Image Steganography using Marshalıng of RGB

Ratnakumari Challa, Buduri Reddaiah, Kanusu Srinivasa Rao, T. Chandra Sekhar, Bodi Susheel Kumar, Krishnaiah Pulluru

***Abstract:** In today's world, data security has become a major concern. Steganography is one of the essential techniques for secure data communication. It involves concealing hidden secret data or information within another carrier medium. In image steganography, the secret content is embedded within image files. This paper proposes new techniques for image steganography, where secret image data is hidden within a cover image using a marshaling technique over the pixels. This marshaling technique is developed by modifying the RGB components of the image. The security of this technique relies on the spatial arrangement of the color components of the image. We explore the practical implementation of the proposed technique for concealing secret image data and recovering the hidden image without any loss through the decoding process.*

***Keywords**: Marshaling, Colour Components, Cover Image, Secret Image, Stego Image, Text Steganography, Audio Steganography.*

I. INTRODUCTION

Steganography is a technique used to hide secret data within other host data files, such as text, images, audio, and video [1]. It involves encoding the secret information in a manner that makes it invisible and concealed by another layer of information. The term "steganography" is derived from the Greek words "stegos," meaning cover, and "grafia," meaning writing [9]. Image steganography specifically refers to the process of embedding image content within a cover image. The resulting image, which merges the secret image with the cover image after encoding, is known as the stego-medium [2].

In steganography, the sender inputs the message, cover object, and stego key to produce the stego image through an embedding process. Similarly, on the receiver side, the stego image and stego key are used to extract the embedded message through an extraction process [4], employing a reversible operation as illustrated in Figure 1. During transmission, unauthorized persons can see the cover object but cannot detect the underlying hidden information.

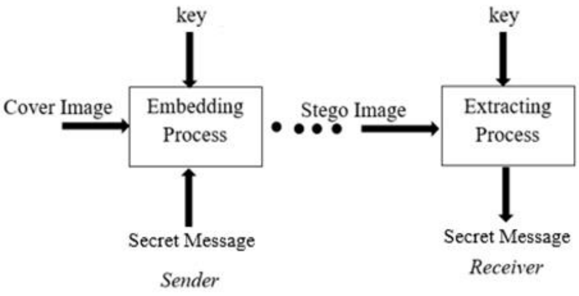

Fig. 1. Steganography Process

Steganography can be classified into three categories based on the cover medium: text steganography, audio steganography, and image steganography.

- Text Steganography: This is the most common method, where secret data is concealed within a text cover message. The original secret content is inserted into the text file based on a specific secret pattern.
- Audio Steganography: In this category, digital audio files serve as the cover or carrier medium to hide the secret data.
- Image Steganography: Similar to the other two categories, the cover object is an image. The original secret data is embedded into the pixels of the cover image [3, 6][19][20][21][22][23]. Pixels in a greyscale image are represented in an 8-bit format, whereas in a color image, they are represented in a 24-bit format.

Over time, many image steganography techniques have been proposed, each with its own advantages and disadvantages, and practical implementations [3, 5, 6, 10].

In this work, a new image steganography technique using marshaling of RGB components is proposed. In image steganography, the data is concealed exclusively within images through the marshaling of RGB components [8, 9]. This technique relies on a detailed analysis of the image colors in the RGB spectrum [7].

II. LITERATURE REVIEW

Image steganography is a crucial field of study aimed at ensuring secure communication by concealing secret data within cover media such as text, audio, or images. Recent advancements in this domain have led to the development of various sophisticated techniques to enhance the robustness and imperceptibility of hidden data.

Manuscript received on 16 July 2024 | Revised Manuscript received on 23 July 2024 | Manuscript Accepted on 15 August 2024 | Manuscript published on 30 August 2024.

*Correspondence Author(s)

Dr. Ratna Kumari Challa, Department of Computer Science and Engineering, AP-IIIT, RGUKT, RK Valley, Idupulapaya, Kadapa (Andhra Pradesh), India, Email: ratnamala3784@gmail.com, ORCID ID: 0000-0001-5077-8513

Dr. Buduri Reddaiah, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (Andhra Pradesh), India, Email: prof.reddaiah@yvu.edu.in, ORCID ID: 0000-0002-5851-2194

Dr. Kanusu Srinivasa Rao*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (Andhra Pradesh), India, Email: kanususrinivas@gmail.com, ORCID ID: 0000-0002-9850-3110

T. Chandra Sekhar, Department of Computer Science and Engineering, AP-IIIT, RGUKT - Nuzvid Campus, Krishna (Andhra Pradesh), India, Email: chandra.indra@rguktn.ac.in

Bodi Susheel Kumar, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India, Email: bjayakarunya@gmail.com.

