

Binary decomposition-based Image cipher algorithm with flexible method for key construction

Salim Muhsin Wadi¹, Huda Hussein Abed¹, Nada Taher Malik², Ahmed Taha Abdulsadah¹

¹Department of Communication Techniques Engineering, Engineering Technical College-Najaf (ETCN),
Al-Furat Al-Awsat Technical University (ATU), Kufa, Iraq

²Computer Center, Al-Dewaniyah Technical Institute, Al-Furat Al-Awsat Technical University (ATU), Kufa, Iraq

Article Info

Article history:

Received Mar 30, 2022

Revised Jul 28, 2022

Accepted Aug 5, 2022

Keywords:

ASCII codes pixels

Binary codes decomposition

Confidential images

Secret keys

Smart key constructions

ABSTRACT

Image security is still one of the important fields in multimedia processing because it's used in our daily lives. Watermarking, steganography, and ciphering are three directions to keep an image secret. Encryption defined as the process of changing information (which called plaintext) into an unreadable secret format (which called cipher-text). A new ciphering algorithm based on binary decomposition and binary codes conversion is proposed in this paper. The key is constructed in a flexible way based on the size of a secret image using some logical operations to increase the security levels. Three test images in different sizes were used to evaluate the performance of the proposed algorithm. The results of the visual scene and statistical factors proved that the suggested method was ciphering the image with high security. The proposed work was validated to confirm its effectiveness. As conclusions, the uses of decomposition and simple binary operations have given high-level image security. Also, key construction is an important step to face several types of attackers.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Salim Muhsin Wadi

Department of Communication Techniques Engineering, Engineering Technical College-Najaf

Al-Furat Al-Awsat Technical University

Najaf, Iraq

Email: coj.sal@atu.edu.iq

1. INTRODUCTION

Multi-media fast developing in last years required improving the processing techniques for video, audio and image files. Digital image was one of the interest fields in the multi-media word that need to enhance its tools and techniques in the several directions such as enhancement, recognition, security, comparison, segmentation, etc. Today, keeping images secure become one of the complicated challenges that facing security technicians in transferring and storing images operations [1]-[5].

Image encryption techniques play a important role in multimedia applications to secure and authenticate digital images. In general, the multimedia security techniques are classified into encryption and hiding. Encryption techniques effectively protect multimedia information by converting it into an unknown form by the adversary [6]. Since the 16th century, encryption techniques appeared and remained constantly evolving in parallel line with hacking techniques improving. Image encryption techniques classified depends several vactors to multiple techniques for example: based on representation to frequency or spatial domain, based on key to private or public key, the data size that encrypted at a time to block or stream [7]-[10]. Encryption in the spatial domain is more effective than frequency domain in terms of simplicity and computational cost, consequently encryption in the spatial domain is more compatible with image encryption.

The values or locations or values and locations pixels in digital image will be changed in ciphering techniques that based on spatial domain [9]. Recently, much ciphering algorithms based on chaos theory were proposed for image encryption [11]-[16]. However, the computation more complicated and the security levels are low in chaos theory based ciphering algorithms [17]. Other ciphering algorithms were proposed based on decomposition techniques [15], [18]-[21]. However, the drawbacks of those techniques were the security levels rustiness because of the bit planes numbers and its contents are constant in additive to key space were little. Advanced encryption standard (AES) and data encryption standard (DES) are famous ciphering algorithms called naïve encryption algorithm which used in many applications such as smart cards, cell phone, automated teller machines, and internet servers [22]-[23]. Main problems in the naïve algorithm were computation cost so much and have artifacts appearance in the ciphered image when the original has a large region of a single colour [24]-[25].

In this paper, binary codes decomposition-based image ciphering algorithm was proposed. Binary codes were used to decompose the image before reordering the bit planes. Image confusion was achieved using ASCII codes and add round key. New method was used to extraction key from secret image itself. The paper sections will be explained in Section 2 the details of proposed image ciphering algorithm for encryption and decryption will be shown. The results will be showed in Section 3. The paper conclusions explained in Section 4.

