Combination of Hiding and Encryption for Data Security

https://doi.org/10.3991/ijim.v14i09.14173

Ibtisam A. Aljazaery (✉)
University of Babylon, Babylon, Iraq
ibtisamalasady@gmail.com

Haider Th. Salim Alrikabi
University of Wasit, Wasit, Iraq

Mustafa Rabea Aziz
General Directorate of Education, Nineveh, Iraq

Abstract—One of the techniques used in information security is the concealment technique, where the information to be hidden within another information medium to be saved in the process of messaging between two sides without detection. In this paper, an algorithm was proposed to conceal and encrypt data using several means.in order to ensure its preservation from detection and hackers. Wavelet transformer was used to change the shape of a wave of information (one and two-dimensional data) and its different mathematical formulas. Two sets of data were used, the first group used in a hidden process. The second group was considered as a means of both embedding and encryption. The data in the second group is reduced to the extent of sufficient for the modulation process, by extracting its high-value properties and then removing them from the mother's information wave. The process of encrypting of the two sets of data comes together using an exponential function. The result is undetectable information signals. Algorithms were built to hide and encrypt one and two-dimensional data. High-security signals and images were obtained. Decryption algorithms were built to return encrypted data to their original forms, and getting the replica data.

Keywords—Embedding and encryption, exponential function, information security technique, Wavelet transformer.

1 Introduction

Cryptography and steganography are common methods to secure communications. For the purpose of protection against unauthorized access, confidentiality and data integrity must be observed. Cryptography scrambles a message so it cannot be understood. The Steganography hides the message so it cannot be seen [1, 2]. This research is made to combine both cryptography and Steganography methods into one system for better confidentiality and security. In this advanced encrypting data hiding method, encrypted data can be embedded and extracted from both encrypted images

and signals [3-5]. The data is encrypted using two scenarios. The first was to use a wavelet transformer to change the shape of the signal or image to a different form of the original[6, 7]. In the second stage, the exponential function was used to complete the encoding process to the final form. While the hiding algorithm was built between the two encryption phases. (Stego-crypto) as a term, goes to attain its importance attributable to the exponential growth and secret communication of potential users over the web [8, 9]. In addition, it has become an important tool for data security especially in military applications for example 5 G is more security others wireless communication techniques [10, 11]. The proposed work includes: decompose both encrypting data and hiding data, generate the modulated medium, data embedding, data extraction, and data recovery.

1.1 Wavelet transformer

Wavelet conversion is known to convert other data types from time domain to frequency domain. It is used to analyze a signal that does not produce information about "frequency" in the traditional sense, but a time and size distribution is created. The change in the size of the wavelet is represented by a two factor. It is therefore possible to reconstruct any signal using one wave as a base and to place as many waves as needed at different times with different amplitudes and scales [12-14].The equations for conversion can be summarized as follows:

$$y_{low}[n] = \sum_{k=-\infty}^{+\infty} x[k]g[2n-k] \quad (1)$$

$$y_{high}[n] = \sum_{k=-\infty}^{+\infty} x[k]h[2n+1-k] \quad (2)$$

Where:
x is chosen data.
g is high pass filter.
h is low pass filter.

This decomposition reduced the time resolution by half as half of each output filter distinguishes the signal. However, each output has half the frequency band of the input, thus multiplying the frequency resolution [15, 16].

2 Literature Review

In [17], they presented a biometric authentication scheme that uses two separate biometric features combined by watermark embedding with hidden password encryption to obtain a non-unique identifier of the personage. They provided experimental results. The transformed features and templates trek through insecure communication line like the Internet or intranet in the client-server environment. The authors in [18], proposed technique is a composition of both encryption and data hiding using some properties of Deoxyribonucleic Acid (DNA) sequences. The proposed scheme consists mainly of two phases. In the first phase, the secret data is encrypted

