Research on Coverless Image Steganography

Kurnia Anggriani[1,2], Nan-I Wu[3], and Min-Shiang Hwang[1,4]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science & Information Engineering, Asia University[1]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taichung, Taiwan, ROC
Faculty of Engineering, University of Bengkulu, Indonesia[2]
Department of Digital Multimedia, Lee-Ming Institute of Technology[3]
No.2-2, Lijhuan Rd., Taishan Township, Taipei County 243, Taiwan, ROC
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[4]
Email: mshwang@asia.edu.tw

(Received May 12, 2022; Revised and Accepted Dec. 8, 2022; First Online Dec. 10, 2022)

Abstract

In recent years, Coverless Image Steganography (CIS) has become an essential research topic for many scholars. This research topic was initiated in 2015 under steganography without embedding. Accordingly, CIS was presented to withstand the inadequacies of the general steganography method against the risks of steganalysis tools. This is because information concealed in CIS has no modification left on the stego image. Conversely, CIS performs a mapping operation to select a stego image containing secret information. This paper attempts to examine the development of CIS over the past five years, summarizing and analyzing the benefits and challenges of the current methods used by each survey paper. Moreover, we present the experimental results in tables and graphs to provide a precise performance comparison. This is done to outline future research requirements and opportunities in the CIS research topic. For example, in the future, developing a CIS method that is resistant to steganalysis tools, has a large hiding capacity, and can be used in real-time applications would be ideal.

Keywords: Coverless Data Hiding; Coverless Image Steganography; Mapping Operation

1 Introduction

In an internet-based world, the necessity for secure communication routes is unavoidable. One of the solutions to achieve safe communication is to use data hiding, commonly known as steganography. Steganography is described as a secret mechanism that conceals confidential data in other mediums while causing undetectable alterations in human perception [21, 26, 27]. Aside from the benefits of data hiding in establishing a safe environment, one of the most significant obstacles in the traditional steganographic approach is the risk of steganalysis tools. It is due to the stego image's alteration traces [16, 28].

In the traditional steganographic approach, image modification can occur in the spatial, transform, and compressed domains. In the spatial domain, the modification is performed directly in the pixel value of the image [2]. The standard method of spatial domain data hiding is utilizing the least significant bit (LSB) [10, 23–25, 29] and pixel value differencing (PVD) [14, 22]. As a result, spatial domain data hiding achieved high hiding capacity and, as a trade-off, was very vulnerable to steganalysis attacks [8]. In the transform domain and compressed domain data hiding, the modification deals with the transform coefficients [3, 20, 31] and compressed code [9, 11] of the images, respectively. As a result, transform domain, and compressed domain data hiding perform more robust against steganalysis attacks. However, the traditional steganographic approach has become increasingly susceptible and insufficiently safe due to the rapid development of steganographic tools in the previous year [6, 19]. Especially with the potential of image processing attacks like Additive Gaussian White Noise, Salt & Pepper noise, low-pass filtering, and JPEG compression. Because of the difficulties above, traditional data hiding must continue to evolve to improve the robustness of the data hiding method.

To address the challenges mentioned above, in 2015, Zhou *et al.* [33] proposed a concept of steganography without embedding, often known as coverless data hiding. Instead of embedding secret information by modifying the images' attributes, this technique matches the image to the secret information. The mapping operation's unique key is a hash sequence comprising secret information and an image. The picture will automatically incorporate the secret information when they have the same hash sequence. In the last five years, abundant methods have been introduced in the CIS. As a result, CIS can be divided into image-mapping-based CIS [4, 13, 30, 32, 34] and image-generation-based CIS [1, 5, 7, 12, 15, 17, 18]. In the image-mapping-based CIS, the main character is the mapping operation between hashing sequences of secret information to find the most similar image in the image dataset. On the other hand, image-generation-based CIS utilizes the capabilities of deep learning to produce an image representing secret information.

In this paper, we presented and summarized some articles in credible journal papers to analyze existing methods in coverless image steganography (CIS). Furthermore, this survey paper aims to identify a research gap to develop new strategies for future research.