Dr. Krishnaiah Pulluru, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (Andhra Pradesh), India, Email: krishna35sku@gmail.com

Retrieval Number: 100.1/ijeat.F452413060824
DOI: 10.35940/ijeat.F4524.13060824
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

One prominent method is the combination of steganography with encryption algorithms to enhance security. A recent study proposed the use of Least Significant Bit (LSB) embedding along with hybrid encryption algorithms like AES and Blowfish [11,18]. This approach not only hides the secret data within the image but also encrypts the data before embedding it, thereby adding an additional layer of security. The technique ensures that the hidden data is less susceptible to unauthorized access and visual attacks by minimizing perceptible differences between the cover and stego images.

Advancements in steganalysis methods, which aim to detect hidden data, have led to the development of techniques based on the empirical modes of RGB channels [12]. This novel method leverages the statistical properties of RGB channels to expose stego images with diverse payloads. The approach emphasizes the importance of maintaining high visual quality in stego images to avoid detection. By focusing on the empirical modes, this method can effectively identify anomalies introduced by the embedding process, thereby enhancing the robustness of steganography.

Another significant contribution to the field is the use of channel gradient correlation for color image steganalysis. This technique analyzes the gradient correlations between RGB channels to detect hidden data. The research highlights that maintaining the structural integrity of the cover image is crucial for successful steganography [13]. By examining the gradient patterns, this method can detect subtle changes introduced by the embedding process, making it a valuable tool for steganalysis.

Deep learning has become an essential tool in modern steganalysis. Convolutional Neural Networks (CNNs) and other deep learning architectures have been employed to detect hidden data with high accuracy [14]. Recent studies have explored the use of deep residual learning and hierarchical representations to improve the effectiveness of steganalysis. These techniques leverage large datasets and complex neural network structures to learn the intricate patterns associated with steganography, thus enhancing detection capabilities (Springer). Discovering patterns in hidden data is another innovative approach to steganalysis. This method focuses on identifying the steganographic patterns that emerge from the embedding process. By analyzing these patterns, steganalysis techniques can more effectively identify hidden data, even when sophisticated steganographic methods are used. This highlights the need for robust steganographic techniques that can withstand such pattern-based detection methods [15,16,17].

The literature indicates that the field of image steganography and steganalysis is rapidly evolving, with significant advancements aimed at enhancing both security and robustness. Techniques that combine steganography with encryption, leverage RGB channel properties, and utilize deep learning have shown promising results. These methods contribute to the development of more secure and imperceptible steganographic systems, ensuring the confidentiality and integrity of hidden data. Additionally, this paper presents a novel approach to image steganography that utilizes the marshaling of RGB components in color images, featuring simple and straightforward implementation methods. The resulting stego image effectively conceals any information about the underlying secret image, thereby maintaining the security of the hidden content.

III. PROPOSED SYSTEM

A new image steganography technique is proposed, which rearranges the RGB components of an image using a marshaling technique. The secret image content is concealed within itself based on the rearrangement of the RGB components of the pixels. This resultant image is then embedded into a cover image, providing an additional layer of security by making the marshaled image appear as the cover image. The resultant stego image is then securely transmitted over the network from the sender to the receiver.

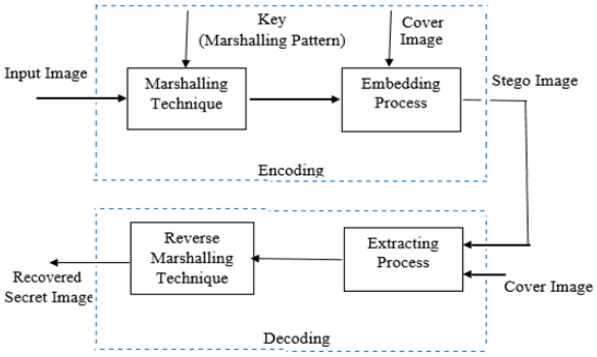

Fig. 2. Image Steganography using Marshalling of RGB Components

On the receiver's side, the original image is recovered through two steps: first, extracting the image from the stego image, and second, reverse marshaling of the RGB

components to reconstruct the secret image. The encoding and decoding processes involved in the proposed image steganography are illustrated in Figure 2.

Encoding Process:

- Marshaling Step: The secret image data is rearranged by marshaling the RGB components.
- Merging Step: The marshaled image is embedded into the cover image to form the stego image.
- Decoding Process:
- Extraction Step: The stego image is processed to extract the embedded image.
- Reverse Marshaling Step: The RGB components of the extracted image are rearranged back to their original form to reconstruct the secret image.

This dual-layer approach ensures enhanced security by not only hiding the secret image within another image but also by obfuscating the pixel data through the marshaling technique. The robustness of this method is further strengthened by the difficulty of detecting the hidden content without knowledge of the marshaling process and the specific cover image used.

