Bulletin of Electrical Engineering and Informatics
Vol. 9, No. 2, April 2020, pp. 573~581
ISSN: 2302-9285, DOI: 10.11591/eei.v9i2.2068

Analysis review on spatial and transform domain technique in digital steganography

Farah Qasim Ahmed Alyousuf[1], Roshidi Din[2], Alaa Jabbar Qasim[3]
[1]Information Technology Department, Lebanese French University, Erbil, Iraq
[2,3]School of Computing, UUM College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Article Info

Article history:

Received Oct 31, 2019
Revised Dec 28, 2019
Accepted Feb 8, 2020

Keywords:

Digital steganography
Medium-based
Performance metric
Spatial domain
Transform domain

ABSTRACT

This paper presents several techniques used in digital steganography in term of spatial and transform domain. Additionally, it analyses the performance and the metric evaluation of the techniques used in digital steganography based on spatial and transform domain. This paper aims to identify the main mediums of digital steganography, which are image-based, video-based and audio-based, in order to recognize the various techniques used with them. As a result, the primary technique used in the digital medium was LSB technique in the spatial domain, while in the transform domain, the main technique used was differentiated between DTC and DWT. Meanwhile, the common domain utilized in digital steganography was the spatial domain due to its simplicity and high embedding capacity. The future efforts for this paper will be considering the feature based in text steganography.

Corresponding Author:

Farah Qasim Ahmed Alyousuf,
Information Technology Department,
Lebanese French University, Erbil, Iraq.
Email: frhalyousuf@gmail.com

1. INTRODUCTION

Recently, digital steganography has become a crucial tool used in sensitive sectors to protect critical communication when exchanging the vital information, such as in military, medical field or banks. In addition, it is the art that conceals the data inside the signals for any multimedia based (cover medium) such as image, video, or audio-based. Accordingly, it has been recognized among the recent methods and most usable techniques.

There are numerous terminologies employed with digital steganography, such as a secret file, cover medium, secret key, and hiding algorithm [1]. The secret file is the message that needs to be protected, such as text, image, video, or audio. Meanwhile, the cover medium is the carrier that holds the secret file, while secret key works as a tool used with the algorithm to conceal the data. Lastly, hiding algorithm is the method utilized to hide the secret file in the cover medium by using the secret key.

To hide the data in the digital multimedia, there are some techniques should be utilized to enhance the embedding performance. Furthermore, there are five domains used with digital steganography, each domain has some techniques that help to improve the hiding processing. These domains are spatial domain, transform domain, spread spectrum domain, statistical domain, and distortion domain. The main focus of this paper will be on spatial and transform domain due to their commonly used among the researchers.

Spatial domain performs some operations on the pixels to enhance the medium quality [2], while the transform domain deals with hiding the existence of the communicated message [3]. As shown in Figure 1, the techniques used in each domain. Thus, measuring the performance of the techniques needs

some metrics used in digital steganography that helps to evaluate the performance. This paper will analyze the performance, as well as the metric evaluation of digital steganography techniques based on spatial and transform domain.

