Encryption System for Hiding Information Based on Internet of Things

https://doi.org/10.3991/ijim.v15i02.19869

Hala A. Naman, Naseer Ali Hussien
Wasit University, Wasit, Iraq

Mohand Lokman Al-dabag
Northern Technical University, Mosul, Iraq

Haider Th. Salim AlRikabi (✉)
Wasit University, Wasit, Iraq
hdhiyab@uowasit.edu.iq

Abstract—One of the unexpected intelligence tactics known in World War II was to conceal the data in images that were reduced to the size of a point that was used in every text and transported in front of the enemy's eyes. In the new age, and after the expansion of Internet science and the use of the Internet worldwide, we will establish a security feature of the IOT service that will work more reliably and more effectively to deal with the Internet of Things and ensure the work of the services that the customer interacts with. A secret-key stenographic scheme that embeds four gray-scale secret size (128*128) pixel images into a size (512*512) pixel cover image in this work. Wavelet transform is the method used in this project to analyses the cover into its frequency components. In this work, combinations of steganography and cryptography were made to increase the level of safety and make the device more difficult for attackers to beat. The resulting stego-image that will be transmitted did not raise any suspicion by both objective and subjective evaluation, so the primary objective of Steganography is achieved. The proposed system was designed by using (MATLAB R2018b) and running on a Pentium-4 computer. The Internet of Things works with the encryption system for data in a synchronized manner with the technological development, and in order to maintain the stability of any Internet of things service, whether it is information signal services, visual or audio data, a remote-control system, or data storage in the Internet cloud, we must focus on data preservation from internet pirates and internet system hackers. The picture Figure 4 below shows the method of encryption and dealing with the Internet of things system.

Keywords—Internet of things, Encryption, wavelet transform, PSNR, Stego image

1 Introduction

The fundamental idea behind hiding is to give us more security in our dealings. This hiding system of image consist some of steps[1, 2]. At first, we have introduced hiding image using wavelet transform be distinguished by in transforming to the frequency domain, time information is known. When looking at a wavelet transform of a signal, it is possible to tell when a particular event took place, which was chosen for this per pose, because of its simplicity. However, it runs us more security in our nature dealings as we say. This system (hiding image) will be illustrated which embeds four gray-scale secret images of size (128 x 128) pixels into cover image of size (512 x 512) pixels. The techniques will be used in this work is talks about some process that we apply on these four images that I will to hide it to apply it to vector decimal to binary 8-bit[3-5]. Another hand, we most select this image that names cover and also apply some process by using wavelet transform until we get on anew vector decimal to binary 23-bit at this stage embedding process will have happened as coming explain this program in the research. In the context of multilevel secure systems (e.g. military computer systems), Lampson defined covert channels as communication routes that were neither designed nor intended to transmit information at all. Traditionally, untrustworthy programs use these channels to leak information to their owner when performing a service for another program. In the past, these contact networks were researched at length to find ways to restrict certain systems[6]. Except as an example of clandestine communication on Ethernet networks, the idea of the Internet of Things IOT and in the sense of image downgrading, we will not expand much further on this topic[7, 8]. Anonymity is seeking ways to mask the meta content of massages, that is, a message's sender and recipients. Early examples, suggested by include anonymous re-mailers as described and onion routing. The premise is that by using a collection of re-mailers or routers, one can obscure the trail of a message as long as the intermediaries do not collude, so trust remains the cornerstone of these methods[9-11]. Notice that there are distinct depending arc variants on who is "anonymized," sender, receiver, or both. Web applications have concentrated on receiver anonymity, while sender anonymity is concerned with email users. In the Internet of Things (IOT) concept, we aim to maintain a more safe use of user data. Steganography is an important sub-discipline of data hiding. Although cryptography is about protecting messages' content, steganography is about concealing their very existence. This modern steganography adaptation, presumed from Greek, literally means "covered writing", and is generally interpreted to mean covering information in other information. Examples involve sending a message to a spy by using invisible ink to mark certain letters in a newspaper and adding sub-perceptible echoes at certain locations in an audio file[12-14]. The general model and key stenographic strategies of hiding data in other data will be demonstrated.