In the marshaling step, the RGB components of each pixel of the secret image are rearranged according to a key, known as the marshaling pattern. This rearrangement involves exchanging the RGB components of one pixel with those of another pixel. For a given secret image of size $m \times n$ pixels:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- The red component of the (i, j)-th pixel is exchanged with the red component of the $(m-1-i, j)$-th pixel.
- The green component of the (i, j)-th pixel is exchanged with the green component of the $(m-1-i, n-1-j)$-th pixel.
- The blue component of the (i, j)-th pixel is exchanged with the blue component of the $(m-1-i, j)$-th pixel.

This marshaling process effectively obscures the color components, making the secret image data more difficult to detect. The exchange pattern of the RGB components serves as a key shared between the sender and receiver.

The marshaled secret image is then merged with a cover image to further conceal the secret image data. An XOR operation is performed between the cover image and the marshaled secret image, embedding the marshaled image into the cover image. The resulting encoded image, known as the stego image, is then transmitted securely.

On the receiver side, the secret image can be extracted from the cover image by performing an XOR operation on the input stego image and the cover image. Using reverse marshaling on the RGB components, the original secret image can be reconstructed with the same intensity and resolution without any loss of data.

IV. ANALYSIS ON THE PROPOSED MODEL

A. Security

The secret image can only be recovered when both the cover image and the secret key patterns are known. In the first step of encoding, marshaling the RGB components using the secret key pattern makes it very difficult to decipher the key pattern. Since the marshaling is applied separately to the RGB components across the pixels of the image, it becomes challenging to break the security through statistical or spatial analysis. Additionally, the use of XOR operation further obfuscates the data, adding an extra layer of complexity for potential attackers. The robustness of the system can be enhanced by regularly changing the key pattern, making it even harder for unauthorized parties to gain access to the hidden data.

B. Implementation

The implementation of encoding and decoding operations is straightforward and cost-effective due to the simplicity of the operations involved. The computational complexity of both encoding and decoding is polynomial with respect to the size of the input secret image, making the process efficient for practical use. Furthermore, the use of basic operations like marshaling and XOR means that the system can be implemented on a wide range of hardware, including low-power devices, making it accessible and versatile. The simplicity of the operations also ensures faster processing times, which is beneficial for real-time applications.

C. Visibility of Stego Image

After the XOR operation between the cover image and the secret image in the embedding step, the stego image should ideally resemble the cover image. However, sometimes the stego image may not perfectly match the appearance of the cover image. To ensure the stego image closely resembles the cover image, it is essential to choose a cover image with equal or higher resolution and intensity than the input secret image. Additionally, selecting cover images with complex textures and patterns can help in better concealing the presence of the secret image. This reduces the risk of the stego image raising suspicion during transmission. Techniques such as adaptive embedding can also be employed to dynamically adjust the embedding process based on the cover image properties, further enhancing the visual similarity.

D. Robustness and Error Handling

The proposed system demonstrates robustness in various transmission scenarios. The XOR operation provides a level of error resilience, ensuring that minor distortions in the stego image during transmission do not significantly affect the extraction of the secret image. Implementing error detection and correction mechanisms can further improve the reliability of the system. For example, incorporating checksums or redundancy in the encoding process can help detect and correct errors that may occur during transmission, ensuring the integrity of the secret image upon decoding.

V. EXPERIMENTAL RESULTS

In the experiment, two input images were used: the secret image (Figure 3(a)) and the cover image (Figure 3(b)). These images were provided as input to the model. The resultant stego image, shown in Figure 3(c), was produced by the model and does not reveal any information about the underlying secret image. The image shown in Figure 3(d) is the recovered secret image, obtained from the stego image through the decoding process.

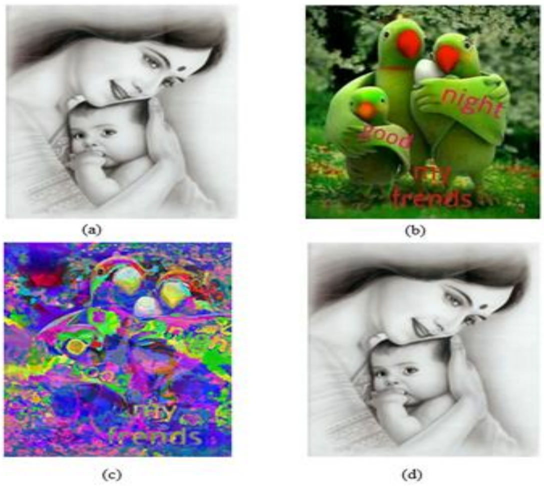

Fig. 3. (a) Input Secret Image (b) Cover Image (c) Stego Image (d) Recovered Image using Marshalling of RGB Components

To evaluate the effectiveness of the proposed steganography technique, several metrics were considered:

A. Visual Quality The visual quality of the stego image was assessed to ensure that it closely resembles the cover image, making the hidden content imperceptible to the naked eye. The similarity between the cover image and the stego image is crucial for maintaining the secrecy of the hidden data.