using a DNA and Amino Acids-Based Play fair cipher. While in the second phase the encrypted data is steganography ally hidden into some reference DNA sequence using an insertion technique. In [19]proposed an LSB & DCT-based steganography method for hiding the data. Each bit of data is embedded by altering the least significant bit of low frequency DCT coefficients of cover image blocks. They used some techniques to utilizes the idea of SSB-4 technique in modifying the other bits to obtain the minimum variation between the original and the modified coefficient. The author in [20] explored the limits of Steganography theory and practice. He printed out the enhancement of the image Steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. The recent explosion of research in watermarking to protect intellectual property is evidence that Steganography is not just limited to military or espionage applications.In [21]designed sequence the combined scrambling operation is utilized for changing the pixel position of secret image under the control of a random matrix. At the same time, the pixel value is altered by random bit shift for obtaining an encrypted image encoded in N-bit data. These operations are employed for all pixels of original secret image. The authors in [22], they proposed a method, which combines the techniques of Steganography and cryptography, to hide the secret data in an image. In the first phase, the sender will embed the secret data in an image by using the Least Significant Bit (LSB) technique. The embedded image will be encrypted by using an encryption algorithm. In [23], they Advanced Encryption Standard (AES) algorithm has been modified and used to encrypt the secret message. the encrypted message has been hidden by Enhancing Pixel Value Difference (PVD) image using Mobile Phone Keypad (MPK) Coding. In [24], they introduced PASH, a privacy-aware s-health access control system, which the key ingredient is a large universe CP-ABE with access policies partially hidden. In PASH, attribute values of access policies are hidden in encrypted SHRs and only attribute names are revealed.

3 Quality Measures of the Method

In order to assess the quality of the method of hiding and encrypting information, commonly used measures are, arithmetic mean (average), and entropy. Mean is used to quantify the difference between the initial (cover signal) or (modulated signal) and the Mixed encrypted hidden signal, distorted signal, equation (3) [25-26]. Entropy is the average rate at which information is produced by a stochastic source of data. The measure of information entropy associated with each possible data value is the negative logarithm of the probability mass function for the value equation (4) [27-29].

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i = \frac{a_1+a_2+\cdots+a_n}{n} \tag{3}$$

Where:

ai = elements.
n = number of elements.

$$Corr = \frac{\sum_{i=1}^{N}\sum_{J=1}^{M}(I_1(i,j)-\bar{I}_1)(I_2(i,j)-\bar{I}_2)}{\sqrt{\left[\sum_{i=1}^{N}\sum_{J=1}^{M}(I_1(i,j)-\bar{I}_1)^2\right]\left[\sum_{i=1}^{N}\sum_{J=1}^{M}(I_2(i,j)-\bar{I}_2)^2\right]}} \quad (4)$$

Where:
I1(i,j) = the value of pixel at (i,j) of the original image.
$\bar{I}_1$ = the mean of the original image.

$$\bar{I}_1 = \frac{1}{M\times N}\sum_{i=1}^{N}\sum_{j=1}^{M} I_1\,(i,j) \quad (4.1)$$

I2(i,j) = the value of pixel at (i,j) of reconstructed image.
$\bar{I}_2$ = the mean of the reconstructed image.

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M} I_2\,(i,j)$$

M = height of image.
N = width of image.
(i,j) = row and column numbers.

$$S = -\sum_i P_i \log P_i \quad (5)$$

Where: Pi = probability.

4 Algorithms and Results

In this section of this research, the algorithms designed to build the proposed work will be presented with the results obtained. Calculations were performed and all algorithm were implemented using MATLAB. Each cryptographic algorithm will be presented for each case discussed with decipher algorithm as well as the results for both cases, as follows:

Table 1. ALGORITHM (1-a): encryption of one-dimension signal for two cases, low frequency signal (LFS) sine wave and high frequency (HFS) of EEG signal.

ALGORITHM (1-a): Encryption Algorithm	
	Read the first data signal with high frequency, modulated signal, signal=m sample.
	Read second data signal with low frequency signal (LFS) or high frequency signal (HFS) to be encrypted and hidden, EEG or sin=n sample.
	Decompose the first signal (modulated signal) using wavelet packet transform law (wpt): wpt=wpdec(signal, 3, 'db1'). Find the best tree of (wpt) using the rule: bt=besttree(wpt). Find the coefficients of (besttree). Link these coefficients together to get the modulated signal (the mother signal=m samples).
	Zeroing the positive values of the mother signal after saving them and their locations, c11, loc1.
	Decompose second signal (signal to hide) using the second wavelet transform law: [C, L]=wavedec(sin, 3, 'db1'), C=n samples.