1.1 Encryption

We should wonder why encryption is so important and why people need to research it more. We'll learn more about encryption and the knowledge that encryption and its value should be understood to any information specialist[15, 16]. Encryption-is the analysis of mathematical methods relevant to information security aspects, such as confidentiality, integrity of data, authentication, and origination of data[17, 18]. The science behind any form of protection, mechanisms of authentication, protection of information or data, in our words, security of information and whatnot. The explanation is that whatever operating system you use, whatever programs or authentication mechanisms you implement, the actual strength of the system is highly dependent on encryption and a secret-key steganographic system to withstand attacks against potential methods. Considering several public-key encryption methods, each individual has a public key and the public key determines an encryption transformation in protected systems with a corresponding private key. Whereas the private key determines the decryption transformation associated with it[19]. A private key is accessed by any person wishing to send a message to an individual. The public key does not need to be kept secret and, in fact, only its authenticity is needed to ensure that A is indeed the only party who knows the corresponding private key is publicly available[20]. A primary benefit of such systems is that it is usually easier to have valid public keys than to securely distribute secret keys, as required in encryption systems[21].

1.2 Digital image

The interest in methods of digital image processing stems from two key fields of application. Improving pictorial information for human interpretation, and processing autonomous machine perception of scene data. Improving digitized newspaper photographs sent by submarine cable between London and New York was one of the first implementations of image processing techniques in the first category[22-24]. The invention of the Bart lane cable image transmission system in the early 1920s reduced the time required from more than a week to less than three hours to move a picture across the Atlantic. Specialized printing equipment coded and then restored images for cable transmission at the receiving end.

1.3 Fourier transform and wavelet transform

The utility of Fourier transforms lies in its ability to evaluate a signal for its frequency content in the time domain. By first transforming a function in the time domain into a function in the frequency domain, the transformation works. As the Fourier coefficients of the transformed function represent the contribution of each sinus and cosine function at each frequency, the signal can then be evaluated for its frequency content. An inverse Fourier transform converts data from the frequency domain into the time domain, exactly as you might expect[25, 26].

1.4 Wavelet transform

Wavelets are mathematical functions that split data into various components of frequency and then analyze each component with a resolution suited to its size. They have advantages in examining physical conditions where the signal includes discontinuities and sharp spikes over conventional Fourier techniques. In the areas of mathematics, quantum physics, electrical engineering, and seismic geology, wavelets were developed independently. During the past ten years, interchanges between these fields have led to many new wavelet applications, such as image compression, vibration, human vision, radar, and prediction of earthquakes. This paper presents wavelets outside of the digital signal processing area to the technical person concerned. Starting with Fourier, we explain the background of wavelets, Compare wavelet transformations with Fourier transformations, state characteristics and other special wavelet aspects, and finish with some interesting applications such as compression of images, musical tones, and noisy data de-noising[27, 28].