2. METHOD

The proposed method for encryption and decryption will be described in details as the following steps. Part A explain the steps of encryption, while the decryption steps explained in part B. After that, part C shows the steps of key construction. Finally, the block diagrams of encryption, decryption and key construction steps are shown in Figures 1 and 2.

A. Encryption part: the steps of the proposed encryption algorithm are explained below.

1. After reading the secret image, it will be decomposed using binary bit planes to get 8-planes with ones and zeros values then these bit planes reordered before reconstruction secret images from reordered bit planes.
2. Convert the pixels values of the reconstructed image from decimal to hex-decimal, where the value of each pixel is represented in two digits in the hex-decimal system.
3. Each digit of the hex-decimal pixel value is converted to its equivalent in ASCII codes which are represented in two digits.
4. Add round key is the final step where XOR logical operation between key results from key expansion operation (will be explained in subsection c) and pixel values results from ASCII operation.

B. Decryption part: it is reverse of encryption steps as shown below:

1. Add round key operation through EX-OR logical operation between secret pixel and key
2. Convert the resulted image from AddRoundKey operation Hex-decimal system
3. The Hex-decimal number converted to its equivalent in decimal.
4. Decomposing the image to binary bit planes before re-ordering its to initial order, then reconstructing the image from reordered bit-plane to get the secret image.

C. The key construction operation: the steps for the key construction according to the size of the desired image are demonstrated as follows:

1. Choose four pixels from the same image that needs to encrypt.
2. Create a logical AND operation between two of them and a logical OR operation between the other two, and then perform a logical XOR between the outcome of the two processes, as demonstrated below.


```
Pixel_1= image (150,25)
Pixel_2= image (15,150)
Pixel_3= image (100,105)
Pixel_4= image (115,10)
Outcome_1=bitand (Pixel_1, Pixel_2)
Outcome_2= bitor (Pixel_3, Pixel_4)
Outcome =bitxor (Outcome_1, Outcome_2)
```
3. Derive an entire key according to the size of the image based on the outcome of the previous logical operation, as explained below.
 - Decrease the value of the outcome logical operation by one and if the value reaches zero, then complemented it to become 255.
 - Create a matrix that contains all values of the entire key.

4. Perform a logical XOR operation between the derived key and the required image that needs to encrypt.
5. Return the values of four pixels to the cipher image in order to utilize them in the receiving part for reconstructing the original image.

Figure 1 illustrates the block diagram of the key construction steps. Figures 2 demonstrate the different stages used for the proposed scheme at the sending and the receiving sides, which mean encryption steps in Figure 2(a) and decryption steps in Figure 2(b).

