Review on secured data capabilities of cryptography, steganography, and watermarking domain

Farah Qasim Ahmed Al-Yousuf, Roshidi Din
School of Computing, UUM College of Arts and Sciences, Universiti Utara Malaysia, Malaysia

Article Info

Article history:

Received Jun 14, 2019
Revised Aug 15, 2019
Accepted Aug 29, 2019

Keywords:

Algorithm used
Secured data
Technique used

ABSTRACT

Due to the increment of using Internet to transfer the critical and secret data, many studies interested in secured data and investigated many ways to secure the transferred information. This paper presents a review study on the field that used in a secured data domain. The main objective of this study is explore the capabilities of secured data that used widely by researchers. Furthermore, the benefits and the drawbacks for each of secured data domain are also studied. This paper concludes that cryptography techniques could be utilized with steganography and watermarking in secured data domain to enhance the security mechanisms.

Corresponding Author:

Roshidi Din,
School of Computing,
UUM College of Arts and Sciences,
Universiti Utara Malaysia,
06010 Sintok, Kedah, Malaysia.
Email: roshidi@uum.edu.my

1. INTRODUCTION

The improvement of the digital communication has become an essential part of life, for example, in work or school environment and even in daily uses such as e-mail correspondence and instant messaging. With the development of technology on storing and exchanging data in different ways over the network from one location to another, the security of these data, namely secured data, try to protect the information from threats or a barrier resists. Securing the information should be accomplished by using a protection techniques that make the data secured among the authorized parties [1]. There are three fields used widely in the domain of secured data known as cryptography, steganography, and watermarking. Thus, this paper will try to review the secured data capabilities on cryptography, steganography, and watermarking domain.

Cryptography is a technique that secures the transferred data, which concerns about confidentiality, integrity, and availability of the information [2]. Besides that, steganography is the technique that conceal the data into the same or in a different form to create a cover that holds the secret data called the cover medium which is to protect them from spying attacks [3]. So, it is a technique to create a hidden communication [4]. Meanwhile, watermarking is used to classify and shield the content of the copyrighted media by coding the data into the main content [5]. Figure 1-3 shows the process for cryptography (Figure 1.), steganography (Figure 2.), and watermarking (Figure 3.) through their security processes.

There are some purposes for cryptography, steganography, and watermarking have been identified where each of field has its own strength and weaknesses points. Table 1 has present a general view on the secured data fields in term of purpose, strength, weakness and used-based.