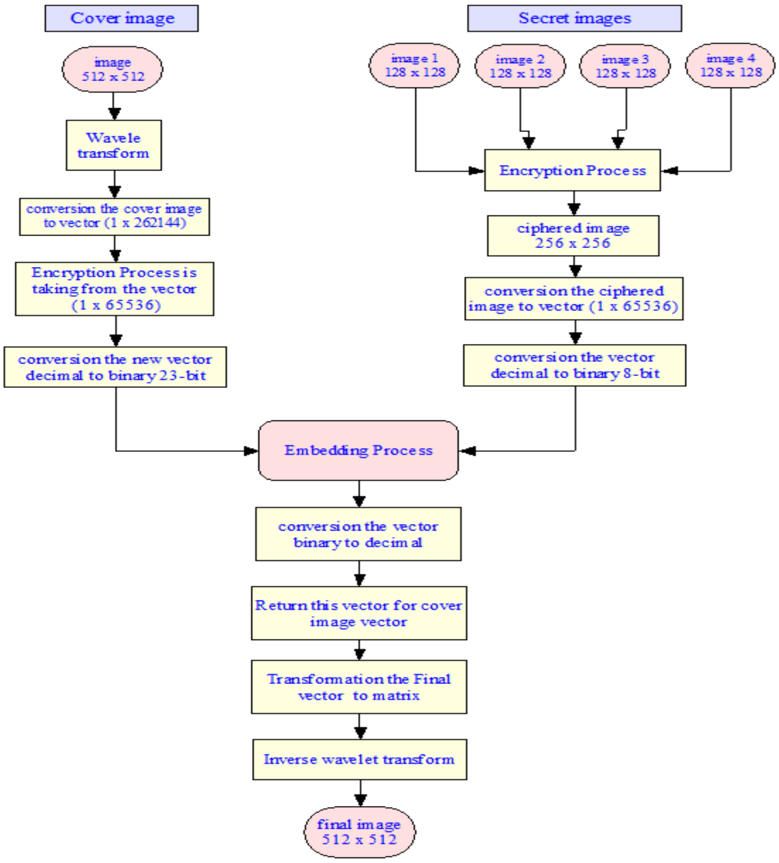

Cover image
image 512 x 512
Wavele transform
conversion the cover image to vector (1 x 262144)
Encryption Process is taking from the vector (1 x 65536)
conversion the new vector decimal to binary 23-bit
Secret images
image 1 128 x 128
image 2 128 x 128
image 3 128 x 128
image 4 128 x 128
Encryption Process
ciphered image 256 x 256
conversion the ciphered image to vector (1 x 65536)
conversion the vector decimal to binary 8-bit
Embedding Process
conversion the vector binary to decimal
Return this vector for cover image vector
Transformation the Final vector to matrix
Inverse wavelet transform
final image 512 x 512

Fig. 1. The flow chart of Image hiding

2 Proposed Method

We have two partitions fundamental as follows

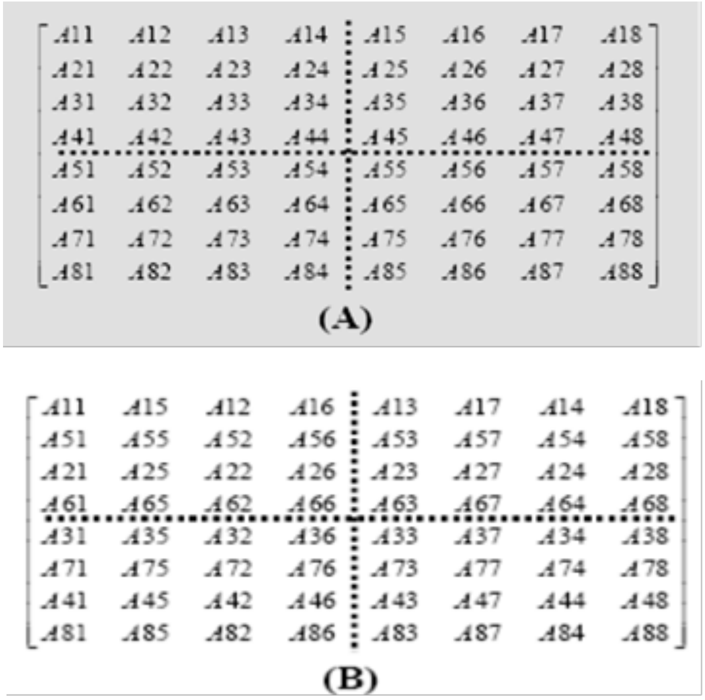
- Secret images.
- Cover image.

2.1 Secret images

Consist from the two steps as the following for:

Encryption process: The four secret images of size ***(128 x 128)*** pixel after transitions to grayscale are encrypted in such a way to form one encrypted image of size ***(256 x 256)*** pixel. The resultant image encompasses all secret images but in scrambled form as in

The additional stage redistributes the pixels of stream ciphered image according to a secret Algorithm. The above algorithm divides the stream ciphered image into four blocks of equal size. As the stream ciphered image is of size (256×256) pixels then the blocks will be of size (128×128) pixels each as fig. (A & B) [2-3].