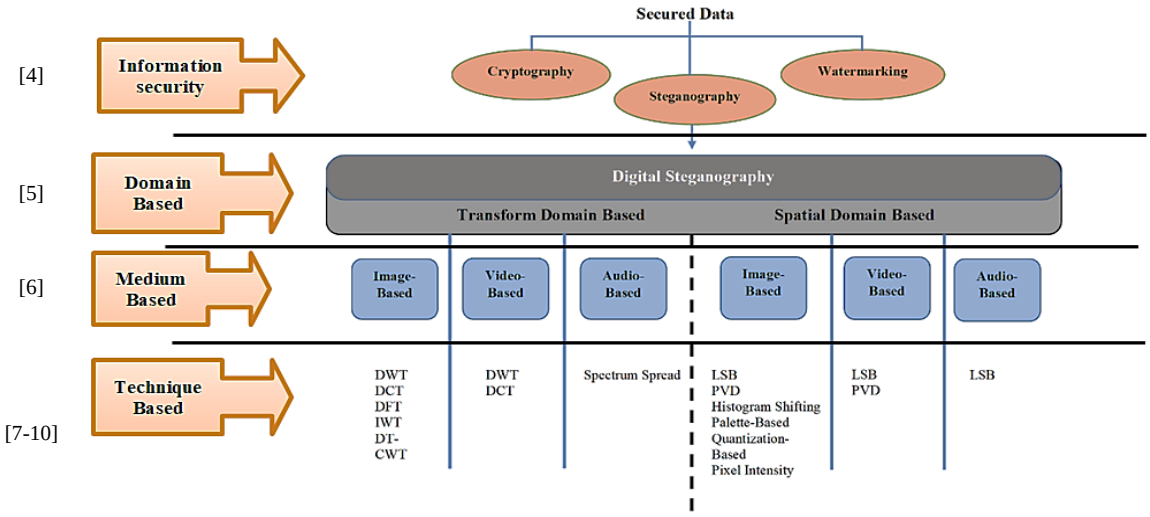

Figure 1. Classification of digital stergasnography

2. PERFORMANCE OF SPATIAL AND TRANSFORM DOMAIN TECHNIQUES OF DIGITAL STEGANOGRAPHY

There are many techniques used in digital steganography that contribute to boosting the performance for the embedding process in digital steganography. This section will study these techniques based on medium-based.

2.1. Image-based

Image steganography is the most common and popular among the digital steganography types, due to its utilization in various application [6, 11-13]. Hence, there are many techniques in spatial and transform domain used with the image to conceal the secret data in the chosen medium. These techniques in term of spatial and transform domain are shown in Table 1.

From Table 1, the spatial domain enhanced the performance for the embedding process in image-based, such as high quality, high security as well the capacity. However, some of the techniques need to be improved in term of the PSNR, MSE and BER. Moreover, the transform domain for image-based also presented in Table 1, the quality and the security have been improved, but some disadvantages need to be improved. For example, the BER is high and complexity in the computation.

2.2. Video-based

Video steganography is a method that hides the secret message inside an ordinary video that no one apart from the authorized people can realize that there is a hidden message inside this clip [36]. Wherefore, to hide the data in a video, it needs to use specific methods and techniques in spatial and transform domain to assist hiding data in a secured and un-noticeable way. Techniques used in video steganography in term of spatial and transform domain are presented in Table 2.

By using the spatial domain technique in video-based, the PSNR will be improved as well the MSE will be decreased as mentioned in Table 2. Therefore, the transform domain for video-based also illustrated in Table 2, and it reaches the highest PSNR and low MSE. However, sometimes the security should be improved to enhance the performance.

Table 1. Review of techniques used in image-based

Spatial Domain			
Techniques used	Advantages	Disadvantages	Review
LSB	Sufficient security and better hiding capacity [14-17].	Low quality due to the limited imperceptibility [15].	Decreasing in processing time and increasing in security.
PVD	Improving in image quality in coloured and grey-scale images [18-21].	Low PSNR and high MSE when using low density objects because it needs observation accuracy [19].	The proposed method has a better imperceptibility because of the construction of the new value.
Histogram Shifting	Hight capacity and secured, andgood quality [13]. Low noise and high capacity [22].		Enhancement in performance due to the good quality that does not affected by the occupied bits.
Palette Based	Better quality and less noise [23].		Better quality due to embedding without any loss.
Quantization Based	Average capacity[24].	High BER because the average of BER is consumed by using the proposed technique.	Increased in image quality when the palette size increased.
Pixel Intensity Modulation	High capacity because each 3×3 window hosts one character instead of four [25].		The good performance in PSNR and MSE enhances the quality.
Transform Domain			
Techniques used	Advantages	Disadvantages	Review
DWT	Better quality and robustness [26-28].	Complex in computations due to the increasing in number of bin histograms [27].	High PSNR and low MSE made the robustness high.
DCT	Better performance in embedding process [29-31]. High capacity and less distortion[31].	Quality not considered by the author [30].	Better security due to high PSNR and good concealing capacity.
DFT	High capacity and quality [32].		High PSNR.
IWT	High capacity and security [33]. High robustness after applying attack and salt & peppers noise [34].		A good performance in embedding and quality because of the good performance in PSNR.
DT-CWT	High capacity because of low patch size results in higher number of individual patches in the cover image [35].	High BER because increasing in number of patches will generate more sub-images and quantization errors.	High SSIM and good PSNR compared to the cover image.