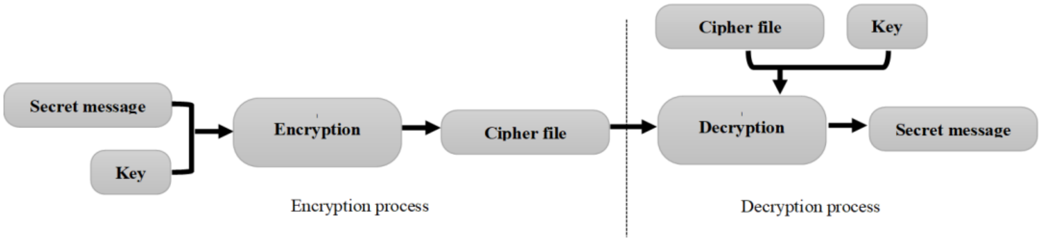

Figure 1. Secured data processes: Cryptography process

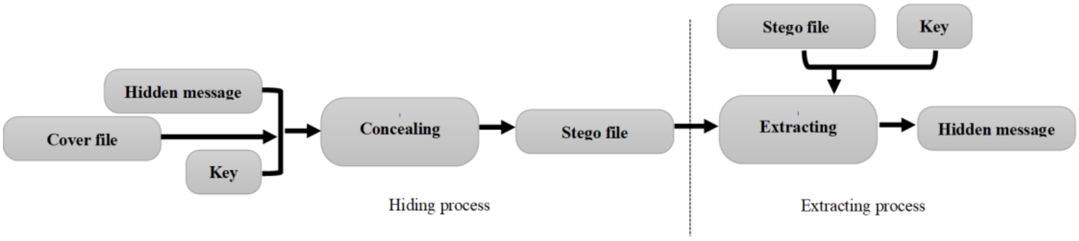

Figure 2. Secured data processes: Steganography process

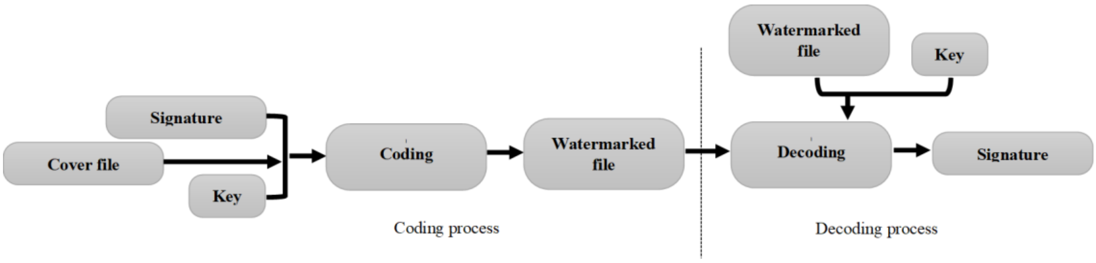

Figure 3. Secured data processes: Watermarking process

Table 1. General Capabilities for Secured Data

	Cryptography	Steganography	Watermarking
Purpose	Provide information security and transfer them through insecure communication [6] Protect the confidentiality, integrity, and non-repudiation (availability) of the data [7]	It is a private communication and protecting the data from alteration as an authentication purpose [8]	Copyright protection, broadcast monitoring, video authentication, and ID card security [9]
Strength	Secure the data as well as protect the privacy by using cryptography with another technique [10], for example, steganography [11] Provide a secure process of authorization and better security functionalities [12]	Provide end-to-end data confidentiality for sensitive information and robust authenticity [13]	Enhance imperceptibility and computational complexity for the digital media [14]
Weakness	Complex key management, especially in public key infrastructure [15]	By using only the text steganography, the scheme will be more natural to interrupt or deciphered [10]	Using a universal logo without encryption in the embedding algorithm [16]
Used-based	Algorithm-based	Domain-based	Application-based

2. REVIEW OF TECHNIQUES AND ALGORITHMS IN SECURED DATA

This section mentions the current techniques and algorithms for secured data domain. There are different techniques used to increase the capabilities for each field in secured data. Table 2 illustrates the techniques and algorithms used by researchers in term of the domain used in secured data.

Table 2. A Review of Techniques/Algorithms in Secured Data

Domain			Techniques/Algorithms
Cryptography	Image		Binary image encryption algorithm [17], Elliptic curve random generator and advanced encryption system [18], Entropy accumulation [19], and Rapid hyper-chaotic system [20]
	Coloured image		Gyrator transform [21] and Colour image encryption scheme and multiple piece-wise linear chaotic map [22]
	Cloud Environment		Searchable encryption [23], Ciphertext-policy attribute-based encryption [24], and Attribute based encryption, distributed hash table network, and identity based timed-release encryption [25]
	Communication, Protocol, Network, Mobile Wireless Networks		Cognitive cryptography [26] Identity-based public key cryptography technique [27]
	Audio		Original speech encryption method [28]
	Proxy		Digital right management [29]
	Storage		Commutative re-encryption techniques [30]
Steganography	Image		Adaptive neural networks with an adaptive [genetic algorithm] [31], Uniform embedding revisited distortion [32], Image steganography algorithm and compressive sensing with sub-sampling [33], Absolute moment block truncation coding [34], Domain separation technique [35], Least significant bit [36], Adaptive steganography algorithm based on Gabor filters and anisotropic diffusion [37], Colour pixel vectors [38], Optimal asymmetric encryption padding and information dispersal algorithms [39] and Optimized efficient methodology [40]
	Wireless Psychological Signal		Discrete wavelet transform [39]
	Synthetic Gene Circuits		Encryption then steganography [41]
Watermarking	Digital-based	Image-based	Non-integer PE embedding approach [42] Multiple colour-image fusion and watermarking [43] Algorithm for invisible grayscale logo watermarking [44]
		Video-based	Self-embedding fragile image watermarking [45] Sparse domain-based information hiding [46] Medical image watermarking technique [47].
		Audio-based	Watermarking algorithm based on non-subsampled contourlet transform [48] Non-blind digital watermarking technique [49] Fragile blind quad watermarking [50]
		Hybrid-based	Blind image watermarking based on redundant discrete wavelet transform [51] High-efficiency video coding [52] Discrete cosine transform and singular value decomposition [53] Hybrid and blind watermarking scheme [54]