$$\left[\begin{array}{cccc|cccc}
A11 & A12 & A13 & A14 & A15 & A16 & A17 & A18 \\
A21 & A22 & A23 & A24 & A25 & A26 & A27 & A28 \\
A31 & A32 & A33 & A34 & A35 & A36 & A37 & A38 \\
A41 & A42 & A43 & A44 & A45 & A46 & A47 & A48 \\
\hline
A51 & A52 & A53 & A54 & A55 & A56 & A57 & A58 \\
A61 & A62 & A63 & A64 & A65 & A66 & A67 & A68 \\
A71 & A72 & A73 & A74 & A75 & A76 & A77 & A78 \\
A81 & A82 & A83 & A84 & A85 & A86 & A87 & A88
\end{array}\right]$$

(A)

$$\left[\begin{array}{cccc|cccc}
A11 & A15 & A12 & A16 & A13 & A17 & A14 & A18 \\
A51 & A55 & A52 & A56 & A53 & A57 & A54 & A58 \\
A21 & A25 & A22 & A26 & A23 & A27 & A24 & A28 \\
A61 & A65 & A62 & A66 & A63 & A67 & A64 & A68 \\
\hline
A31 & A35 & A32 & A36 & A33 & A37 & A34 & A38 \\
A71 & A75 & A72 & A76 & A73 & A77 & A74 & A78 \\
A41 & A45 & A42 & A46 & A43 & A47 & A44 & A48 \\
A81 & A85 & A82 & A86 & A83 & A87 & A84 & A88
\end{array}\right]$$

(B)

Fig. 2. The algorithm used for final ciphered image. a) Stream-Ciphered Image. b) Final- Ciphered Image.

This matrix is the first block of the final ciphered image. By doing this operation to the whole pixels of the stream ciphered image we will get the final ciphered image. Figure 2 shows a typical encryption process.

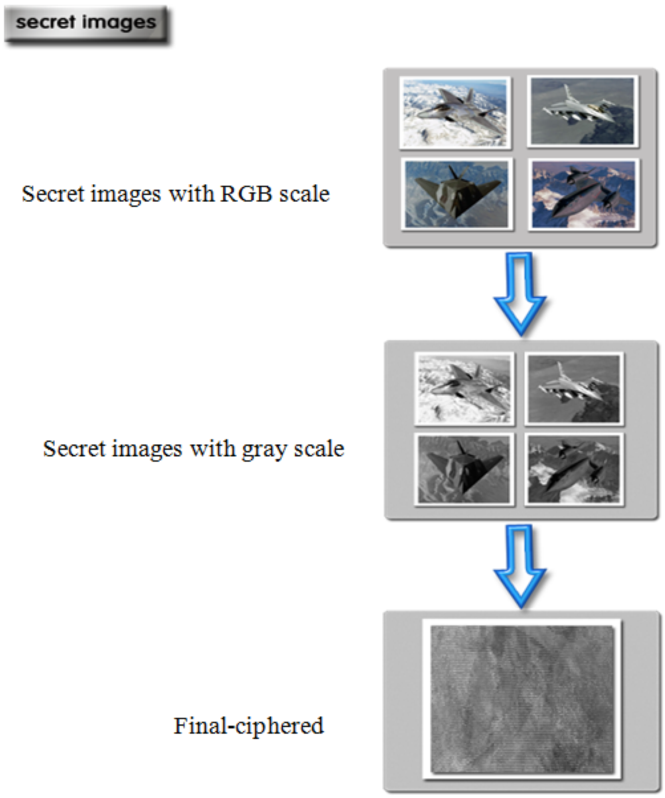


Fig. 3. The Encryption Process

Corresponding vector: The final level of the ciphering technique. The stage of ciphering is applied to the final resultant image. After conversion, the image to vector where all pixels are taken from this vector and then each pixel is converted into 8-bits. Since the image is a grayscale of 256 -level then the 8-bits is sufficient for all image.

The final step is encrypted vector Secret images with vector cover image from through repetition Encryption Process but for the cover image.

Cover image: After getting the final ciphered image, the cryptography technique has been completed; after that, the embedding process will be started with the cover image.

a) *Load cover image:* After reading any image used to cover on Secret images where completion Conversion of size ***(512 x 512)*** pixel and transitions to grayscale because that wavelet transforms requirement that .as in **fig**. **3**

b) *Encryption Process for the cover image:* After the Conversion of the cover image to vector and to Encryption Process for the cover image which taken best locations could be used to embed a secret image or message Where divide the vector into four partitions, we have taken from each part the odd number as follow in this array Will be used as a host to the 8-bits from the final encryption image.