Table 2. Review of techniques used in video-based

Spatial Domain			
Techniques used	Advantages	Disadvantages	Review
LSB	High quality and high imperceptibility [37, 38]. Less distortion [39]. High security [40].		High PSNR and SNR, and low MSE.
PVD	Better hiding performance [41, 42].		High PSNR and low MSE.
Transform Domain			
Techniques used	Advantages	Disadvantages	Review
DWT	High quality [43]. High robustness due to the resistance to the noise attacks [44].	The security should be improved because it is not resisting to all security attacks.	High PSNR and low MSE.
DCT	High security[45, 46].	To secure the communication, the video characteristics should be developed [45].	High PSNR more than 36dB and low bit error rate.

2.3. Audio-based

Audio steganography is the way that hides the secret data, (which could be a text, image, audio, or a video), in an audio medium that make the secret data unnoticeable by the intruders [47]. Hence, to hide the secret data in an audio medium, it needs some algorithms. The main technique used with audio steganography in the spatial domain, is the LSB technique, while in the transform domain spread spectrum technique, as shown in Table 3. Table 3 presents the spatial and the transform domain for audio-based. As presented, by using a spatial domain, the security enhanced with a high SNR. Also, in transform domain low BER is achieved but low SNR in the transform domain.

Table 3. Review of techniques used in audio-based

Spatial Domain			
Techniques used	Advantages	Disadvantages	Review
LSB	High capacity and high secured environment because of using a security key [47, 48]. High security [49].		Secured audio communication due to high SNR value.
Transform Domain			
Techniques used	Advantages	Disadvantages	Review
Spread Spectrum	robust and secured [50].	Slightly high cost and low SNR due to higher noise inherited while implemented spread spectrum.	Different messages size has been implemented with low average BER obtained.

3. PERFORMANCE METRIC ON SPATIAL AND TRANSFORM DOMAIN

Digital steganography has many performance measurements that assist in evaluating the performance in digital steganography. These measurements are Signal-to-Noise-Ratio (SNR), Peak-Signal-to-Noise-Ratio (PSNR), Mean Square Error (MSE), Root MSE (RMSE), Structural Similarity Index Measurement (SSIM), Normalized Correlation (NC), Mean Absolute Error (MAE), and Bit Error Rate (BER). Each measurement has its formula.

As shown in Figure 2, the mathematical formula for each metric is presented to evaluate the performance of the proposed scheme. Whereas, each technique used in medium-based has its performance metric that evaluates the embedding process in order to enhance the quality, security, or the steganography imperceptibility. As shown in Table 4, is the metrics used in each technique for all medium-based. Table 4 illustrates that the techniques used for digital steganography mediums evaluated by using different metrics. However, the standard metric that has been used was PSNR because it shows the robustness of the proposed method, as well as the quality for the stego medium, will be calculated by this metric.

Table 4. Performance metric used on spatial and transform domain based

Spatial Domain Based			
	Image-based	Video-based	Audio-based
LSB	PSNR, MSE, SSIM, NCC, MAE [14-17].	PSNR, MSE, SNR [37-40].	SNR [47-49].
PVD	PSNR, MSE [18-21].	PSNR, MSE [41, 42].	
Histogram Shifting	PSNR, MSE, NCC, BER [13, 22].	-	-
Palette based	PSNR, MSE, NCC [23].	-	-
Quantization based	PSNR, MSE, NCC [24].	-	-
Pixel intensity modulation	PSNR, MSE [25].	-	-
Transform Domain Based			
	Image-based	Video-based	Audio-based
DWT	PSNR, MSE [26-28].	PSNR, MSE [43, 44].	-
DCT	PSNT, MSE, RMSE [29-31].	PSNR, MSE [45, 46].	-
DFT	PSNR [32].	-	-
IWT	PSNR, MSE, NCC, SSIM [33, 34].	-	-
DT-CWT	PSNR, SSIM, BER [35].	-	-
Spread Spectrum	-	-	PSNR, BER, SNR [50].