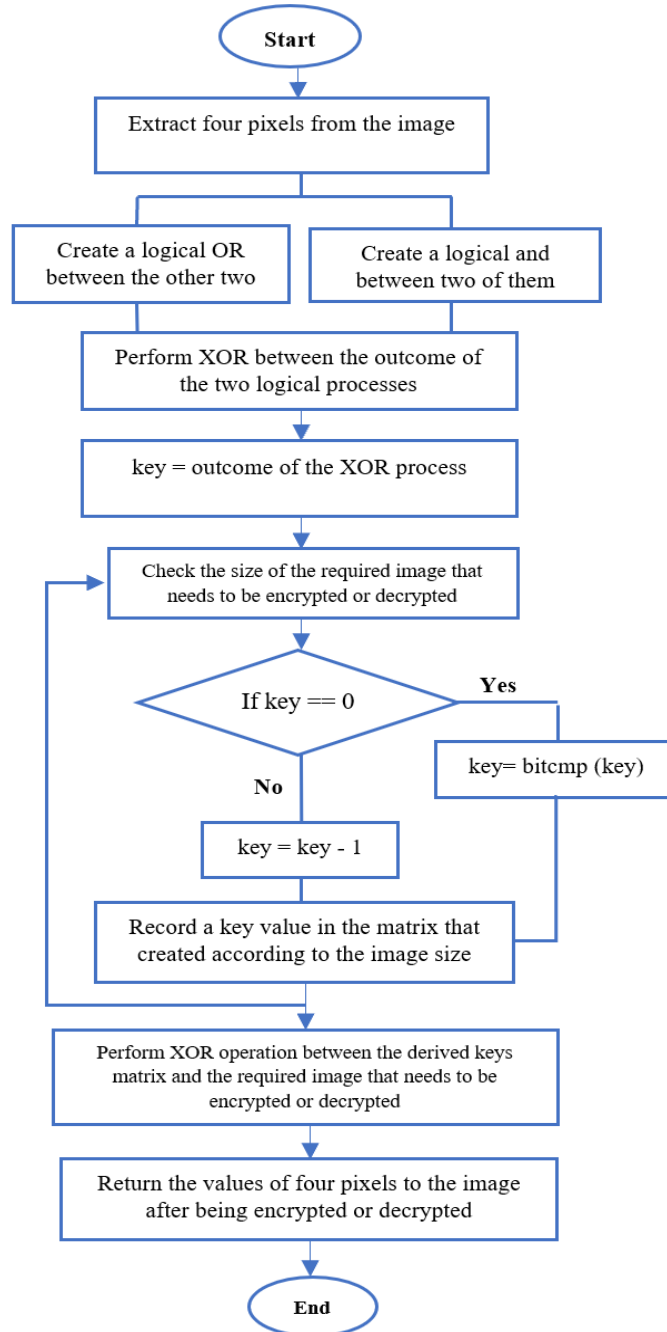


Figure 1. The key construction process

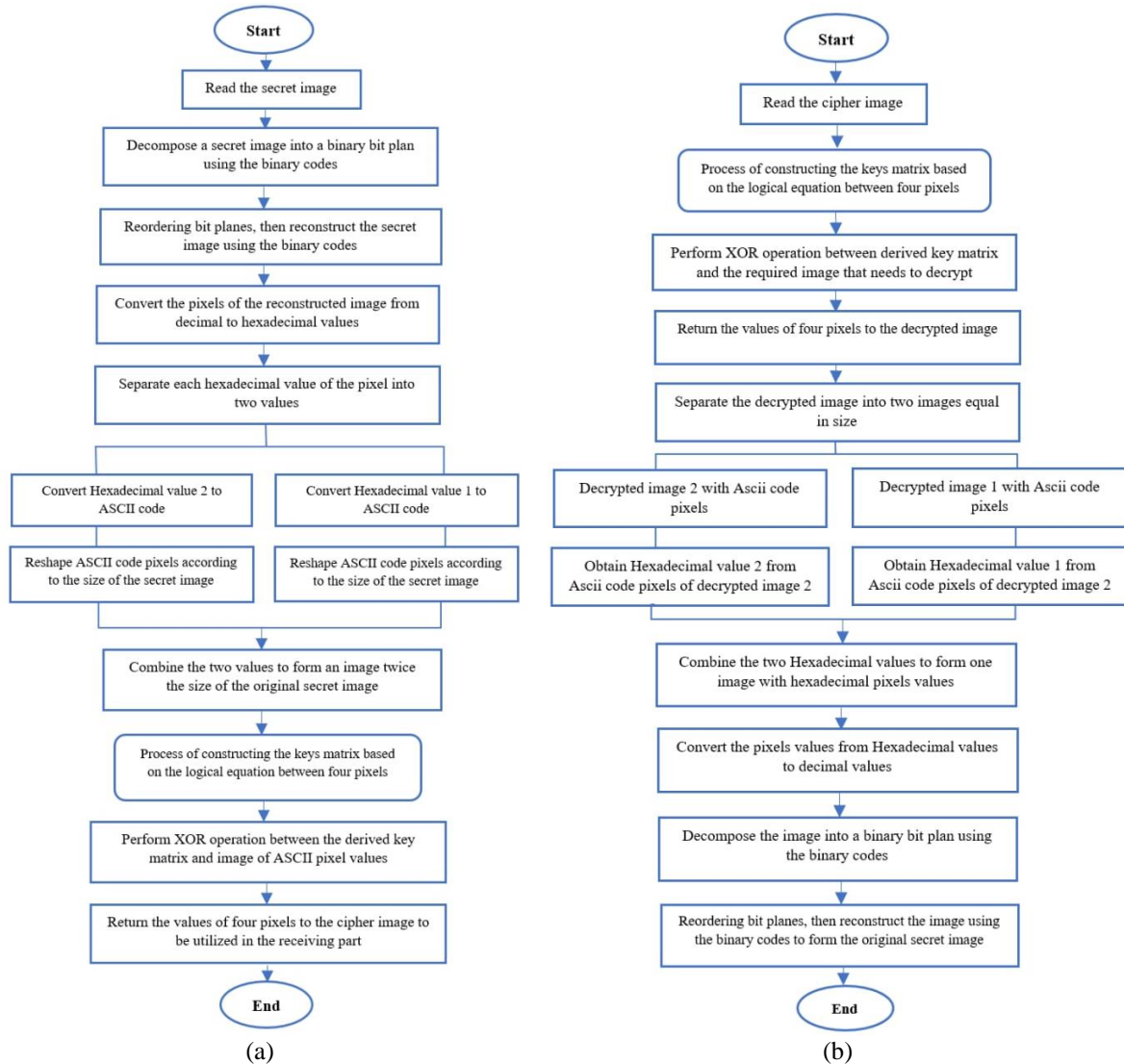


Figure 2. Proposed ciphering algorithm (a) the sending side and (b) the receiving side

3. RESULTS AND DISCUSSION

MATLAB (R2020a) is utilized for the implementation of the proposed algorithm. Images of different sizes (256×256, 512×512 and 1024×1024) are tested to observe the performance of the proposed scheme at sending and receiving sides, respectively. All images utilized for the test are taken from the image database (“SIPI Image Database”). The suggested algorithm performance was evaluated through visual scenes of image after each step with its histogram (see Figures 3-5) in additive to statistical evaluation as shown in Table 1. Figures 3(a)-(d), Figures 4(a)-(d), and Figure 5(a)-(d) depict the images with their histogram through the different stages used for the encryption scheme at the sending side.

As depicted according to the figures above, ciphered image visual scenes of all tested images are compatible with ciphering requirements. The histogram of the encrypted image is different from the histogram of the original image, it is close to the uniform distribution and that indicates the strength of the suggested encryption algorithm performance. On the other hand, the other important point is the encrypted image is quite different from the original image in terms of size, which increases the security levels through camouflaging the attacker about the original image size. However, this increases the transmitting channel requirements.

Table 1 explains the entropy values for the tested images and the time spent for the images tested at the sending and receiving sides, respectively. Relative to the values shown in Table 1, the efficiency of the proposed algorithm can be observed in terms of the little time spent at the sending and receiving sides, respectively. In addition to entropy values that are close to 8 for the images utilized to examine the

performance of the suggested algorithm. To confirm the effectiveness of proposed algorithm was validated with work in [26] through comparison the ciphered image entropy and algorithms execution time as shown in Tables 2 and 3.