In this survey paper, we highlighted five of the most relevant papers, "Towards a High Capacity Coverless Information Hiding Approach" [1] identified as survey paper 1 (Abdulsattar's scheme), "A Novel Coverless Information Hiding Method Based on the Most Significant Bit (MSB) of the Cover Image" identified as survey paper 2 (Yang *et al.*'s scheme), "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification" [32] identified as survey paper 3 (Zhang *et al.*'s scheme), "A novel coverless information hiding method based on the average pixel value of the sub-images" [34] identified as survey paper 4 (Zou *et al.*'s scheme) and "Coverless Information Hiding Based on the Molecular Structure Images of Material" [4] identified as survey paper 5 (Cao *et al.*'s scheme).

The remaining paper is managed as follows: Section 2 presents the related works in detail. Section 3 discusses the comparison of survey papers' performance. Then, in Section 4, future research is provided. Lastly, the paper is concluded in Section 5.

2 Related Works

The fifth survey paper shared the same phase of coverless information hiding. The first is image hashing generation. The second is database or lookup table production, and the last is mapping operation. The main difference is in the used algorithm and image selection. The summarization of the fifth survey paper characteristic is shown in Table 1.

2.1 Survey Abdulsattar's Scheme

In 2021, Abdulsattar [1] introduced a coverless data hiding by utilizing the eigenvalues decomposition in a block of sub-images. This schema employs a single image, subsequently segmented into several block images. Each block image has its eigenvalues computed, which are then utilized to construct a hash sequence. The hash sequence is then saved in an ASCII code lookup table. When a secret message is provided, it is transformed into ASCII code format. Following that, mapping the hash sequence in the lookup table will begin. The lookup table contains the hash sequence's x and y coordinates to ensure an efficient mapping operation. Parlier public key algorithm encrypts the location information of the block image, which is shared between the sender and receiver in a public transmission channel. The flowchart of Abdulsattar's scheme is shown in Figure 1.

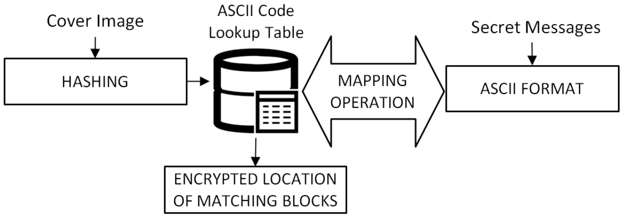

Figure 1: The flowchart of Abdulsattar's scheme [1]

In this scheme, the longer the hash sequence, the higher the hiding capacity. Therefore, Abdulsattar [1] investigated three parameters, namely block arrangement, block size, and overlapping block on the number of hash sequences. Figure 2 depicts four alternative arrangements. Several experiments revealed that arrangement two could generate more hash sequences than the other arrangements. Abdulsattar [1] adjusts six different block sizes. As a result, block sizes in the range of 3×3 and 6×6 can generate more hash sequences. The last parameter is the overlapping block. After the in-depth experiment, it can be concluded that overlapping blocks will produce more hash sequences.

To assess the robustness of Abdulsattar's scheme, seven types of image attacks were employed, including Gaussian noise, Salt & Pepper attack, speckle noise, median filtering, mean filtering, gaussian filtering, and histogram equalization. The test results are presented in Table 2.

2.2 Survey Yang *et al.*'s Scheme

In 2020, Yang *et al.* [30] introduced a coverless data-hiding scheme based on the MSB of the cover image. This method utilizes the average value μ of the fragment and maps the binary form of secret bits with the MSB of μ under pre-defined critical K. This approach achieves good image quality and is robust against steganalysis tools. However, Yang *et al.*'s scheme have a lower hiding capacity since one fragment only hides one secret bit. The flowchart of the embedding procedure is presented in Figure 3.

Four image attacks were employed to assess the robustness of Yang *et al.*'s scheme, including Gaussian noise, Salt & Pepper attack, low-pass filtering, and JPEG compression. Table 3 present the robustness analysis of Yang *et al.*'s scheme.