*A*1,1 *A*1,2 *A*1,3 *A*1,4 *A*1,5 *A*1,6 *A*1,7 *A*1,8 *A*1,9 *A*1,10 *A*1,11 *A*1,12 *A*1,13 . . . *A*1,262144

*A*1,1 *A*1,5 *A*1,9 *A*1,13 . . . . *A*1,262144

Each element in the vectors consists of 24-bits. The 24th bit represents the sign of the related coefficient while the 1st bit represents the most significant bit (MSB) of the coefficient. The embedding process will place the 8-bits of the final ciphered image instead of 8- bits from the 23 bits of the coefficient; the selection of which 8- bits will be taken from the 23-bits depends on another Encryption Process for the cover image. These locations are taken between (bit 12-19, bit 13-20, bit 14-21, and bit15-23) we using (bit 15-23).

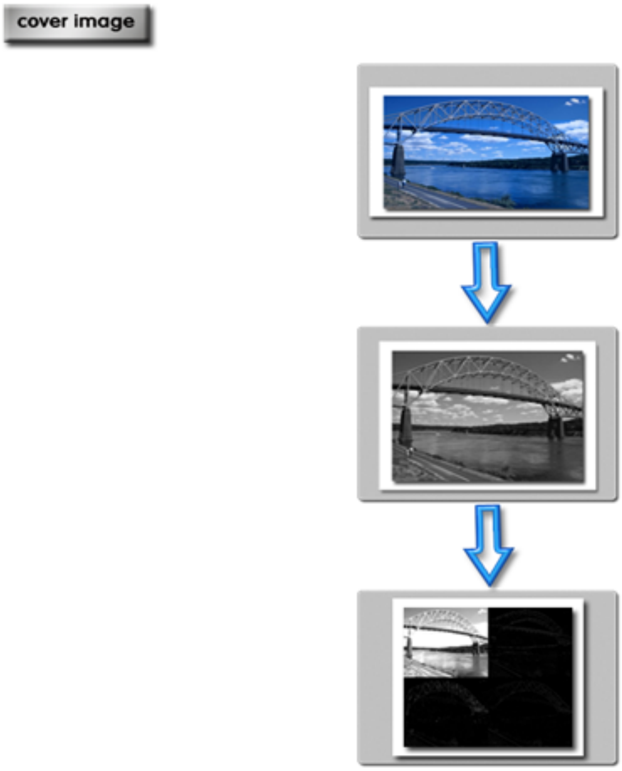


Fig. 4. Cover image by DWT.

Embedding process: After getting the final ciphered image, the cryptography technique has been completed; after that, the embedding process will be started. The coefficients obtained are the randomly organized selected from the vector of the cover image according to a randomly organized then will be used as a host to the 8-bits from the final ciphered image. Each element in the vectors of the cover image consists of 24 bits; the 24th bit represents the sign of the related coefficient while the 1st bit represents the most significant bit (MSB) of the coefficient. The embedding process will place the 8- bits of the final ciphered image instead of 8- bits from the 23 bits of the coefficient; the selection of which 8- bits will be taken from the 23 bits. We choose the best locations that could be used to embed the secret message; these locations are taken between (bit16-23). Where the 8-bit will be embedded can be identified, keeping on this process till all bits of the final ciphered image are completely embedded in the coefficients as the below. Where the number (1) appears to represents the sign coefficient for each one bit from the vector