	Make modulation process, as follow: for i=1:m: [no. of modulated signals' samples]. if c1(i)==0: [(c1) is the modulated signal]. loc(k)=i: [save the locations]. count=count+1 c1(i)=c(k): [put the values of (C signal) in zeros locations of modulated signal (c1)or mother signal]. end; end
	Prepare (exponential function) file of the same dimension of mother signal, e=m sample.
	Make math. Equation between (e and c1).
	Getting encrypted and hidden signal end

Images from (A1 to E) of Figure (1) and from (A1 to E) of Figurer (2), depict in details the experimental results of ALGORITHM (1-a) using (LFS) sine wave and (HFS) EEG signal respectively, as follow:

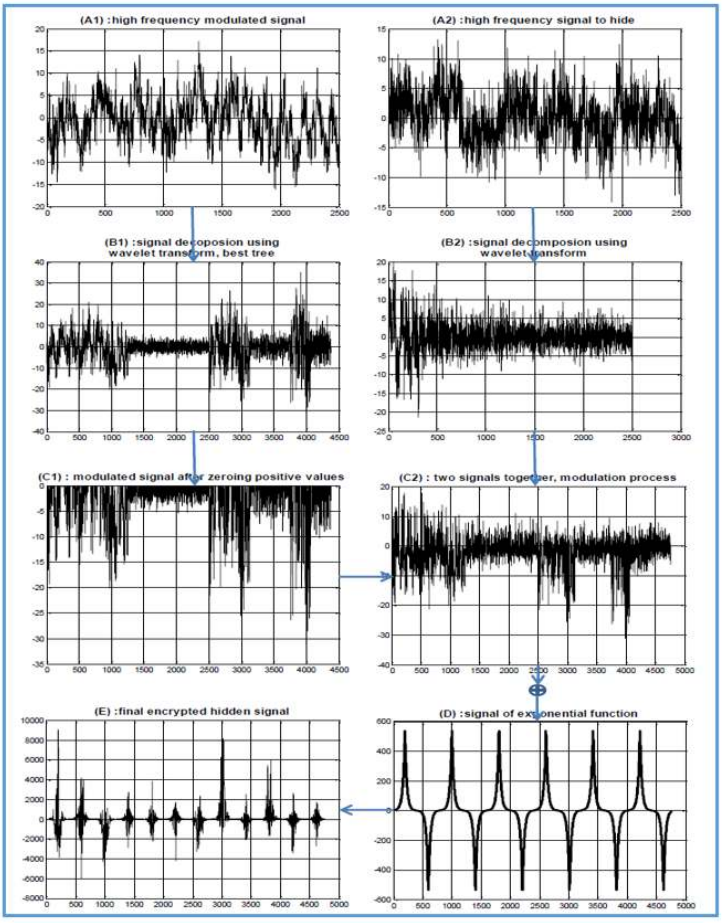

Fig. 1. Encryption of one-dimensional signal using (LFS) sine wave.

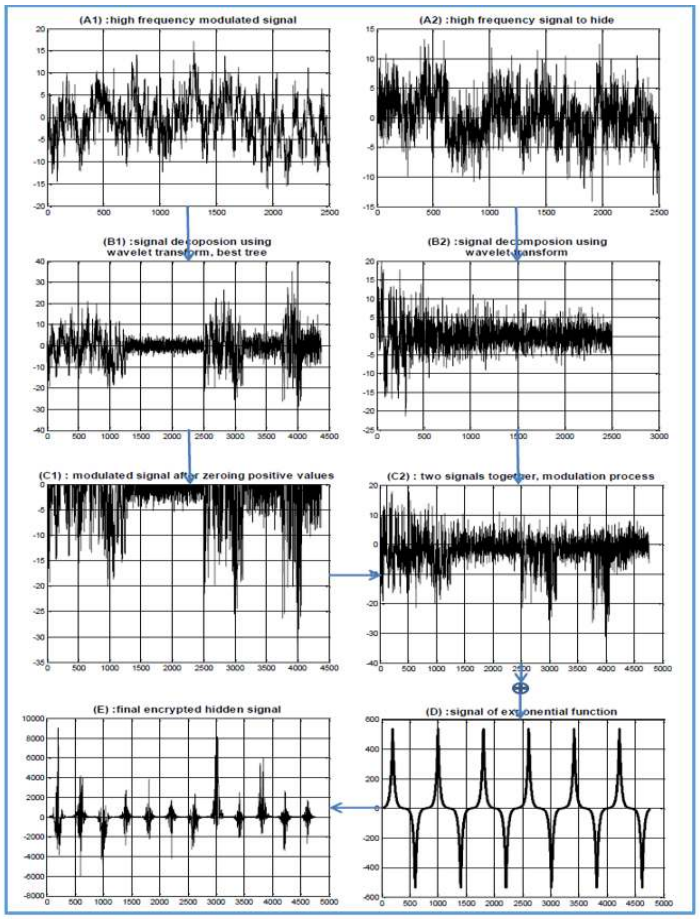

Fig. 2. Encryption of one-dimensional signal using (HFS) EEG signal.