2.3 Survey Zhang *et al.*'s Scheme

In 2018, Zhang *et al.* [32] proposed a robust coverless image steganography based on DCT and LDA Topic Classification. The main idea of this scheme is to find the most relevant image according to secret messages. The purpose is to avoid the susceptibility of an irrelevant picture in a

Table 1: Summarization of survey paper

Schemes	Block Used Properties	Mapping Approach	Key Sharing Approch	Block Division Approch	Robustness Analysis
Abdulsattar's Scheme	Eigen decompistion	ASCII code	Pailier public key encryption algorithm	Partially overlapping	Under 7 kinds of attacks
Yang *et al.*'s Scheme	Average pixel value	Binary code (MSB)	Pseudo-random serial numbers	Non-overlapping	Under 4 kinds of attacks
Zhang *et al.*'s Scheme	Discrete cosine transform	Latent dirichlet allocation	Pseudo-random serial numbers	Non-overlapping	Under 14 kinds of attacks
Zou *et al.*'s Scheme	Average pixel value	Label sequence	Pseudo-random serial numbers	Non-overlapping	Not specified
Cao *et al.*'s Scheme	Average pixel value	Label sequence	Pseudo-random serial numbers	Non-overlapping	Not specified

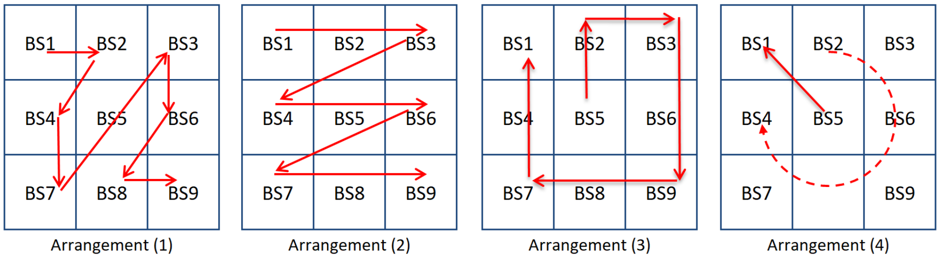

Figure 2: The block arrangement of Abdulsattar's scheme [1]

Table 2: Robustness analysis of Abdulsattar's scheme

Attacks	Parameter	Abdulsattar's Scheme [1]
Gaussian Noise Attack	v = 0.001	27.09
	v = 0.005	35.69
Salt & Pepper Noise Attack	r = 0.001	0.79
	r = 0.005	3.57
Speckle Noise Attack	v = 0.01	31.99
	v = 0.05	26.47
Median Filtering Attack	w = 3×3	16.54
	w = 5×5	25.01
Mean Filtering Attack	w = 3×3	13.18
	w = 5×5	22.64
Gaussian Filtering Attack	w = 3×3	4.01
	w = 5×5	13.13
Histogram Equalization	-	4.78

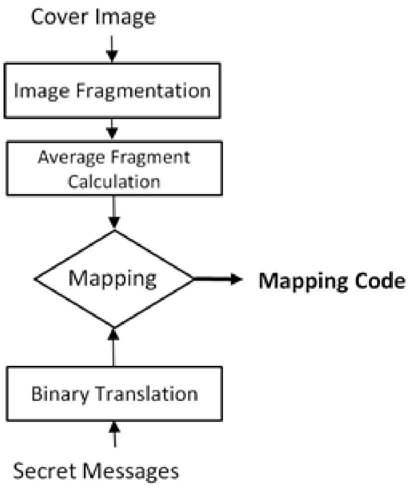

Figure 3: The flowchart of Yang *et al.*'s scheme

Table 3: Robustness analysis of Yang *et al.*'s scheme

Methods	Parameter	Yang *et al.*'s Scheme [30]
Gaussian Noise	v = 0.1	6.75
	v = 0.2	9.13
	v = 0.5	15.13
	v = 0.6	17.37
	v = 0.9	20.38
	v = 1.0	21.25
Salt & Pepper Noise	v = 0.001	0
	v = 0.003	0.13
	v = 0.005	0.25
	v = 0.007	0.63
	v = 0.009	0.88
	v = 1.0	1.38
Low Pass Filtering	w = 3×3	1.25
	w = 5×5	1.25
	w = 7×7	1.25
	w = 9×9	1.87
JPEG Compression	q=90	0.125

specific topic. The flowchart of the embedding procedure of Zhang *et al.*'s method is shown in Figure 4. Table 4 present the robustness analysis of Zhang *et al.*'s scheme.