3 The Steganography System for Recipient

The recipient will certainly get the stego object. But he could not extract the secret information out of the cover without knowledge of which keys (ciphered image & Encryption Process for cover image) have been used in the embedding process. The recipient also should know the manner used in the encryption process. For hiding based stego, when the requirements are present then the extracting process will be started. This can be done by handling the stego-object by hiding decomposition using the same procedure that is used in the proposed Steganography system for the sender, the coefficients results are rearranged like that in the sender. Using the same (ciphered image & Encryption Process for cover image) used in the sender to select the coefficients where the data has been embedded and to extract the bits of the final ciphered image[29, 30]. By taking the inverse of the ways used in the encryption process, the four secret images are perfectly reconstructed. at first, we reading the stego image which to contain Secret images were the size that is (512 x 512) pixel after taking the transitions wavelet transform requirement that. From necessary conversion the stego - image to the array that ranges 1*262144. We reverse the Encryption Process for cover image taking (1 x 65536) after converting the array from decimal to binary 32-bit. we take the position (bit 15-23) which becomes an 8-bit binary after that conversion the 8-bit to decimal value but be array provided that conversion the array to the matrix after that to reverse the encryption process so that extraction of the Secret images. as shown in the block diagram

4 Peak Signal to Noise Ratio (PSNR)

PSNR they are usually measured in decibels (dB). Used PSNR to measuring noise ratio the result from distortion because hiding process in stego image was compared with the cover image. Whenever to be PSNR large value becomes beast hiding to secret images while becoming hiding images is failing when the PSNR small value.

This improvement used psnr to realization make high quality in the work. And used the correlation quality (CQ) distortion to give a similarity range between stego images with cover image[31, 32]. The following equations of PSNR and CQ:

$$psnr = xy \max_{x,y} p_{x,y}^{2} / \sum_{x,y} (p_{x,y} - \tilde{p}_{x,y})^{2}$$

$$CQ = \sum_{x,y} p_{x,y} \tilde{p}_{x,y} / \sum_{x,y} p_{x,y}$$

5 Conclusion

In this paper we gave an overview of different steganographic methods, we present a new steganographic paradigm for digital images in wavelet transform. Secret images are embedded in the cover image by adding a weak noise signal with a specified but arbitrary probabilistic distribution. This embedding mechanism provides the user with the flexibility to mask the embedding distortion as noise generated by a particular image acquisition device. This type of embedding will lead to more secure schemes. Because an attacker must distinguish statistical anomalies that might be created by the embedding process from those introduced during the image acquisition itself. With low embedding and extraction complexity. But most importantly, because the embedding noise can have arbitrary properties that approximate a given device noise.

6 References

[1] Luo Weiqi, Huang Fangjun, Huang Jiwu %J IEEE Transactions on information forensics, and security, "Edge adaptive image steganography based on LSB matching revisited," vol. 5, no. 2, pp. 201-214, 2010. https://doi.org/10.1109/tifs.2010.2041812

[2] Nasfi Rim, Amayri Manar, and Bouguila Nizar %J Knowledge-Based Systems, "A novel approach for modeling positive vectors with inverted Dirichlet-based hidden Markov models," vol. 192, p. 105335, 2020. https://doi.org/10.1016/j.knosys.2019.105335

[3] Ye Zhiyuan, Liu Hong-Chao, and Xiong Jun %J Optics Express, "Computational ghost imaging with spatiotemporal encoding pseudo-random binary patterns," vol. 28, no. 21, pp. 31163-31179, 2020. https://doi.org/10.1364/oe.403375

[4] Waqas Umer Aziz, Khan Majid, Batool Syeda Iram %J Multimedia Tools, and Applications, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," vol. 79, no. 9, pp. 6891-6914, 2020. https://doi.org/10.1007/s11042-019-08570-5

[5] Yahya Omar Hashim, Alrikabi Haider, and Aljazaery Ibtisam "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.

[6] Rizvi Syed, Orr RJ, Cox Austin, Ashokkumar Prithvee, and Rizvi Mohammad R %J Internet of Things, "Identifying the attack surface for IoT network," vol. 9, p. 100162, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

[7] Hong Sun-ha, Technologies of Speculation: The Limits of Knowledge in a Data-Driven Society. NYU Press, 2020.