4. DISCUSSION AND CONCLUSIONS

This paper presents an analysis review on digital steganography techniques based on spatial domain and transform domain. Digital steganography is divided into three main types, which are image, video and audio steganography. Therefore, each type has its technique to secure the data. As shown in Figure 3, the highest technique used was LSB technique due to its simplicity and speed in image-based, while because of its robustness and simplicity in video-based, where the higher efficiency and fast in processing was the reason that used in audio-based. The highest used level that LSB technique reaches was in the year 2016 at 23 times for image-based. Meanwhile, in video-based, LSB technique reaches its highest level in the year 2019 at seven times. Whereas, in the year 2018, audio-based reaches the maximum level at ten times. However, the minimum technique used in digital steganography was PVD in video-based at two times in the year 2016. As for transform domainbased, as displayed in Figure 4 are the techniques used in the transform domain.

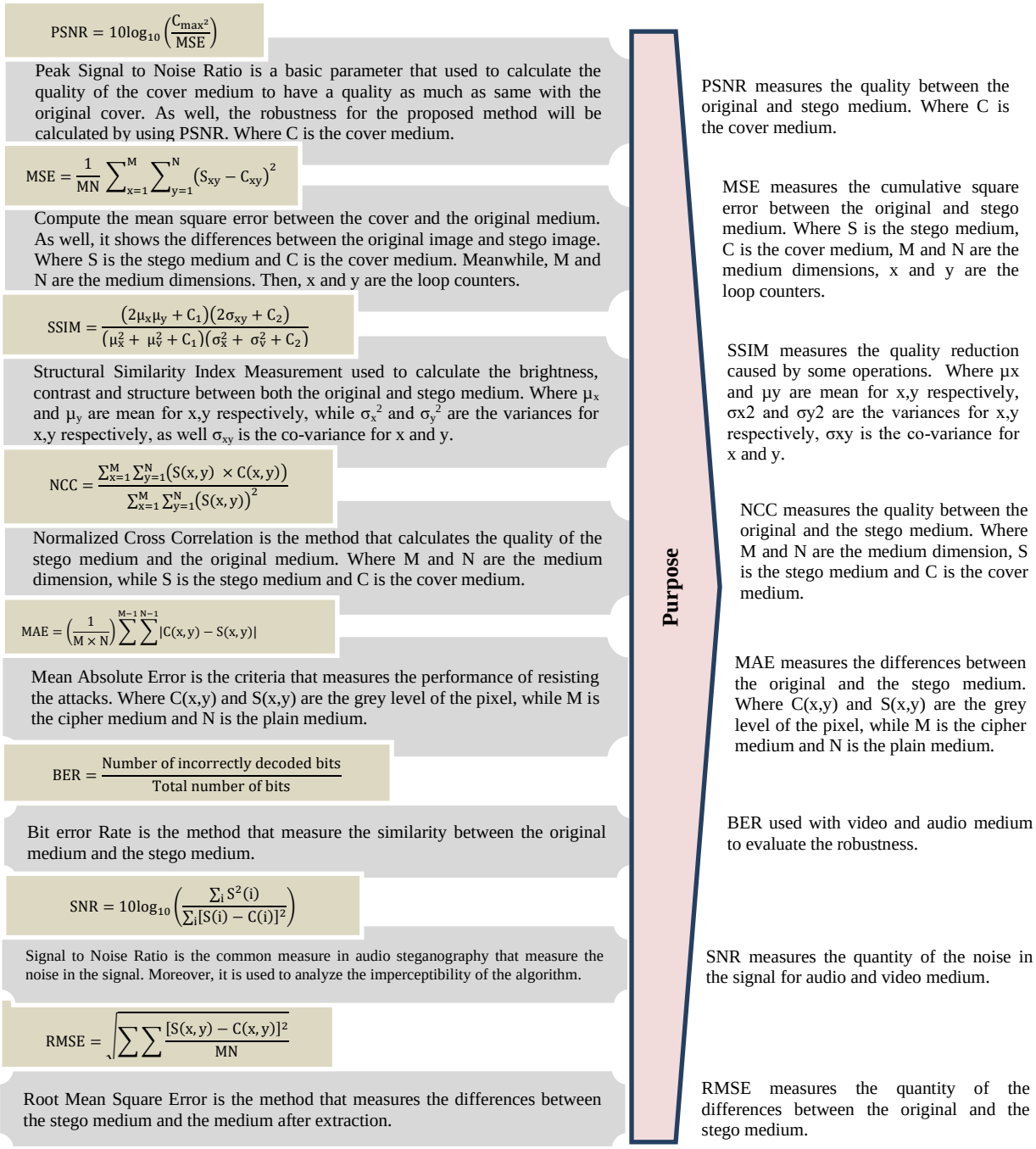

Figure 2. Purpose of using performance metric

Figure 4 presents the most common two techniques used in transform domain were differentiated between DWT and DCT due to their enhanced performance more than DFT and IWT. From the year 2015 to the year 2019, the number of times that these techniques have been used was varying. Accordingly, from the year 2015 to 2017, DWT was the highest in image-based among other techniques and reached its peak in 2017 at ten types of research. Meanwhile, it reduced in the year 2018 and 2019 at 8 and 7 respectively, while DCT increased from 8 types of research on the year 2017 to ten and nine types of research in years 2018 and 2019 respectively. On another hand, the techniques used for video-based were DWT and DCT, as illustrated in Figure 4. The techniques utilizing was fluctuated. The highest was in the year 2018 for DWT at six types of research, and the minimum was for DCT in the year 2015 at one research. Then, spread spectrum was the technique used to enhance the performance in audio-based at one research in the years 2015, 2016 and 2018.

Figure 5 shows the highest usage between spatial and transform domain from the year 2015 to 2020. Because of the better earning outcomes, high proficiency and better security, the spatial domain can take advantages over the transform domain as presented in Figure 5. As well the simplicity of spatial domain and high embedding capacity will make the spatial domain a better tool to enhance the embedding performance.