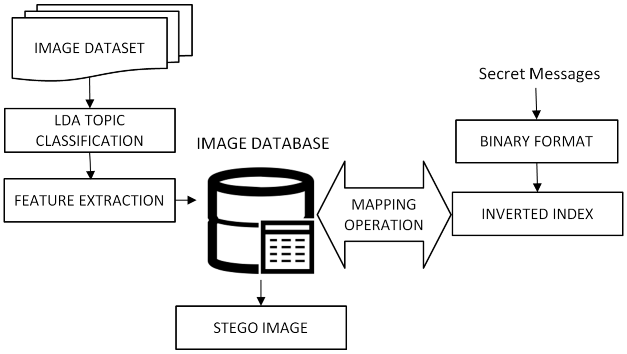

Figure 4: The Flowchart of Zhang's method [32]

2.4 Survey Zou *et al.*'s Scheme

In 2018, Zou *et al.* proposed a coverless information-hiding method based on the average pixel value of the sub-images. First, a Chinese-based dictionary is generated to manage the secret messages. Next, a hash sequence is generated by a hashing algorithm. Then a mapping relationship between the secret messages and a hashing sequence is operated to obtain the most appropriate image. The flowchart of Zou *et al.*'s scheme [34] is shown in Figure 5.

Table 4: Robustness analysis of Zhang *et al.*'s scheme

Attacks	Parameter	Zhang *et al.*'s Scheme [32]
Gaussian Noise	v = 0.001	3,01
	v = 0.005	1,72
	v = 0.1	0,86
Salt & Pepper Noise	r = 0.001	0
	r = 0.005	0
	r = 0.1	2,15
Speckle Noise	v = 0.01	0,86
	v = 0.05	0,86
	v = 0.1	2,15
Median Filtering	w = 3×3	0
	w = 5×5	0,86
	w = 7×7	1,72
Mean Filtering	w = 3×3	0
	w = 5×5	0
	w = 7×7	0
Gaussian Filtering	w = 3×3	0
	w = 5×5	0
	w = 7×7	0
Histogram Equalization	-	26,61

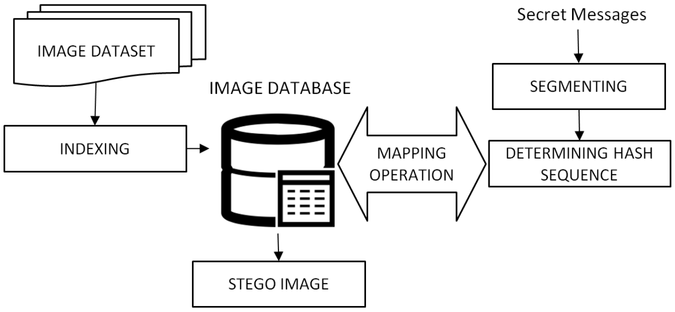

Figure 5: The flowchart of Zou *et al.*'s scheme

2.5 Survey Cao *et al.*'s Scheme

In 2018, Cao *et al.* [4] presented a coverless information hiding based on the molecular structure images of material. This scheme utilizes the average value of the sub-image pixels to represent the secret information, according to the mapping between pixel value intervals and secret information, as shown in Table 5. In addition, a pseudo-random label sequence was used to establish the sub-image location to strengthen the method's security. The Bag of Words Model (BOW) histogram calculates the number of sub-images in a picture that reveals secret information. A multi-level inverted index structure was also created to boost retrieval performance. The flowchart of Cao *et al.*'s scheme [34] is shown in Figure 6.

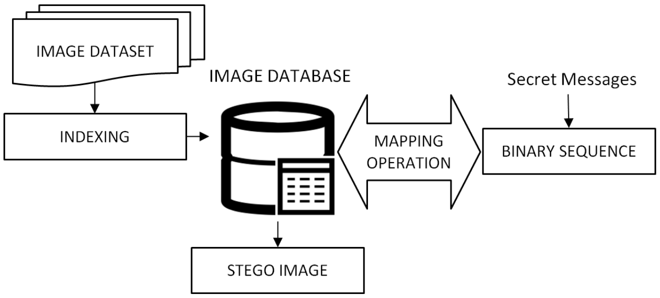

Figure 6: The flowchart of Cao *et al.*'s scheme

Table 5: The mapping relationship of secret information [4]

Pixel value intervals	Binary sequence code
0 ∼ 15	0000
16 ∼ 31	0001
32 ∼ 47	0010
48 ∼ 63	0011
64 ∼ 79	0100
80 ∼ 95	0101
96 ∼ 111	0110
112 ∼ 127	0111
128 ∼ 143	1000
144 ∼ 159	1001
160 ∼ 175	1010
176 ∼ 191	1011
192 ∼ 207	1100
208 ∼ 223	1101
224 ∼ 239	1110
240 ∼ 255	1111

3 Comparisons

In this section, the hiding capacity of five survey papers is summarized in Table 6 and compares the hiding capacity of the survey papers in the number of bits parameter. The hiding capacity is depicted in Figure 7.