Table 2. ALGORITHM (1-b): decryption algorithm of the above case represented in ALGORITHM (1-a).

ALGORITHM (1-b): Decryption Algorithm	
	Make opposite math. Operation to get modulated signal
	Separate the modulated values about the parent signal and put these values in their locations, as follow: for i=1: n: [n is no. of signal's to hide samples]. for j=1: m: [m is no. of modulated signals' samples]. if loc(i)==j: [loc, the locations of sin wave]. cc(1, k)=c1(j):[remove the sin wave values from the modulated signal, demodulation process]. c1(j)=0: [zeroing these location]. k=k+1; end;end;endz

	Retrieve the positive saved values of the mother signal, as follows: for i=1:n:[n is no. of signal' to hide samples]. for j=1: :[m is no. of modulated signals' samples]. if loc1(i)==j:[loc1, the locations of positive values of the mother signal]. c1(j)=c11(i):[retrieve the positive values which saved erlier, c11]. k=k+1; end;end;end
	Aggregation of the two signals using (Idwt= inverse decomposition of wavelet transform).
	Retrieve the original signals…end

Images from (A to E2) of Figure (3) and from (A to E2) of Figurer (4), depict in details the experimental results of ALGORITHM (1-b) using (LFS) sine wave and (HFS) EEG signal respectively, as follow:

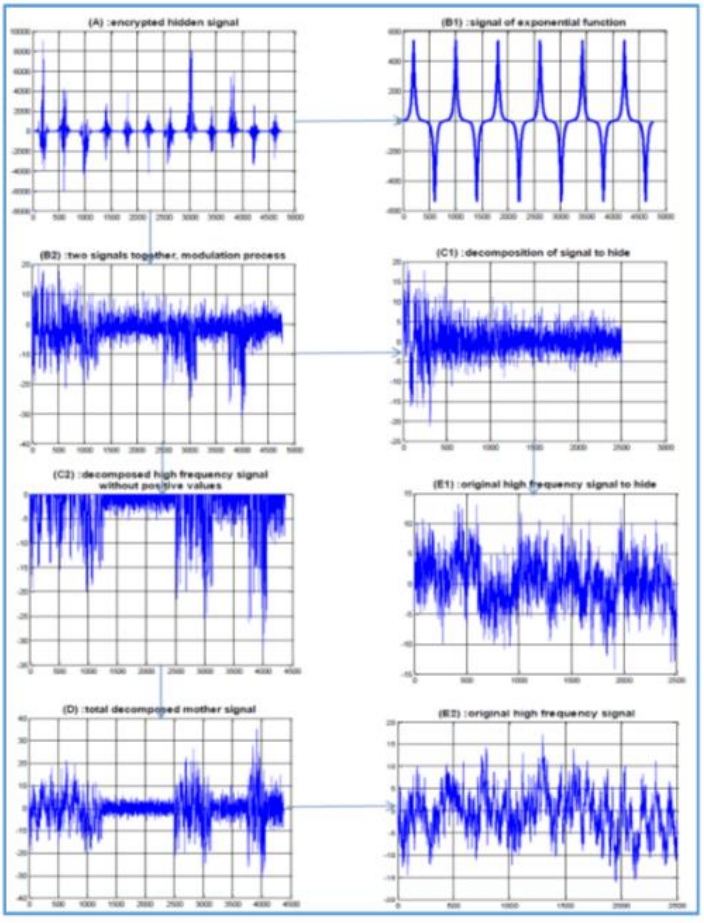

Fig. 3. Decryption of one-dimensional signal using (LFS) sine wave

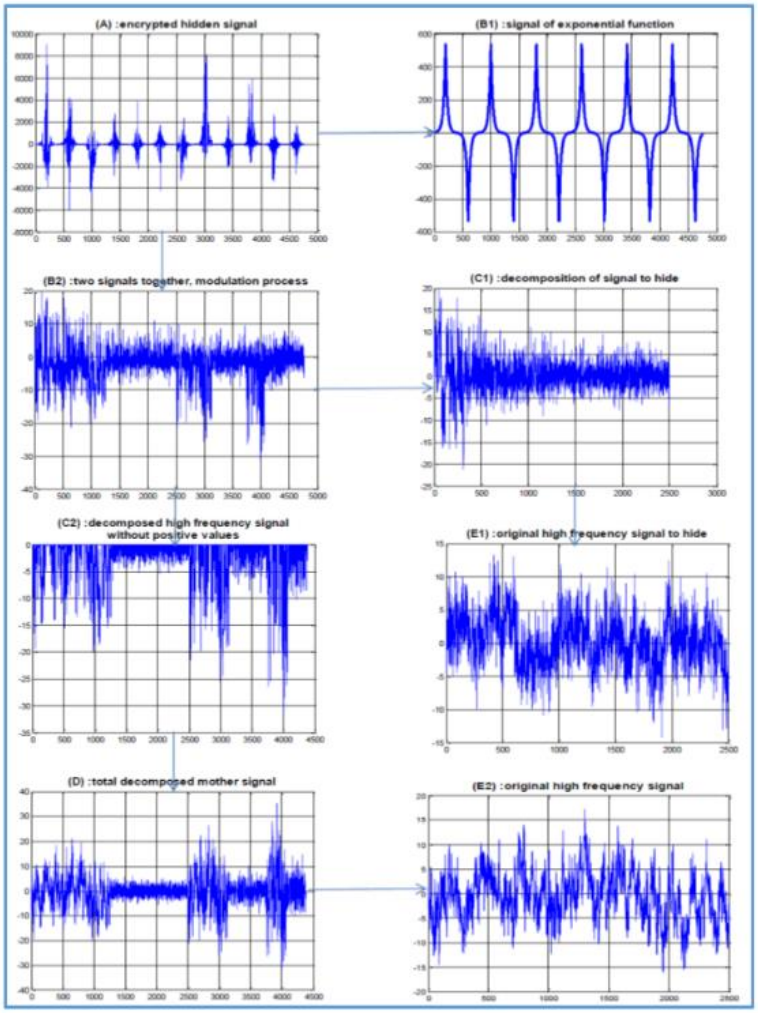

Fig. 4. Decryption of one-dimensional signal using (HFS) EEG signal

Table 3. ALGORITHM (2-a): Encrypt of 2-D image by converting it to one-dimensional signal

	ALGORITHM (2-a): Encryption Algorithm
1.	Read the first image with higher dimensions, modulated image, squares image (365x438).
2.	Read second image with lower dimensions; image to be encrypted and hidden, tree image (258x350).
3.	Decompose the first image (modulated image) using wavelet decomposition for two dimensions transform law: [c1, s1] =wavedec2(I1,3,'db1'). Decompose second image (image to hide) using wavelet decomposition for two dimensions transform law: [c2, s2] =wavedec2(I2,3,'db1').
4.	Zeroing the positive values of the mother image, (modulated signal=c1) after saving them and their locations, c11, loc1.

5.	Zeroing the negative values of image to hide, (signal to hide=c2) after saving them and their locations, c12, loc2.
6.	Make modulation process, as follow: for i=1:m: [no. of modulated signals' samples=c1]. if c1(i)==0: [(c1) is the modulated signal]. loc(k)=i:[save the locations]. count=count+1 c1(i)=c2(k): [put the values of (c2 signal) in zeros locations of modulated signal (c1) or mother signal]. end; end
7.	Prepare (exponential function) file of the same dimension of mother signal, e=m sample.
8.	Make math. Equation between (e and c1).
9.	Getting encrypted and hidden signals (images) end

Images from (A1 to F) of Figure (5) shows in details the experimental results of ALGORITHM (2-a)