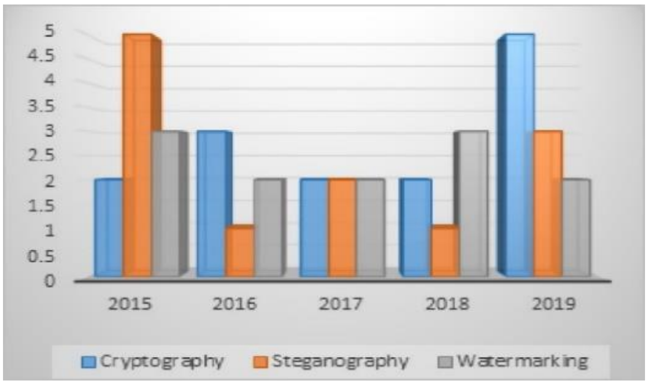

Figure 4. Techniques used on secured data within last five years

Besides that, Figure 4 has illustrated the number of the techniques and algorithms used by the researchers within last five years. In year 2015, cryptography had a minimum amount of applied techniques at two techniques/algorithms, while in same year steganography had the maximum at five techniques/algorithms. In the year 2016, the used of cryptography has been increased to three techniques/algorithms, while remaining unchanged in the year 2017 and the year 2018 at two techniques/algorithms. There was a sudden increase usage of cryptography in the year 2019 up to five techniques/algorithms, which makes it a standard secured data that used in data security.

3. ADVANTAGES AND DISADVANTAGES OF SECURED DATA

Most of the researchers in their studies have advantages of their proposed techniques. However, not all the proposed techniques solved all the issues. Table 3 has illustrated the benefits and drawbacks for the proposed scheme of secured data in the last five years from year 2015 to year 2019. As shown in Table 3, the benefits and drawbacks of the techniques on cryptography, steganography, and watermarking.

Table 3. Benefits and Drawbacks of Techniques Used on Secured Data

Domain	Methods	Benefits	Drawbacks
Cryptography	AES, RSA, and MD5	More secure when AES algorithm used alone [55]	High running time
	Cloud Environment	An efficient method to protect the data, low running time, and increased throughput [29]	
		More secured and accurate against attacks [25]	
	Coloured Image	Efficient for the colored image, strong resistance, strong computational load, time-saving [22]	Inefficient with multiple colour image
Steganography	Image	Less distortion in the sense of color correlation, equipped with the extended CMD strategy [38]	Cannot be directly applied to JPEG image with YCbCr images
		Proper embedding in the noisy region improved in security [37]	The performance should be improved; not enough edge information of the image is returned
		Seven layers protection can be used to fight against statistical visual, structural and attacks [31]	
Watermarking	Digital Image	Adding Arnold scrambling security scheme before embedding [56]	Less payload capacity, poor robustness.
		Robust against attacks [57]	False-positive error, and less fidelity
		Eficient, secure, safe, and applicable for blind and fragile applications [50]	The watermark may be destroyed by image processing because of the fragility

4. CONCLUSION

There are some evolutions in techniques that enhanced the features for each field in secured data. This paper introduced a comparison study between cryptography, steganography, and watermarking techniques that are widely used to ensure information is secured. Thus, secured data techniques try to offer numerous solutions for issues faced by researchers. In summary, cryptography can be used to improve security and prevent attackers and unauthorized persons from estimating the secret message. Hence, this paper found that cryptography techniques could be used to increase the security for other fields on the secured data domain. Consequently, it is expected that future efforts will provide a higher level of security by utilizing the use of integrated between cryptography and steganography techniques.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] R. Bhandari and V. B. Kirubanand, “Enhanced encryption technique for secure iot data transmission,” vol. 9, no. 5, pp. 3732–3738, 2019.