Table 6: Hiding capacity comparison

Scheme	Hiding Capacity
Abdulsattar's Scheme [1]	32.736
Yang *et al.*'s Scheme [30]	16.384
Zhang *et al.*'s Scheme [32]	8.193
Zou *et al.*'s Scheme [34]	16.368
Cao *et al.*'s Scheme [4]	4.092

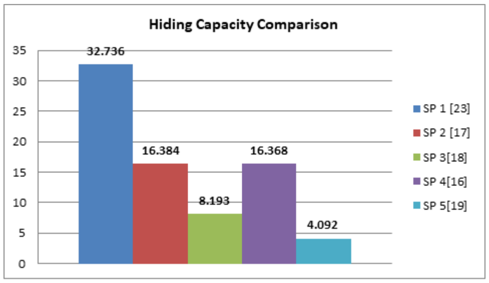

Figure 7: Hiding capacity representation

4 Future Research

According to the studies conducted, the five survey papers are mapping-based CIS. That is, the length of the hash sequence is a crucial component that should be prioritized to improve hiding capacity. Survey paper 1 investigated block size, block arrangement, and overlapping blocks. This will be future research into other properties of an image in expanding the length of the hash sequence. The second option for future CIS study is to devise a hashing algorithm that ensures image dependability against steganalysis tools and image attacks.

In terms of computational difficulty, as the size of the picture database grows, so does the complexity. It is possible to use either an image database or a lookup table to accommodate the secret messages in the basic computation. The secret messages are specified as survey paper 4 implemented a Chinese-based dictionary. It means we should develop specific language-based dictionaries when the secret messages are in the form of other languages. It will be the limit of this scheme and could be a research question for future work.

5 Conclusions

This paper provides a thorough examination of mapping-based coverless image steganography. Because the cover image is not modified, the image quality of the stego image will be the same as the cover, so the quality is optimal. The main concern in mapping-based CIS is hiding capacity. Current mapping-based CIS has limited hiding capacity. Therefore, it is necessary to do further research on how to maximize the image property in secret mapping messages. Overall, the current mapping-based CIS has a high level of robustness against steganalysis tools and image attacks.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 109-2221-E-468-011-MY3, MOST 108-2410-H-468-023, and MOST 108-2622-8-468-001-TM1.

References

[1] F. S. Abdulsattar, "Towards a high capacity coverless information hiding approach," *Multimedia Tools and Applications*, vol. 80, pp. 18821–18837, 2021.

[2] A. M. Alhomoud, "Image steganography in spatial domain: Current status, techniques, and trends," *Intelligent Automation and Soft Computing*, vol. 27, no. 1, pp. 69–88, 2021.

[3] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, pp. 426–437, 2019.

[4] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials and Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[5] X. Chen, Z. Zhang, A. Qiu, Z. Xia, and N. N. Xiong, "Novel coverless steganography method based on image selection and StarGAN," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 219–230, 2022.

[6] I. Gustavo, "Deep learning applied to steganalysis of digital images: A systematic review," *IEEE Access*, vol. 7, 2019.

[7] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, pp. 38303–38314, 2018.

[8] L. C. Huang, L. Y. Tseng, M. S. Hwang, "The study on data hiding in medical images", *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[9] D. Kapoor and A. J. Kulkarni, "Improved cohort intelligence — A high capacity , swift and secure approach on JPEG image steganography," *Journal of Information Security and Applications*, vol. 45, pp. 90–106, 2019.

[10] C. Kavitha and K. Sakthivel, "Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization," *IEEE Access*, vol. 8, pp. 136537–136545, 2020.

[11] X. Liao, J. Yin, S. Guo, X. Li, and A. Kumar, "Medical JPEG image steganography based on preserving inter-block dependencies," *Computers & Electrical Engineering*, vol. 67, pp. 320–329, 2018.

[12] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Q. Zhang, "A rpbust coverless steganography using camouflage image," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 6, pp. 4038–4051, 2022.