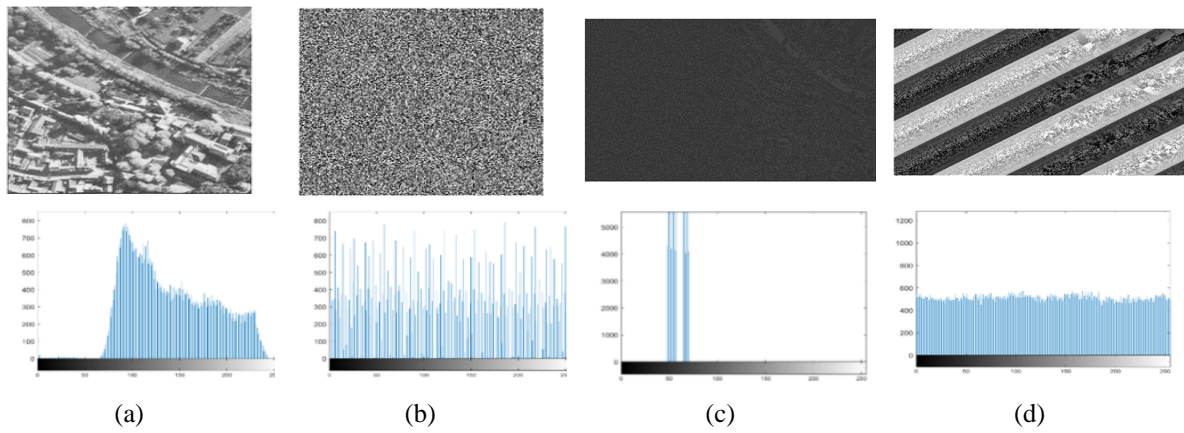


Figure 3. 256×256 Aerial image (a) secret image, (b) decomposed image, (c) converted to ASCII code, and (d) ciphered image

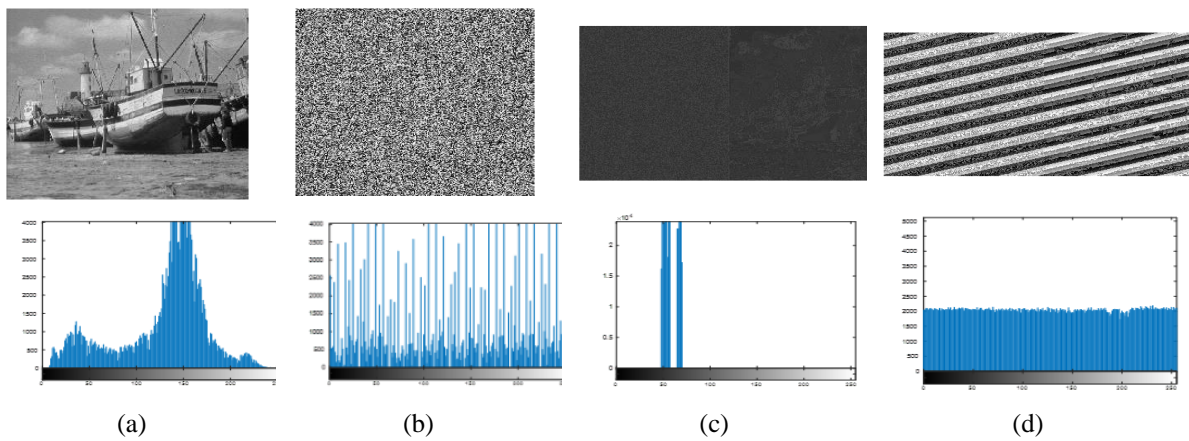


Figure 4. 512×512 Boat image (a) secret image, (b) decomposed image, (c) converted to ASCII code, and (d) ciphered image