[2] S. Pramanik, R. P. Singh, and R. Ghosh, “A new encrypted method in image steganography,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 3, p. 1412, 2019.

[3] R. Din, M. Mahmuddin, and A. J. Qasim, “Review on Steganography Methods in Multi-Media Domain,” *Int. J. Eng. Technol.*, vol. 8, no. 1.7, pp. 288–292, 2019.

[4] F. Z. Mansor, A. Ismail, R. Din, A. Mustapha, and N. A. Samsudin, “Substitution-based linguistic steganography based on antonyms,” vol. 16, no. 1, pp. 530–538, 2019.

[5] P. S. N, C. S. S, and M. C. S, “Performance analysis of DCT and successive division based digital image watermarking scheme,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 15, no. 2, pp. 804–813, 2019.

[6] R. Chałupnik, M. Kędziora, P. Jóźwiak, and I. Jóźwiak, “Correspondent Sensitive Encryption Standard (CSES) Algorithm in Insecure Communication Channel,” in *IEEE Systems Journal*, vol. 12, no. 4, 2020, pp. 90–98.

[7] R. Bhanot and R. Hans, “A review and comparative analysis of various encryption algorithms,” *Int. J. Secur. its Appl.*, vol. 9, no. 4, pp. 289–306, 2015.

[8] R. Din, R. Bakar, S. Utama, J. Jasmis, and S. J. Elias, “The evaluation performance of letter-based technique on text steganography system,” *Bull. Electr. Eng. Informatics*, vol. 8, no. 1, pp. 291–297, 2019.

[9] K. M. Mabrouk, N. A. Semary, and H. Abdul-Kader, “Fragile Watermarking Techniques for 3D Model Authentication: Review,” vol. 723, Springer International Publishing, 2020, pp. 669–679.

[10] C. Rangaswamaiah, Y. Bai, and Y. Choi, “Multilevel Data Concealing Technique Using Steganography and Visual Cryptography,” vol. 70, pp. 739–758, 2020.

[11] N. Singh, “XOR Encryption Techniques of Video Steganography: A Comparative Analysis,” Springer International Publishing, 2020, pp. 203–214.

[12] Y. H. Park, K. S. Park, and Y. H. Park, “Secure user authentication scheme with novel server mutual verification for multiserver environments,” *Int. J. Commun. Syst.*, vol. 32, no. 7, pp. 1–17, 2019.

[13] A. Abuadbba and I. Khalil, “Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid readings,” *Inf. Syst.*, vol. 53, pp. 224–236, 2015.

[14] A. Soualmi, A. Alti, L. Laouamer, and M. Benyoucef, “A Blind Fragile Based Medical Image Authentication Using Schur Decomposition,” vol. 723, Springer International Publishing, 2020, pp. 623–632.

[15] H. Li, Q. Huang, J. Shen, G. Yang, and W. Susilo, “Designated-server identity-based authenticated encryption with keyword search for encrypted emails,” *Inf. Sci. (Ny).*, vol. 481, pp. 330–343, 2019.

[16] M. Jafari Barani, M. Yousefi Valandar, and P. Ayubi, “A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3D quantum map,” *Optik (Stuttg).*, vol. 187, no. November 2018, pp. 205–222, 2019.

[17] A. Houas, Z. Mokhtari, K. E. Melkemi, and A. Boussaad, “A novel binary image encryption algorithm based on diffuse representation,” *Eng. Sci. Technol. an Int. J.*, vol. 19, no. 4, pp. 1887–1894, 2016.

[18] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, “An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System,” *Signal Processing*, vol. 141, no. June, pp. 217–227, 2017.

[19] K. Yi, Z. Leihong, and Z. Dawei, “Optical encryption based on ghost imaging and public key cryptography,” *Opt. Lasers Eng.*, vol. 111, no. June, pp. 58–64, 2018.