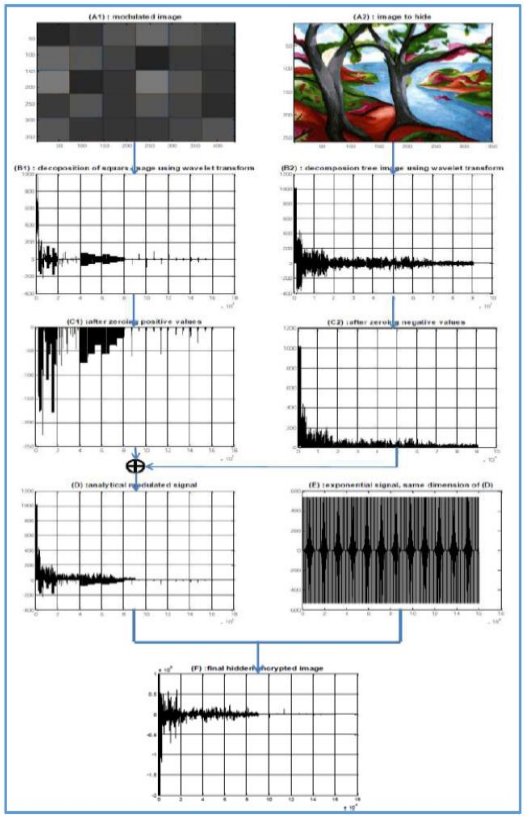

Fig. 5. Encryption of 2-D image by converting it to one-dimensional

Table 4. ALGORITHM (2-b): decrypt of one-dimensional signal to 2-D image

	ALGORITHM (2-b): decryption
1.	Make opposite math. Operation to get modulated signal
2.	Separate the modulated values about the parent signal and put these values in their locations, as follow: for i=1: n: [n is no. of signal's to hide samples]. for j=1:m: [m is no. of modulated signal's samples]. if loc2(i)==j: [loc2, the locations of signal to hide]. c2(1, k) =c1(j): [remove values of signal to hide from the modulated signal, demodulation process]. c1(j)=0: [zeroing these location]. k=k+1; end;end;end
3.	Retrieve the positive saved values of the mother signal, as follows: for i=1: n:[n is no. of signal's to hide samples]. for j=1: m: [m is no. of modulated signals' samples]. if loc1(i)==j: [loc1, the locations of positive values of the mother signal]. c1(j)=c11(i): [retrieve the positive values which saved earlier, c11]. k=k+1; end;end;end
4.	Retrieve the negative saved values of signal to hide, as follows: for i=1: n:[n is no. of signal's to hide samples]. for j=1: [m is no. of modulated signals' samples]. if loc2(i)==j: [loc2, the locations of negative values of signal to hide]. c2(j)=c12(i): [retrieve the positive values which saved erlier, c12]. k=k+1; end;end;end
5.	Aggregation of the two signals using (Idwt2= inverse decomposition of wavelet transform for two dimensions).
6.	Retrieve the original images…end

Images from (A to E2) of Figure (6) shows in details the experimental results of ALGORITHM (2-b)

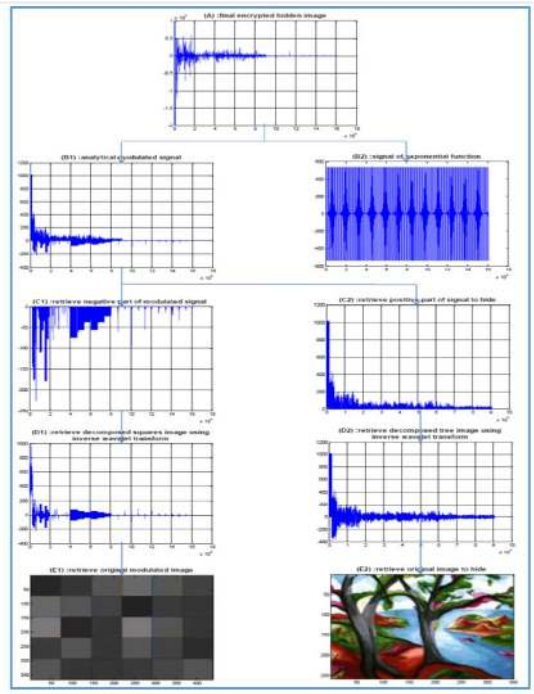

Fig. 6. Decryption of one-dimensional signal to 2D images

Table (1) illustrates the quality measurements used for the purpose of showing the efficiency of the method and comparing cases before and after the hiding and encryption operations. The measurements entropy and average were used, as follows:

Table 5. Quality measurements used for one-dimensional data

	Signal	Average	Entropy
First state	Modulated signal	1.7252	1.9816
	Sine wave (low frequency signal)	6.2422e-004	3.7574
	Mixed encrypted hidden signal (1)	5.5243	1.8805
Second state	Modulated signal	1.7252	1.9816
	High frequency signal	0.2044	1.8980
	Mixed encrypted hidden signal (2)	-2.25	0
Third state	Modulated transferred image (squares image)	8.5889	3.9231
	Hidden transferred image (tree image)	6.3632	5.7006
	Mixed encrypted hidden signal (3)	5.1626	1.0427

5 Conclusion

Many important things can be concluded during of experiments results, it is noticed from (Table 1), the average of encrypted signal differs from both of signals before

encryption because of embedding signals' process. And the entropy of encrypted signal is less than of the two signals before encryption, which means the characteristics which distinguished each signal are completely lost after they are combined into a single signal. Using of the exponential function as an intermediary in the encryption process has proven successful by obtaining completely different results from the original. The whole encryption process gave us forms of information has no similarity to the original. After removing the cover and decrypting, the resulting image or signal is exactly identical to the original.

6 References

[1] O. Abikoye, K. Adewole, and A. Oladipupo, "Efficient data hiding system using cryptography and steganography," 2012.

[2] P. P. Aung, T. M. J. I. J. o. I. T. Naing, Modeling, and Computing, "A novel secure combination technique of steganography and cryptography," vol. 2, no. 1, pp. 55-62, 2014. https://doi.org/10.5121/ijitmc.2014.2105

[3] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 81-84: IEEE. https://doi.org/10.1109/icisc.2018.8398946

[4] C. Anuradha, S. J. I. J. o. A. R. i. C. S. Lavanya, and S. Engineering, "Secure and authenticated reversible data hiding in encrypted image," vol. 3, no. 4, 2013.

[5] H. Alrikabi, A. H. Alaidi, and K. J. I. J. o. I. M. T. Nasser, "The Application of Wireless Communication in IOT for Saving Electrical Energy," vol. 14, no. 01, pp. 152-160, 2020. https://doi.org/10.3991/ijim.v14i01.11538

[6] G. Bhatnagar, Q. J. Wu, and B. J. I. S. Raman, "Discrete fractional wavelet transform and its application to multiple encryption," vol. 223, pp. 297-316, 2013. https://doi.org/10.1016/j.ins.2012.09.053

[7] H. T. S. J. W. J. o. E. S. ALRikabi, "Study the Matching of the Level of Electromagnetic Radiation Emitted by Communication Towers in the Kut City with the International Health organization criterion," vol. 4, no. 1, pp. 101-111, 2016.

[8] F. Petitcolas, R. Anderson, and M. J. S. i. o. p. o. m. c. Kuhn, "Information Hiding-A Survey'Proceedings of the IEEE," vol. 87, no. 7, pp. 1062-1078, 1999. https://doi.org/10.1109/5.771065

[9] H. Rout, B. K. J. I. J. o. E. Mishra, and C. Engineering, "Pros and cons of cryptography, steganography and perturbation techniques," pp. 76-81, 2014.

[10] C. P. Chen and C.-Y. J. I. s. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," vol. 275, pp. 314-347, 2014. https://doi.org/10.1016/j.ins.2014.01.015

[11] H. T. Alrikabi, A. H. M. Alaidi, A. S. Abdalrada, and F. T. J. I. J. o. E. T. i. L. Abed, "Analysis the Efficient Energy Prediction for 5G Wireless Communication Technologies," vol. 14, no. 08, pp. 23-37, 2019. https://doi.org/10.3991/ijet.v14i08.10485

[12] R. J. E. o. I. S. Rao and Technology, "Wavelet transforms," 2002.

[13] A. Grinsted, J. C. Moore, and S. J. N. p. i. g. Jevrejeva, "Application of the cross wavelet transform and wavelet coherence to geophysical time series," vol. 11, no. 5/6, pp. 561-566, 2004. https://doi.org/10.5194/npg-11-561-2004