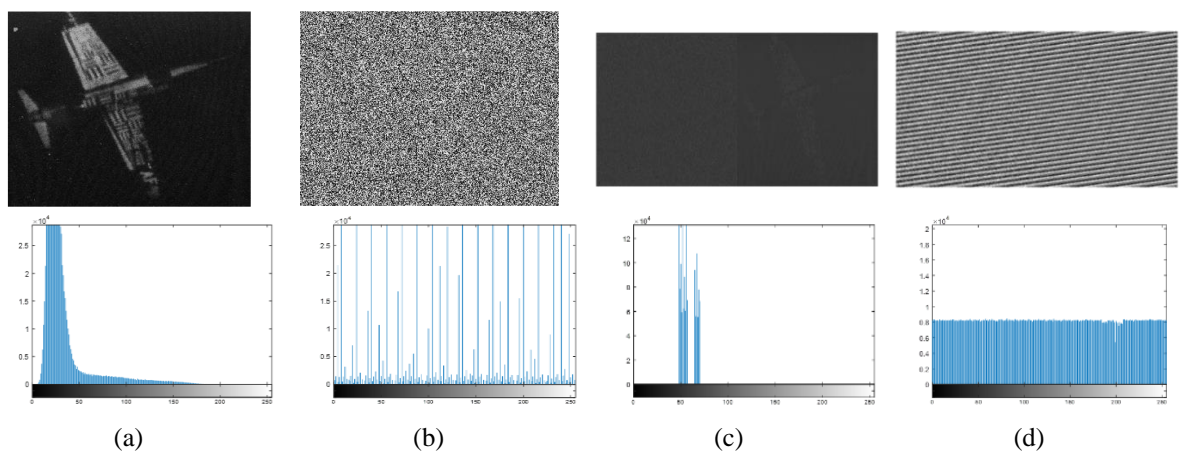


Figure 5. 1024×1024 Airplane image (a) secret image, (b) decomposed image, (c) converted to ASCII code, and (d) ciphered image

Table 1. Exploration of the performance of the suggested algorithm

Details	Entropy	Time spent at the sending side	Time spent at the receiving side
Aerial of Size 256×256	7.9984	2.334467 seconds	0.942702 seconds
Boat of Size 512×512	7.9995	6.370518 seconds	1.793895 seconds
Airplane of Size 1024×1024	7.9994	36.839402 seconds	7.838441 seconds

Table 2. Entropy comparison between proposed work and [26]

Images	Proposed work Entropy	Entropy of Setyono <i>et al.</i> [26]
Bicycle	7.9987	7.9984
City	7.9983	7.9982
Mandrill	7.9982	7.9982
Gold hill	7.9988	7.9983

Table 3. Time execution comparison between proposed work and [26]

Images	Time of reordering bit plans using binary codes	Time of convert pixels from Hex. Value to ASCII code	Time of ciphering the image of ASCII pixel values	Total time for protection the secret image	Time of Setyono <i>et al.</i> [26] for RSA+Vernam
Bicycle	0.778106	0.054770	0.014312	0.847188	1.27736
City	0.767816	0.053364	0.015928	0.837108	1.20308
Mandrill	0.826152	0.041013	0.022173	0.889338	1.38710
Gold hill	0.761701	0.057671	0.015795	0.835167	1.31398

As clearly shown in results of Tables 2 and 3 the entropy and time execution are enhanced in proposed algorithm compared with algorithm in [26]. Six factors used to compare the ciphering algorithm in [26] with proposed method are type of secret image, number of security schemes in algorithm, the inputs required for the image encryption scheme, the inputs required for the image decryption scheme, keys features and the size of the secret image after ciphering. First and final factors are same in two algorithms, while other factors are better in proposed method as in Table 4. As a result, the proposed algorithm is better in most factors from algorithm in [26].

Table 4. Comparison between algorithm in [26] and proposed algorithm

Comparison points	Setyono <i>et al.</i> [26]	Proposed scheme
Type of the secret image	Grayscale image	Grayscale image
Number of security schemes to protect the secret image	Two security schemes: 1. RSA algorithm 2. Vernam cipher	Three security schemes: 1. Decompose the image using binary codes, and then alter the order of bit planes. 2. Convert the image into a hexadecimal system to separate the value of each pixel in the hexadecimal system into two ASCII values. 3. Encrypt the image that contains ASCII pixel values with a secret key matrix that is the same size as the image.
The inputs required for the image encryption scheme	1. Public key of RSA scheme. 2. Vernam key.	Only a secret grayscale image, thus the encryption scheme does not require extra data to be exchanged to retrieve the secret image.
The inputs required for the image decryption scheme	1. Private key of RSA scheme. 2. Vernam key. 3. A cipher grayscale image.	Only a cipher grayscale image, where the procedure of creating confidential keys depends on a logical equation derived from the cipher image itself.
Keys features	A random key for Vernam with the strong key of RSA makes it difficult to decrypt the image. However, it requires the exchange of keys between the sender and the receiver, and this requires time and a secure transfer of the secret keys.	The keys are constructed in a flexible way based on the size of a secret image using a logical equation derived from the secret image itself. Therefore, there is no exchange of keys between the sender and receiver parties.
The size of the secret image after ciphering	Twice the size of the original secret image.	Twice the size of the original secret image.