[20] H. Bouslehi and H. Seddik, “Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation,” *Multimed. Tools Appl.*, vol. 77, no. 23, pp. 30841–30863, 2018.

[21] L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, “An asymmetric color image encryption method by using deduced gyrator transform,” *Opt. Lasers Eng.*, vol. 89, pp. 72–79, 2015.

[22] K. A. Kumar Patro and B. Acharya, “An efficient colour image encryption scheme based on 1-D chaotic maps,” *J. Inf. Secur. Appl.*, vol. 46, pp. 23–41, 2019.

[23] H. Jiang, X. Li, and Q. Xu, “An Improvement to a Multi-Client Searchable Encryption Scheme for Boolean Queries,” *J. Med. Syst.*, vol. 40, no. 12, 2016.

[24] Y. Liu, L., Lai, J., Deng, R. H., & Li, “Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment,” *Secur. Commun. NETWORKS*, vol. 9, no. 22, pp. 5968–5974, 2016.

[25] S. Namasudra, “An improved attribute-based encryption technique towards the data security in cloud computing,” *Concurr. Comput.* , vol. 31, no. 3, pp. 1–15, 2019.

[26] M. R. Ogiela, “Cognitive solutions for security and cryptography,” *Cogn. Syst. Res.*, vol. 55, no. February, pp. 258–261, 2019.

[27] D. He, S. Zeadally, L. Wu, and H. Wang, “Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography,” *Comput. Networks*, vol. 128, pp. 154–163, 2017.

[28] S. Renza, D., & Mendoza, “High-uncertainty audio signal encryption based on the Collatz conjecture,” *J. Inf. Secur. Appl.*, vol. 46, pp. 62–69, 2019.

[29] N. Agarwal, A. Rana, and J. P. Pandey, “Guarded dual authentication based DRM with resurgence dynamic encryption techniques,” *Enterp. Inf. Syst.*, vol. 13, no. 3, pp. 257–280, 2019.

[30] N. Islam, K. M. Rokibul Alam, and S. S. Rahman, "Commutative Re-encryption Techniques: Significance and Analysis," *Inf. Secur. J.*, vol. 24, no. 4–6, pp. 185–193, 2015.

[31] N. N. El-Emam and M. Al-Diabat, "A novel algorithm for colour image steganography using a new intelligent technique based on three phases," *Appl. Soft Comput. J.*, vol. 37, pp. 830–846, 2015.

[32] L. Guo, J. Ni, W. Su, C. Tang, and Y. Q. Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2669–2680, 2015.

[33] J. S. Pan, W. Li, C. S. Yang, and L. J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimed. Tools Appl.*, vol. 74, no. 21, pp. 9191–9205, 2015.

[34] D. Ou and W. Sun, "High payload image steganography with minimum distortion based on absolute moment block truncation coding," *Multimed. Tools Appl.*, vol. 74, no. 21, pp. 9117–9139, 2015.

[35] S. Karri and A. Sur, "Steganographic algorithm based on randomization of DCT kernel," *Multimed. Tools Appl.*, vol. 74, no. 21, pp. 9207–9230, 2015.

[36] A. K. Sahu and G. Swain, "A review on LSB substitution and PVD based image steganography techniques," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 2, no. 3, pp. 712–719, 2016.

[37] Y. Sun, G. Tang, X. Xu, and M. Jiang, "Steganography using Gabor filter and anisotropic diffusion," *Multimed. Tools Appl.*, vol. 77, no. 15, pp. 20247–20265, 2018.

[38] X. Qin, B. Li, S. Tan, and J. Zeng, "A novel steganography for spatial color images based on pixel vector cost," *IEEE Access*, vol. 7, pp. 8834–8846, 2019.

[39] N. Sahu, D. Peng, and H. Sharif, "Unequal steganography with unequal error protection for wireless physiological signal transmission," *IEEE Int. Conf. Commun.*, 2017.

[40] A. Gutub and M. Al-Ghamdi, *Image Based Steganography to Facilitate Improving Counting-Based Secret Sharing*, vol. 10, no. 1. 3D Display Research Center, 2019.