[13] X. Liu, Z. Li, J. Ma, W. Zhang, J. Zhang, and Y. Ding, "Robust coverless steganography using limited mapping images," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4472–4482, 2022.

[14] H. C. Lu, Y. P. Chu, M. S. Hwang, "A new steganographic method of the pixel-value differencing", *The Journal of Imaging Science and Technology*, vol. 50, no. 5, pp. 424–426, 2006.

[15] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2779–2791, 2021.

[16] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019.

[17] F. Peng, G. Chen, and M. Long, "A robust coverless steganography based on generative adversarial networks and gradient descent approximation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 9, pp. 5817–5829, 2022.

[18] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless image steganography based on optical mark recognition and machine learning," *IEEE Access*, vol. 9, pp. 16522–16531, 2021.

[19] S. Q. Saleh, "Digital image steganalysis: Current methodologies and future challenges," *IEEE Access*, vol. 10, no. August, pp. 92321–92336, 2022.

[20] J. Sharafi, Y. Khedmati, and M. M. Shabani, "Image steganography based on a new hybrid chaos map and discrete transforms," *Optik*, vol. 226, no. P2, p. 165492, 2021.

[21] N. Subramanian and O. Elharrouss, "Image steganography: A review of the recent advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021.

[22] G. Swain, "Adaptive and non-adaptive PVD steganography using overlapped pixel blocks," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7549–7562, 2018.

[23] A. O. Vyas and S. V Dudul, "A novel approach of object oriented image steganography using LSB," in *Proceedings of the 1st International Conference on*

Data Science, Machine Learning and Applicationsin (ICDSMLA'19), pp. 144–151, 2019.

[24] Y. L. Wang, J. J. Shen, M. S. Hwang, "An improved dual image-based reversible hiding technique using LSB matching", *International Journal of Network Security*, vol. 19, no. 5, pp. 858–862, 2017.

[25] Y. L. Wang, J. J. Shen, M. S. Hwang, "A novel dual image-based high payload reversible hiding technique using LSB matching", *International Journal of Network Security*, vol. 20, no. 4, pp. 801–804, 2018.

[26] C. C. Wu, M. S. Hwang, S. J. Kao, "A new approach to the secret image sharing with steganography and authentication", *The Imaging Science Journal*, vol. 57, no. 3, pp. 140–151, 2009.

[27] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", *Journal of Systems and Software*, vol. 84, no. 12, pp. 2196–2207, 2011.

[28] C. C. Wu, S. J. Kao, W. C. Kuo, M. S. Hwang, "Enhance the image sharing with steganography and authentication," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1177-1181, 2008.

[29] N. I. Wu, M. S. Hwang, "A novel LSB data hiding scheme with the lowest distortion", *The Imaging Science Journal*, vol. 65, no. 6, pp. 371–378, 2017.

[30] L. Yang, H. Deng, and X. Dang, "A novel coverless information hiding method based on the most significant bit of the cover image," *IEEE Access*, vol. 8, pp. 108579–108591, 2020.

[31] H. Zhang and L. Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," *Signal Processing: Image Communication*, vol. 78, pp. 331–344, 2019.

[32] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223–3238, 2018.

[33] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *International Conference on Cloud Computing and Security (ICCCS'15)*, vol. 1, pp. 123–132, 2015.

[34] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7965–7980, 2019.

Biography

Kurnia Anggriani received BS degree in Informatics from University of Bengkulu, Indonesia in 2011, and the MS degree in Informatics from Bandung Institute of Technology, Indonesia in 2014. Currently she is taking Ph.D degree in Asia University, Taiwan. Her current research interests include steganography and image processing.

Nan-I Wu received a Ph.D. degree in the Institute of Computer Science and Engineering from Nation Chung Hsing University (NCHU), Taichung, Taiwan, in 2009. From 2010 to 2011, he was a post-doctoral research fellow at the Academia Sinica Institute of information science. He was an assistant professor at the Department of Animation and Game Design, TOKO University (Taiwan), during 2011-2018 and an associate professor during 2018-2019. Now he is an associate professor at the Department of Digital Multimedia, Lee-Ming Institute of Technology (Taiwan) since 2019 and also the Director of the eSports Training Centre since 2020. His current research interests include game design, eSports training/magagement, multimedia processing, multimedia security, data hiding, and privacy-preserving. He published more than 10 international journal papers (SCI) and conference papers.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a distinguished professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.