4. CONCLUSION

In this paper, a secure algorithm for encrypting images is suggested. It is capable of providing three levels of security for the images. The first level of security is accomplished by decomposition the image using binary codes, then altering the order of bit planes. After that, bit planes are reconstructed to form the




same size as the image. The second level of security depends on converting the image into a hexadecimal system to separate the value of each pixel in the hexadecimal system into two ASCII values, and then the image is reconfigured to form twice the size of the original image. The third level of security involves encryption image by creating a matrix of secret keys with the same size as the image of ASCII pixel values. The procedure of creating confidential keys depends on a logical equation derived from the secret image itself. The results confirm the efficiency of the suggested algorithm in providing effective protection for confidential images.

REFERENCES




- [1] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, Sep. 2010, doi: 10.1016/j.optcom.2010.04.056.
- [2] J.-W. Han, "Optical image encryption based on XOR operations," *Optical Engineering*, vol. 38, no. 1, p. 47, Jan. 1999, doi: 10.1117/1.602060.
- [3] M. S. Kankanhalli and T. T. Guan, "Compressed-domain scrambler/descrambler for digital video," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 2, pp. 356–365, May 2002, doi: 10.1109/TCE.2002.1010142.
- [4] S. Sudharsanan, "Shared key encryption of JPEG color images," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp. 1204–1210, Nov. 2005, doi: 10.1109/TCE.2005.1561845.
- [5] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Jan. 2020, doi: 10.1007/s11831-018-9298-8.
- [6] M.-C. Chen, S. S. Agaian, and C. L. P. Chen, "Image security and recognition system," University of Texas, 2010.
- [7] H. T. Chang, H. E. Hwang, and C. L. Lee, "Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain," *Optics Communications*, vol. 284, no. 18, pp. 4146–4151, Aug. 2011, doi: 10.1016/j.optcom.2011.04.065.
- [8] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, p. 107340, Mar. 2020, doi: 10.1016/j.sigpro.2019.107340.
- [9] C. Fu, B. Bin Lin, Y. S. Miao, X. Liu, and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, Nov. 2011, doi: 10.1016/j.optcom.2011.08.013.
- [10] J. Daemen and V. Rijmen, "The block cipher rijndael," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1820, 2000, pp. 277–284.
- [11] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *Journal of the Franklin Institute*, vol. 348, no. 8, pp. 1797–1813, Oct. 2011, doi: 10.1016/j.jfranklin.2011.05.001.
- [12] S. E. Borujeni and M. Eshghi, "Chaotic image encryption system using phase-magnitude transformation and pixel substitution," *Telecommunication Systems*, vol. 52, no. 2, pp. 525–537, May 2013, doi: 10.1007/s11235-011-9458-8.
- [13] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16–17, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001.
- [14] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Communications*, vol. 284, no. 22, pp. 5290–5298, Oct. 2011, doi: 10.1016/j.optcom.2011.07.070.
- [15] P. Rakheja, P. Singh, and R. Vig, "An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain," *Optics and Lasers in Engineering*, vol. 134, p. 106177, Nov. 2020, doi: 10.1016/j.optlaseng.2020.106177.
- [16] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, Mar. 2011, doi: 10.1016/j.ins.2010.11.009.
- [17] A. N. Pisarchik and M. Zanin, "Chaotic map cryptography and security," *Encryption: Methods, Software and Security*, pp. 1–28, 2010.
- [18] L. Chen, D. Zhao, and F. Ge, "Image encryption based on singular value decomposition and Arnold transform in fractional domain," *Optics Communications*, vol. 291, pp. 98–103, Mar. 2013, doi: 10.1016/j.optcom.2012.10.080.
- [19] Q. Sun, W. Yan, J. Huang, and W. Ma, "Image encryption based on bit-plane decomposition and random scrambling," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, Apr. 2012, pp. 2630–2633, doi: 10.1109/CECNet.2012.6201673.
- [20] W. Zheng, C. Z. Gang, and C. Y. Li, "Image data encryption and hiding based on wavelet packet transform and bit planes decomposition," in *2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008*, Oct. 2008, pp. 1–4, doi: 10.1109/WiCom.2008.773.
- [21] Y. Zhou, K. Panetta, and S. Agaian, "Image encryption algorithms based on generalized P-Gray Code bit plane decomposition," in *Conference Record-Asilomar Conference on Signals, Systems and Computers*, 2009, pp. 400–404, doi: 10.1109/ACSSC.2009.5469840.
- [22] FIPS PUB, "Data Encryption Standard (DES)," *U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology*, vol. 46, no. 3, 1999.
- [23] National Institute of Standards and Technology Department of Commerce (FIPS Pub 197), *Advanced Encryption Standard (AES)*. 5285 Port Royal Road, Springfield, VA 22161: National Technical Information Service (NTIS), 2001.
- [24] M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," *IEEE Transactions on Multimedia*, vol. 8, no. 5, pp. 905–917, Oct. 2006, doi: 10.1109/TMM.2006.879919.
- [25] S. H. Kamali, M. Hedayati, R. Shakerian, and M. Rahmani, "A new modified version of Advanced Encryption Standard based algorithm for image encryption," in *ICEIE 2010 - 2010 International Conference on Electronics and Information Engineering, Proceedings*, Aug. 2010, vol. 1, pp. V1-141-V1-145, doi: 10.1109/ICEIE.2010.5559902.
- [26] A. Setyono, D. R. I. M. Setiadi, and Muljono, "Dual encryption techniques for secure image transmission," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, no. 3–2, pp. 41–46, 2018.