[8] Waraga Omnia Abu, Bettayeb Meriem, Nasir Qassim, Talib Manar Abu %J Computers, and Security, "Design and implementation of automated IoT security testbed," vol. 88, p. 101648, 2020. https://doi.org/10.1016/j.cose.2019.101648

[9] Goldschlag David M, Reed Michael G, and Syverson Paul F, "Hiding routing information," in International workshop on information hiding, 1996, pp. 137-150: Springer. https://doi.org/10.1007/3-540-61996-8_37

[10] Ando Megumi, Lysyanskaya Anna, and Upfal Eli, arXiv preprint arXiv:.05367, "Practical and provably secure onion routing," 2017.

[11] Hussien Naseer, Ajlan Iman, Firdhous Mohamed Mohamed, and Alrikabi Haider, "Smart Shopping System with RFID Technology Based on Internet of Things,"international journal of interactive mobile technologies, vol. 14, no. 4, pp.17-29, 2020. https://doi.org/10.3991/ijim.v14i04.13511

[12] Al-Sanjary Omar Ismael, Ibrahim Omar Ahmed, and Sathasivem Kaswiini, "A New Approach to Optimum Steganographic Algorithm for Secure Image," in 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 2020, pp. 97-102: IEEE. https://doi.org/10.1109/i2cacis49202.2020.9140186

[13] Alam Firoz, "Secure Data Transmission Using AES Cryptography in Color Image Steganography," 2017.

[14] Roa'a M Al_airaji, Aljazaery Ibtisam A, Al_Dulaimi Suha Kamal, Alrikabi Haider TH Salim, and Informatics, "Generation of High Dynamic Range for Enhancing the Panorama Environment," Bulletin of Electrical Engineering, vol. 10, no. 1, 2020. https://doi.org/10.11591/eei.v10i1.2362

[15] Bashir Imran, Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Packt Publishing Ltd, 2018.

[16] Aljazaery Ibtisam A, Alrikabi Haider Th Salim, and Aziz Mustafa Rabea, international journal of interactive mobile technologies, "Combination of Hiding and Encryption for Data Security," vol. 14, no. 9, p. 35, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[17] Xu Jian, Wei Laiwen, Wu Wei, Wang Andi, Zhang Yu, and Zhou Fucai %J Future Generation Computer Systems, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," vol. 108, pp. 1287-1296, 2020. https://doi.org/10.1016/j.future.2018.04.018

[18] Alrikabi Haider TH, Alaidi Abdul Hadi M, Abdalrada Ahmad Shaker, and Abed Faisal Theyab, International Journal of Emerging Technologies in Learning, "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

[19] Abdeldaym Rasha Samir, Abd Elkader Hatem Mohamed, Hussein Reda %J IJ of Electronics, and Engineering Information, "Modified rsa algorithm using two public key and chinese remainder theorem," vol. 10, no. 1, pp. 51-64, 2019.

[20] Lebedev Ilia, Hogan Kyle, and Devadas Srinivas, "Secure boot and remote attestation in the sanctum processor," in 2018 IEEE 31st Computer Security Foundations Symposium (CSF), 2018, pp. 46-60: IEEE. https://doi.org/10.1109/csf.2018.00011

[21] Narayana V Lakshman, Bharathi CR %J Journal of Theoretical, and Technology Applied Information, "Identity based cryptography for mobile ad hoc networks," vol. 95, no. 5, p. 1173, 2017.

[22] Yadav Krishna Chandra, "Removal of High-Density Salt and Pepper Noise in Digital Image Using Proposed Algorithm," 2018.

[23] Salhaoui Marouane, Molina-Molina J Carlos, Guerrero-González Antonio, Arioua Mounir, and Ortiz Francisco J %J Remote Sensing, "Autonomous Underwater Monitoring System

for Detecting Life on the Seabed by Means of Computer Vision Cloud Services," vol. 12, no. 12, p. 1981, 2020. https://doi.org/10.3390/rs12121981

[24] Shaima Miqdad Mohamed Najeeb Haider Th. Salim Alrikabi, Shaima mohammed Ali, "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," Telkomnika, vol. 19, no. 1, 2020. https://doi.org/10.12928/telkomnika.v19i1.17884

[25] Panna Bhaskar, Kumar Sumit, and Jha Rajib Kumar %J IETE Technical Review, "Image encryption based on block-wise fractional fourier transform with wavelet transform," vol. 36, no. 6, pp. 600-613, 2019. https://doi.org/10.1080/02564602.2018.1533892

