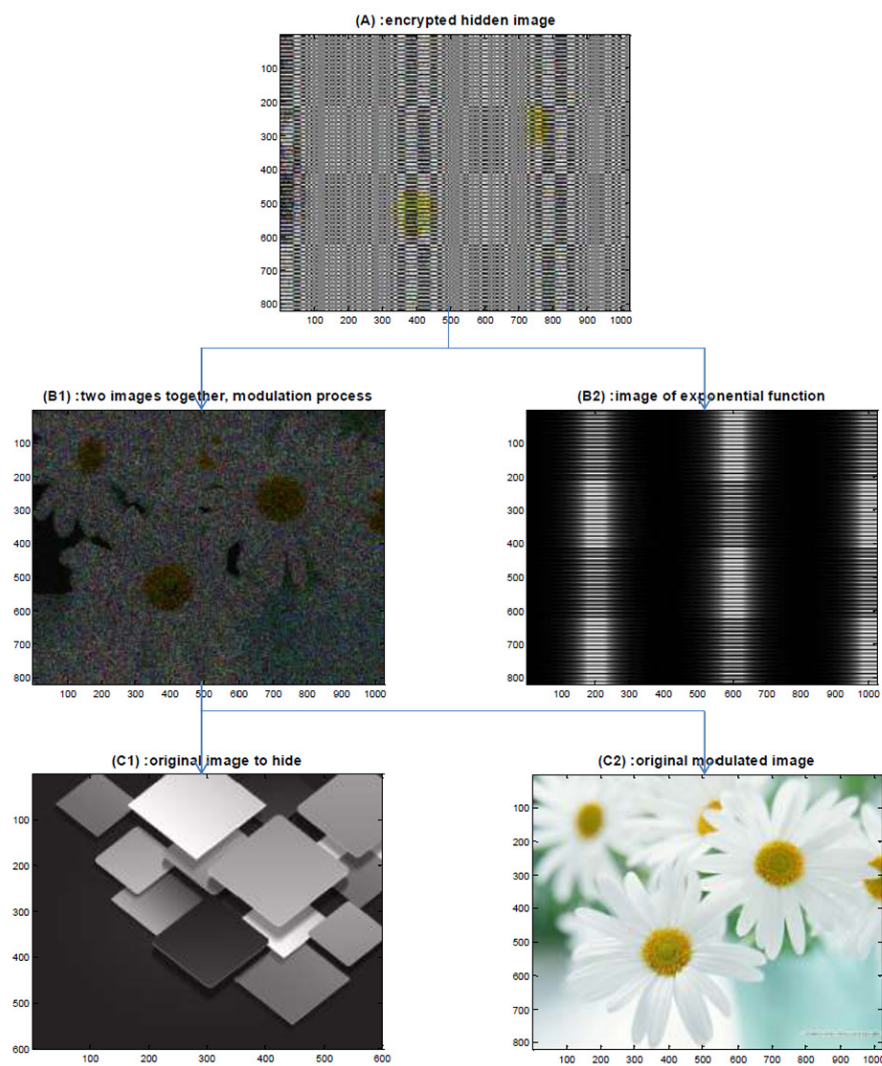Images from (A to C2) of Figure (6) display the investigational results of ALGORITHM (4).

Fig. 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

6 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 characterists 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.

7 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

[19] N. A. Hussein. H. A. Naman, M. Al-dabag, Haider Th.Salim Alrikabi, "Encryption System for Hiding Information Based on Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[20] K. Bhowal, D. Bhattacharyya, A. J. Pal, and T.-H. J. T. S. Kim, "A GA based audio steganography with enhanced security," Telecommunication Systems, vol. 52, no. 4, pp. 2197–2204, 2013. https://doi.org/10.1007/s11235-011-9542-0

[21] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 2308–2312: IEEE. https://doi.org/10.1109/WiSPNET.2016.7566554

[22] R. M. Al_airaji, I. A. Aljazaery, S. K. Al_dulaimi, and H. T. S. Alrikabi, "Generation of high dynamic range for enhancing the panorama environment," Bulletin of Electrical Engineering and Informatics, Article vol. 10, no. 1, pp. 138–147, 2021. https://doi.org/10.11591/eei.v10i1.2362

[23] A. M. Abdullah and R. Aziz, "New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm," International Journal of Computer Applications, vol. 143, no. 4, pp. 11–17, 2016. https://doi.org/10.5120/ijca2016910143

[24] W. Alexan, A. Hamza, and H. Medhat, "An aes double–layer based message security scheme," in 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), 2019, pp. 86–91: IEEE. https://doi.org/10.1109/ITCE.2019.8646461

[25] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020, pp. 64–69: IEEE. https://doi.org/10.1109/ICOEI48184.2020.9142896

[26] O. H. Yahya, H. Alrikabi, and I. Aljazaery, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," International Journal of Online and Biomedical Engineering (iJOE), vol. 16, no. 03, pp. 107–116, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

[27] S. M. M. Najeeb, H. ALrikabi, and S. M. Ali, "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," Telkomnika (Telecommunication Computing Electronics and Control), Article vol. 19, no. 1, pp. 285–292, 2021. https://doi.org/10.12928/telkomnika.v19i1.17884

[28] S. Khan, N. Abbas, M. Nasir, K. Haseeb, T. Saba, A. Rehman, Z. J. M. T. Mehmood, and Applications, "Steganography-assisted secure localization of smart devices in internet of multimedia things (IoMT)," pp. 1–21, 2020. https://doi.org/10.1007/s11042-020-09652-5

[29] R. Dubey, A. Saxena, and S. Gond, "An innovative data security techniques using cryptography and steganographic techniques," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 6, no. 3, pp. 2175–2182, 2015.

[30] P. S. Nagdive, A. Raut, "Visual cryptography and steganography: a review," International Journal of Advanced Research in Computer Science and Management Studies, vol. 3, no. 2, 2015.

[31] R. Hussein and W. Alexan, "Secure message embedding in audio," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1–6: IEEE. https://doi.org/10.1109/CAIS.2019.8769505

8   Authors

Haider Th. Salim ALRikabi He is presently Asst. Prof and one of the faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut, Wasit, Iraq. He received his B.Sc. degree in Electrical Engineering in 2006 from the Al Mustansiriya University in Baghdad, Iraq. His M.Sc. degree in Electrical Engineering focusing on Communications Systems from California state university/Fullerton, USA in 2014. His current research interests include Communications systems with the mobile generation, Control systems, intelligent technologies, smart cities, and the Internet of Things (IoT). Al Kut city – Hay ALRabee, Wasit, Iraq. E-mail: hdhiyab@uowasit.edu.iq. The number of articles in national databases – 10, and the number of articles in international databases – 30.

Hussein Tuama Hazim is presently one of the faculty college of engineering, electrical engineering department, University of Misan in Misan, Iraq. Master degree in Electronics and Telecommunication Engineering focusing on Mobile communications. The current research interests include wiress Communications, mobile computing, AI, Information Technology, IoT, intelligent Control systems, sustainable energy, deep learning.