BIOGRAPHIES OF AUTHORS






Salim Muhsin Wadi    B.Sc. in Communication Techniques Engineering, Al-Najaf Technical College 2002, Najaf. M.Sc. in Communication Engineering, Electric and Electronic Dept. University of Technology 2005, Baghdad. Ph.D. in Communication Engineering, Electrical, Electronic and System Engineering Dept. The National University of Malaysia (UKM) 2015, K.L. He is currently working as Scientific Division Responsible of engineering technical college, Al-Furat Al-Awsat Technical University. Senior lecturer/Technical College-Najaf, Communications Techniques Engineering Department-Najaf, Iraq. His interested, security of communication system, image processing, IoT health care. He can be contacted at email: coj.sal@atu.edu.iq.






Huda Hussein Abed    Assistant Lecturer at Communication Techniques Engineering Department, Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University. She received Bachelor's and Master's degrees in Communication Techniques from Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Iraq in 2010 and 2019, respectively. Her current research interests include communication security, image processing, steganography, and digital communication. She can be contacted at email: eng.huda2020@atu.edu.iq.



Nada Taher Malik    is a Assistant Lecturer at Technical Institute/Diwaniyah, Al-Furat Al-Awsat Technical University, Iraq. She was born was born in 1979 in Iraq. She obtained her Bachelor's degree in communication Engineering from technical college of Najaf Al-Furat al-Awsat University in 2002, and the M.Sc degree in communication Engineering in 2019 from the from Engineering technical college of Najaf Al-Furat al-Awsat University. Her fields of interest include the security and saving energy of wireless communication networks and their application to energy management systems, control, and optimization. Also, her current field of interest internet of things, Technical 5G. She can be contacted at email: nadamalik@atu.edu.iq.



Dr. Ahmed Taha Abdulsadah    received his Bachelor in electrical engineering from Tikret university. Received his MSC in electrical engineering from university of Baghdad and PhD from electrical and computer department of Michigan state university. He has more than 29 papers published in different valuable journals and conferences. He is currently working as head of communication engineering Dept. of engineering technical college, Al-Furat Al-Awsat Technical University. His interested control theory, advance image processing, security of communication system, robotics manipulation systems. He had been chosen as a reviewer for many journals and conferences. He can be contacted at email: coj.abdulsad@atu.edu.iq.