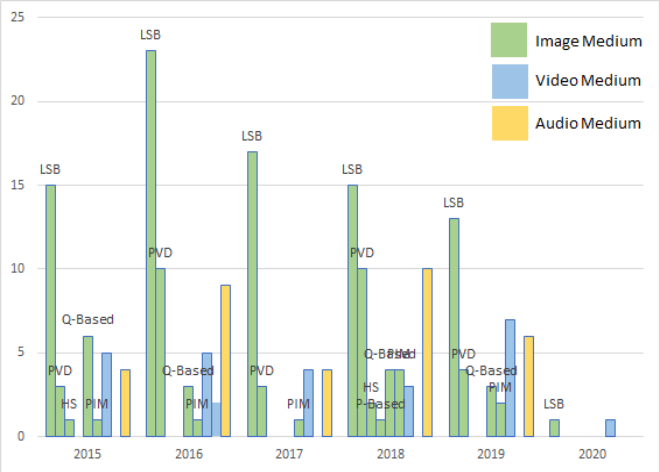

Figure 3. Spatial domain-based techniques

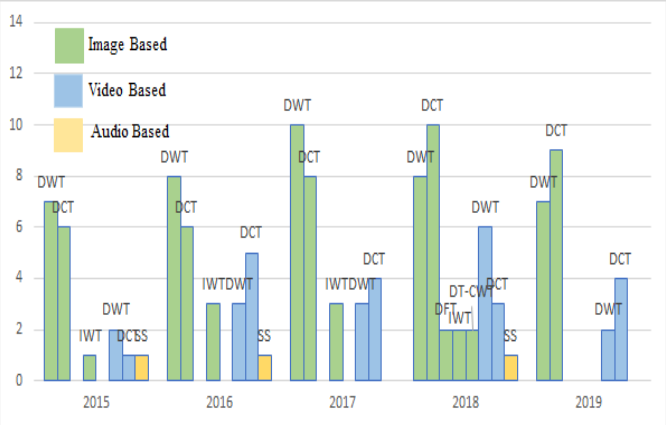

Figure 4. Transform domain-based techniques

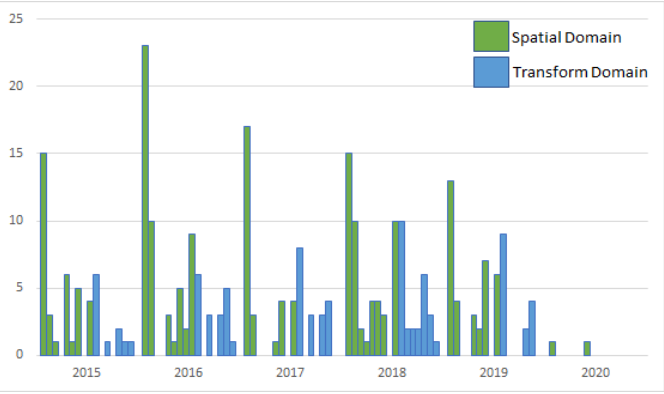

Figure 5. Spatial and transform domain utilizing review

ACKNOWLEDGMENT

We would like to thank Dean, School of Computing, Universiti Utara Malaysia and director of Awang Had Salleh Graduation School (AHSGS) for their moral support to the achievement of this work. A special thanks to Lebanese French University / Kurdistan region-Iraq, for providing a special support to finalize this work.

REFERENCES

[1] R. Din, O. Ghazali, and A. J. Qasim, "Analytical Review on Graphical Formats Used in Image Steganographic Compression," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 5, no. 3, pp. 401-408, 2017.
[2] S. Jeevitha and N. Amutha Prabha, "A comprehensive review on steganographic techniques and implementation," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 17, pp. 4780-4791, 2018.
[3] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *J. Inf. Secur. Appl.*, vol. 34, pp. 142-151, 2017.
[4] R. Din, R. S. Sabri, A. Mustapha, and S. Utama, "A comparative review on data hiding schemes," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 2, pp. 768-774, 2018.
[5] Y. Pu, N. Zhang and H. Wang, "Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things," in *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6368-6383, Aug. 2019.
[6] P. Maniriho and T. Ahmad, "Enhancing the capability of data hiding method based on reduced difference expansion," *Eng. Lett.*, vol. 26, no. 1, pp. 45-55, 2018.
[7] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *Eurasip J. Audio, Speech, Music Process.*, vol. 2012, no. 1, pp. 1-16, 2012.
[8] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, "Video steganography: a comprehensive review," *Multimed. Tools Appl.*, vol. 74, no. 17, pp. 7063-7094, 2015.
[9] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, no. 28, pp. 299-326, 2019.
[10] Disha and K. Saini, "A review on video steganography techniques in spatial domain," *2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017*, vol. 3, pp. 366-371, 2018.
[11] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 518, paper. 052003, 2019.