[14] H. T. S. Al-Rikabi, *Enhancement of the MIMO-OFDM Technologies*. California State University, Fullerton, 2013.
[15] I. A. Aljazaery, A. A. Ali, and H. M. J. S. P. A. I. J. Abdulridha, "Classification of electroencephalograph (EEG) signals using quantum neural network," vol. 4, no. 6, p. 329, 2011.
[16] Z. Liu and S. J. O. L. Liu, "Random fractional Fourier transform," vol. 32, no. 15, pp. 2088-2090, 2007.
[17] M. R. Islam, M. S. Sayeed, and A. Samraj, "Biometric template protection using watermarking with hidden password encryption," in *2008 International Symposium on Information Technology*, 2008, vol. 1, pp. 1-8: IEEE. https://doi.org/10.1109/itsim.2008.4631572
[18] A. Atito, A. Khalifa, S. J. J. o. C. Rida, and C. Engineering, "DNA-based data encryption and hiding using playfair and insertion techniques," vol. 2, no. 3, p. 44, 2012. https://doi.org/10.20454/jcce.2012.242
[19] D. Singla and R. J. I. J. O. C. E. R. Syal, "Data security using LSB & DCT steganography in images," vol. 2, no. 2, pp. 359-364, 2012.
[20] M. H. J. I. J. o. E. T. Rajyaguru and I. Advanced Engineering, "Crystography-combination of cryptography and steganography with rapidly changing keys," pp. 2250-2459, 2012.
[21] Z. Liu *et al.*, "Optical color image hiding scheme based on chaotic mapping and Hartley transform," vol. 51, no. 8, pp. 967-972, 2013.
[22] A. A. Nair, D. J. I. J. o. E. T. Job, and Technology, "A Secure Dual Encryption Scheme combined With Steganography," vol. 13, no. 5, pp. 218-225, 2014. https://doi.org/10.14445/22315381/ijett-v13p246
[23] M. E. Saleh, A. A. Aly, F. A. J. I. I. J. o. A. C. S. Omara, and Applications, "Data security using cryptography and steganography techniques," vol. 7, no. 6, pp. 390-397, 2016.
[24] Q. Han, Y. Zhang, and H. J. F. G. C. S. Li, "Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things," vol. 83, pp. 269-277, 2018. https://doi.org/10.1016/j.future.2018.01.019
[25] P. Salama and B. King, "Efficient secure image transmission: compression integrated with encryption," in *Security, Steganography, and Watermarking of Multimedia Contents VII*, 2005, vol. 5681, pp. 47-58: International Society for Optics and Photonics. https://doi.org/10.1117/12.587011
[26] S. V. Vaseghi, *Advanced digital signal processing and noise reduction*. John Wiley & Sons, 2008.
[27] H. T. S. J. I. J. o. S. E. ALRikabi and Research, "Implementation and Estimation of Wireless Communication Channel," vol. 4, no. 10, p. 4, 2016.
[28] C.-S. Wong, J. Goree, Z. Haralson, and B. J. N. P. Liu, "Strongly coupled plasmas obey the fluctuation theorem for entropy production," vol. 14, no. 1, p. 21, 2018. https://doi.org/10.1038/nphys4253
[29] H. T. S. ALRikabi, A. H. M. Alaidi, F. T. J. J. o. A. R. i. D. Abed, and C. Systems, "Attendance System Design And Implementation Based On Radio Frequency Identification (RFID) And Arduino," vol. 10, no. 4, p. 6, 2018.
[30] O. H. Yahya, H. Alrikabi, I. A. J. I. J. o. O. Aljazaery, and B. Engineering, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," vol. 16, no. 03, pp. 107-116, 2020. https://doi.org/10.3991/ijoe.v16i03.13021
[31] C. Finn and J. J. E. Lizier, "Probability Mass Exclusions and the Directed Components of Mutual Information," vol. 20, no. 11, p. 826, 2018. https://doi.org/10.3390/e20110826

7 Authors

Ibtisam A. Aljazaery is a lecturer in the Department of Electrical Engineering, College of Engineering, University of Babylon. Babylon, Iraq. Email: ibtisamalasady @gmail.com.

The number of articles in national databases – 6. The number of articles in international databases – 5.

Haider Th. Salim ALRikabi He is presently 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 mobile generation, Control systems, intelligent technologies, smart cities, and Internet of Things (IoT). Al Kut city – Hay ALRabee, Wasit, Iraq. Contact: - +9647732212637

E-mail: - hdhiyab@uowasit.edu.iq

The number of articles in national databases - 10

The number of articles in international databases – 10

Mustafa Rabea Aziz is a lecturer at the General Directorate of Education in Nineveh. Contact: - +9647729839600 E-mail: - mustafarabee@yahoo.com

Article submitted 2020-03-06. Resubmitted 2020-04-21. Final acceptance 2020-04-21. Final version published as submitted by the authors.