[41] O. Purcell, J. Wang, P. Siuti, and T. K. Lu, "Encryption and steganography of synthetic gene circuits," *Nat. Commun.*, vol. 9, no. 1, 2018.

[42] S. Xiang and Y. Wang, "Non-integer expansion embedding techniques for reversible image watermarking," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, 2015.

[43] M. R. Abuturab, "Multiple color-image fusion and watermarking based on optical interference and wavelet transform," *Opt. Lasers Eng.*, vol. 89, pp. 47–58, 2015.

[44] M. Andalibi and D. M. Chandler, "Digital Image Watermarking via Adaptive Logo Texturization," *IEEE Trans. Image Process.*, vol. 24, no. 12, pp. 5060–5073, 2015.

[45] C. Qin, H. Wang, X. Zhang, and X. Sun, "Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode," *Inf. Sci. (Ny).*, vol. 373, no. 516, pp. 233–250, 2016.

[46] C. Liu, Q. Chen, H. Liang, and H. Li, "Digital Watermarking Processing Technique Based on Overcomplete Dictionary," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 30, no. 10, p. 1658002, 2016.

[47] A. Ustubioglu and G. Ulutas, "A New Medical Image Watermarking Technique with Finer Tamper Localization," *J. Digit. Imaging*, vol. 30, no. 6, pp. 665–680, 2017.

[48] K. L. Hua, B. R. Dai, K. Srinivasan, Y. H. Hsu, and V. Sharma, "A hybrid NSCT domain image watermarking scheme," *Eurasip J. Image Video Process.*, vol. 2017, no. 1, pp. 1–17, 2017.

[49] S. Shaukat, J. Tariq, S. Shabieh, F. Muhammad, and U. Khan, "A new technique of frequency domain watermarking based on a local ring," *Wirel. Networks*, 2017.

[50] B. Bolourian Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, "TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA," *Inf. Sci. (Ny).*, vol. 486, pp. 204–230, 2019.

[51] M. H. Vali, A. Aghagolzadeh, and Y. Baleghi, "Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition," *Expert Syst. Appl.*, vol. 114, pp. 296–312, 2018.

[52] C. Wang, R. Shan, and X. Zhou, "Anti-HEVC Recompression Video Watermarking Algorithm Based on the All Phase Biorthogonal Transform and SVD," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 35, no. sup1, pp. 42–58, 2018.

[53] A. Kanhe and A. Gnanasekaran, "Robust image-in-audio watermarking technique based on DCT-SVD transform," *Eurasip J. Audio, Speech, Music Process.*, vol. 2018, no. 1, pp. 1–12, 2018.

[54] D. Dhaou, S. Ben Jabra, and E. Zagrouba, "A Review on Anaglyph 3D Image and Video Watermarking," *3D Res.*, vol. 10, no. 2, pp. 1–12, 2019.

[55] M. Harini, K. Pushpa Gowri, C. Pavithra, and M. Pradhiba Selvarani, "A novel security mechanism using hybrid cryptography algorithms," *Proc. - 2017 IEEE Int. Conf. Electr. Instrum. Commun. Eng. ICEICE 2017*, vol. 2017-Decem, pp. 1–4, 2017.

[56] R. Thanki, A. Kothari, and D. Trivedi, “Hybrid and blind watermarking scheme in DCuT – RDWT domain,” *J. Inf. Secur. Appl.*, vol. 46, pp. 231–249, 2019.
[57] D. G. Savakar and A. Ghuli, “Robust Invisible Digital Image Watermarking Using Hybrid Scheme,” *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 3995–4008, 2019.

BIOGRAPHIES OF AUTHORS

Farah Qasim Ahmed Alyousuf is an assistant lecturer in Lebanese Frenh University in department of information technology / Kudistan Region - Erbil - Iraq. PhD candidate in Information Technology – School of Computing (SOC) – Awang Had Salih Graduate School (AHSGS) – Universiti Utara Malaysia / Sintok - Kedah - Malaysia

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. He is 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.