[12] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Secure Image Steganography Using Dual-Tree Complex Wavelet Transform Block Matching," *Proc. 2nd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2018*, pp. 41-47, 2018.
[13] N. A. Amita, A. Kaur, and M. Kumar, "Reversible data hiding in absolute moment block truncation coding compressed images using adaptive multilevel histogram shifting technique," *Int. J. Inf. Comput. Secur.*, vol. 10, no. 2/3, paper. 261, 2018.
[14] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, "Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 17799-17823, Jul. 2019.
[15] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimed. Tools Appl.*, vol. 75, no. 22, pp. 14867-14893, 2016.
[16] M. Soleimanpour-Moghadam and H. Nezamabadi-Pour, "The pair-wise LSB matching steganography with a discrete quantum behaved Gravitational Search Algorithm," *J. Intell. Fuzzy Syst.*, vol. 30, no. 3, pp. 1547-1556, 2016.
[17] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in image hiding using developed LSB and random method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 4, pp. 2091-2097, 2018.
[18] S. S. Newaj Bhuiyan, N. A. Malek, O. O. Khalifa, and F. D. Abdul Rahman, "An Improved Image Steganography Algorithm Based on PVD," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 2, paper. 569, May 2018.
[19] B. Santoso, "Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm," *J. Phys. Conf. Ser.*, vol. 1175, paper. 012057, Mar. 2019.
[20] C. Lee, J. Shen, and T.-Y. Ou-Yang, "A High Payload Edge Detection-Based Image Steganography Robust to RS-Attack by Using LSB Substitution and Pixel Value Differencing," Springer International Publishing, vol. 82, pp. 272-279, 2019.
[21] S. Prasad and A. K. Pal, "Logistic Map-Based Image Steganography Scheme Using Combined LSB and PVD for Security Enhancement," *Springer Singapore*, vol. 755, pp. 203-214, 2019.
[22] M. R. Jeppiaar, "A Prediction Based Reversible Image Steganographic Algorithm for JPEG Images," *J. Appl. Secur. Res.*, vol. 10, no. 3, pp. 362-374, 2015.
[23] H. N. Patel, D. R. Khant, and D. Prajapati, "Design of a color palette based image steganography algorithm for fractal images," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018, pp. 2584-2589, 2018.
[24] Y. C. Hu, C. F. Lee, and Y. H. Liu, "Reversible image steganography for color image quantization based on lossless index coding," *Adv. Intell. Syst. Comput.*, vol. 733, pp. 185-195, 2018.