[26] Borisagar Komal R, Thanki Rohit M, and Sedani Bhavin S, "Fourier Transform, Short-Time Fourier Transform, and Wavelet Transform," in Speech Enhancement Techniques for Digital Hearing Aids: Springer, 2019, pp. 63-74. https://doi.org/10.1007/978-3-319-96821-6_4

[27] Tary Jean Baptiste, Herrera Roberto Henry, van der Baan Mirko %J Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Sciences Engineering, "Analysis of time-varying signals using continuous wavelet and synchrosqueezed transforms," vol. 376, no. 2126, p. 20170254, 2018. https://doi.org/10.1098/rsta.2017.0254

[28] Rhif Manel, Ben Abbes Ali, Farah Imed Riadh, Martínez Beatriz, and Sang Yanfang %J Applied Sciences, "Wavelet transform application for/in non-stationary time-series analysis: a review," vol. 9, no. 7, p. 1345, 2019. https://doi.org/10.3390/app9071345

[29] Esin Joseph Okon, Agana Moses Adah, Ofem Ofem Ajah, Bukie Paultu Tawo, and Ana Prince Onebieni, "Amalgamation of Cryptography and Steganography on Global Security Systems."

[30] Taha Mustafa Sabah, Rahim Mohd Shafry Mohd, Lafta Sameer Abdulsattar, Hashim Mohammed Mahdi, and Alzuabidi Hassanain Mahdi, "Combination of steganography and cryptography: A short survey," in IOP conference series: materials science and engineering, 2019, vol. 518, no. 5, p. 052003: IOP Publishing. https://doi.org/10.1088/1757-899x/518/5/052003

[31] Erfurt Johannes, Helmrich Christian R, Bosse Sebastian, Schwarz Heiko, Marpe Detlev, and Wiegand Thomas, "A study of the perceptually weighted peak signal-to-noise ratio (WPSNR) for image compression," in 2019 IEEE International Conference on Image Processing (ICIP), 2019, pp. 2339-2343: IEEE. https://doi.org/10.1109/icip.2019.8803307

[32] Tanabe Yoshinori, Ishida Takayuki %J Radiological physics, and technology, "Quantification of the accuracy limits of image registration using peak signal-to-noise ratio," vol. 10, no. 1, pp. 91-94, 2017. vol. 10, no. 1, pp. 91-94, 2017 https://doi.org/10.1007/s12194-016-0372-3

7 Authors

Hala A. Naman Received M.Sc degree in computer engineering in 2014, from university of technology and I am a PhD. Candidate in information engineering and communication.

Naseer Ali Hussien is presently an Associate Professor and the Assistant Dean for Scientific Affairs of the Education College for Pure Sciences, Wasit University in Al Kut, Wasit, Iraq. He received his B.Sc. degree in Computer Science in 2000 from the Baghdad University in Baghdad, Iraq, his M.Sc. degree in Computer Science focusing on Computer Network and Communications from Hamdard University, Delhi, India

in 2008 and the PhD in Information Technology from University Utara Malaysia in 2013. His current research interests include network performance monitoring and analysis, wireless and mobile ad hoc networks, network protocol engineering, network simulation, network applications, smart cities, Internet of Things (IoT) and Internet of Vehicle (IoV). Al Kut city – Hay ALRabee, Wasit, Iraq. Contact:- +9647711021768. E-mail: - naseerali@uowasit.edu.iq

Mohand Lokman Aldabag completed his Ph.D. Program at Yasar University, Turkey. He received his B.E. in computer engineering degree from technical college\Mosul and his MSc. Degree in computer engineering from Mosul University, 1n 1998 and 2002 respectively. He worked at the department of technical computer engineering\ Northern Technical university as an assistant lecturer in 2002-2012 and as a lecturer in the same university from 2012 till now. He published five articles in signal processing and hardware simulation of discrete wavelets. His research interests are biomedical signal processing, wavelet transform, and signal classification.

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 – 20.

Article submitted 2020-10-16. Resubmitted 2020-11-17. Final acceptance 2020-11-17. Final version published as submitted by the authors