[25] S. Das, S. Sharma, S. Bakshi, and I. Mukherjee, "A Framework for Pixel Intensity Modulation Based Image Steganography," *Adv. Intell. Syst. Comput.*, vol. 563, pp. 3-14, 2018.
[26] A. Nevriyanto, S. Sutarno, S. D. Siswanti, and E. Erwin, "Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio," *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, vol. 17, pp. 147-152, 2019.
[27] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model," *Multimed. Tools Appl.*, 2019.
[28] G. V. K. Murugan and R. Uthandipalayam Subramaniyam, "Performance analysis of image steganography using wavelet transform for safe and secured transaction," *Multimed. Tools Appl.*, 2019.
[29] R. Patidar, B. Prajapat, and A. Sakreja, "Image Steganography Based on Random Pixel Addition and Discrete Cosine Transform (DCT)," *Springer Singapore*,vol. 870, pp. 453-458, 2019.
[30] M. K. Shyla and K. B. Shiva Kumar, "Novel Color Image Data Hiding Technique Based on DCT and Compressed Sensing Algorithm," *Springer Singapore*, vol. 545, pp. 1151-1157, 2019.
[31] S. A. El Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput. Electr. Eng.*, vol. 70, pp. 380-399, 2018.
[32] O. Evsutin, A. Kokurina, R. Meshcheryakov, and O. Shumskaya, "The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation,"*Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28567-28599, 2018.
[33] E. Emad, A. Safey, A. Refaat, E. Sayed, Z. Osama, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *J. Syst. Eng. Electron.*, vol. 29, no. 3, pp. 639-649, 2018.
[34] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 9971-9989, Apr. 2019.
[35] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform," *Springer International Publishing*, vol. 10956, pp. 544-550, 2018
[36] B. Chandel and S. Jain, "Video Steganography : A Survey," vol. 18, no. 1, pp. 11-17, 2016.
[37] N. Singh and J. Bhardwaj, "Randomized LSB based video steganography for hiding acoustic data using XOR Technique," *2017 Int. Conf. Comput. Electr. Commun. Eng. ICCECE 2017*, pp. 1-7, 2018.
[38] S. Abed, M. Al-Mutairi, A. Al-Watyan, O. Al-Mutairi, W. AlEnizy, and A. Al-Noori, "An Automated Security Approach of Video Steganography-Based LSB Using FPGA Implementation," *J. Circuits, Syst. Comput.*, vol. 28, no. 5, paper. 1950083, 2019.
[39] N. Singh, "XOR Encryption Techniques of Video Steganography: A Comparative Analysis," Springer International Publishing, pp. 203-214, 2020.
[40] Z. S. Younus and G. T. Younus, "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data," *J. Intell. Syst.*, 2019.
[41] S. Priya and P. P. Amritha, "Information Hiding in H.264, H.265, and MJPEG," in *Advances in Intelligent Systems and Computing*, vol. 397, pp. 479-487, 2016.
[42] T. F. Idbeaa, S. A. Samad, and H. Husain, "An adaptive compressed video steganography based on pixel-value differencing schemes," *Int. Conf. Adv. Technol. Commun*, vol. 2016, pp. 50-55, 2016.
[43] S. K. Yadav and R. K. Bhogal, "A video steganography in spatial, discrete wavelet transform and integer wavelet domain," *Proc-2nd Int. Conf. Intell. Circuits Syst. ICICS 2018*, pp. 265-270, 2018.
[44] M. Dalal and M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," *Multimed. Tools Appl.*, vol. 78, no. 5, pp. 5769-5789, 2019.
[45] Y. Zhang, M. Zhang, X. Yang, D. Guo, and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC," *Tsinghua Sci. Technol.*, vol. 22, no. 2, pp. 198-209, 2017.
[46] M. Suresh and I. Shatheesh Sam, "High Secure Video Steganography Based on Shuffling of Data on Least Significant DCT Coefficients," in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, no. Iciccs, pp. 877-882, 2018.
[47] J. Mohajon, Z. Ahammed, and K. Hasan Talukder, "An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key," in *2018 21st International Conference of Computer and Information Technology (ICCIT)*, pp. 1-6, 2018.
[48] A. A. Hosny, W. A. Murtada, and M. I. *Youssef, "Improving LSB audio steganography using simulated annealing for satellite telemetry," ICENCO 2018 - 14th Int. Comput. Eng. Conf. Secur. Smart Soc., pp. 11-16, 2019.*
[49] *S. M. H. Alwahbani and H. T.* I. Elshoush, "Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad," vol. 15, pp. 755-768, 2018.
[50] A. Anjana Krishnan, C. Satheesh Chandran, S. Kamal, and M. H. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," *2nd Int. Conf. Circuits, Control. Commun. CCUBE 2017-Proc.*, pp. 109-114, 2018.

BIOGRAPHIES OF AUTHORS

Farah Qasim Ahmed Alyousuf is an assistant lecturer in Lebanese French University in department of information technology/Kurdistan Region-Erbil-Iraq. PhD candidate in Information Technology-School of Computing (SOC)-Awang Had Salleh Graduate School (AHSGS)-Universiti Utara Malaysia/Sintok-Kedah-Malaysia since January 2019.

Assoc. Prof. Dr. Roshidi Din received his Bachelor of Information Technology and Master of Science in Information Technology degrees from Universiti Utara Malaysia (UUM) in 1996 and 1999 respectively. He later completed his Ph.D from Universiti Sains Malaysia (USM) in 2015. Heis currently a Senior Lecturer at the School of Computing, UUM. His current research interests are more on the application of Discrete Mathematics in various areas especially in Information Security, Steganography and Steganalysis, and Natural Language Steganology.

Alaa Jabbar Qasim received the B.S.in Computer Science/ information system Department at Al Rafidain University College in (2000)-Iraq; he is doing M.Sc. (Computer Science) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur, Andra Pradeesh, India. Ph.D. candidate in Information Technology-School of Computing (SOC)-Awang Had Salih Graduate School (AHSGS)–at the University Utara Malaysia (UUM)–Malaysia, He is interested in the following Fields (Steganography, Cryptology, Information Security and Information System).