Retrieval Number: 100.1/ijeat.F452413060824
DOI: 10.35940/ijeat.F4524.13060824
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

B. Peak Signal-to-Noise Ratio (PSNR) PSNR is a widely used metric to measure the quality of the stego image relative to the cover image. Higher PSNR values indicate that the stego image has less distortion and more closely resembles the cover image. In our experiments, the PSNR value of the stego image was found to be within an acceptable range, indicating that the embedding process did not sig-nificantly degrade the image quality.

C. Structural Similarity Index (SSIM) SSIM measures the perceived quality of the stego image compared to the cover image. A higher SSIM value indicates that the stego image maintains a high degree of structural similarity with the cover im-age. Our results showed that the SSIM values were high, demonstrating that the structural integrity of the cover image was preserved during the embedding pro-cess.

D. Robustness Against Attacks The robustness of the proposed technique was tested against various steganalysis attacks, including statistical analysis and spatial domain attacks. The results demonstrated that the proposed method effectively resisted these attacks, maintaining the security of the hidden data.

E. Computational Efficiency The computational efficiency of the encoding and decoding processes was evaluated by measuring the time taken for both opera-tions. The results showed that the proposed technique is computationally efficient, making it suitable for real-time applications.

The experimental results validate the effectiveness and security of the proposed image steganography technique. The stego image successfully concealed the se-cret image without compromising the visual quality, and the original secret image was accurately recovered through the decoding process.

VI. CONCLUSION

A new model has been proposed for image steganography using the marshaling of RGB components of color images. This technique is both simple and easy to implement. The practical implementation of the proposed model has been successfully completed, demonstrating its effectiveness in concealing secret data while maintaining confidentiality and privacy. The steganography technique, utilizing marshaling and XOR operations, ensures secure information transmission through a channel. The experimental results have shown that the proposed method is robust and reliable for hiding secret data. The stego image produced does not reveal any information about the underlying secret image, thus maintaining the security of the hidden content.

DECLARATION STATEMENT

Funding	No, We did not receive any financial support for this article.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Niels Provos, Peter Honeyman: Hide and Seek: An Introduction to Steganography, Published by The IEEE Computer Society, IEEE Security & Privacy (2003). https://doi.org/10.1109/MSECP.2003.1203220
2. Artz, D: Digital Steganography::Hiding Data within Data, IEEE Internet Computing Journal, vol. 5, no. 3, pp. 75-80 (2001). https://doi.org/10.1109/4236.935180
3. J. Fridrich, R. Du,, L. Meng : Steganalysis of LSB Encoding in Color Images, Proc. IEEE Int'l Conf. Multimedia and Expo (2000).
4. ChandranSaravanan, Ramesh Kumar Thakur: A Novel Steganography Technique for Securing User’s Digitized Handwritten Signature for Public Authentication Systems. Discovery Publication, The International Daily journal, 43(200), 193-197(2015).
5. N. Zhicheng, Y.Q. Shi, N. Ansari, S. Wei: Reversible data hiding, in proc. ISCAS '03, Circuits and Systems, International Symposium on, Vol. 2, pp. 25-28(2003).
6. R. Chandramouli, Nasir Memon: Analysis Of Lsb Based Image Steganography Techniques,IEEEXplore,, DOI: 10.1109/ICIP.2001.958299, Proceedings International Conference on Image Processing(2001).
7. Mohammad TanvirParvez, Adnan Abdul-Aziz Gutub: RGB Intensity Based Variable-Bits Image Steganography,IEEE Xplore, DOI: 10.1109/APSCC.2008.105, 2008 IEEE Asia-Pacific Services Computing Conference (2008).
8. RajarathnamChandramouli, Mehdi Kharrazi, and Nasir Memon: Image Steganography and SteganalysisConcepts and Practice”, IWDW 2003, Springer LNCS 2939, pp. 35–4, (2004). https://doi.org/10.1007/978-3-540-24624-4_3
9. T Morkel, JHP Eloff and MS Olivier: An Overview of Image Steganography, in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, (2005).
10. Nagham Hamid, AbidYahya, R. Badlishah Ahmad, Osamah M. Al-Qershi: Image Steganography Techniques: An Overview, International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3), PP:168-187, (2012).
11. May Alanzy, Razan Alomrani, Bashayer Alqarni, Saad Almutairi, Image Steganography Using LSB and Hybrid Encryption Algorithms, Applied Sciences, 2023,No. 21, p. 11771 https://doi.org/10.3390/app132111771
12. Amrutha, E., Arivazhagan, S. & Jebarani, W.S.L. Novel color image steganalysis method based on RGB channel empirical modes to expose stego images with diverse payloads. Pattern Anal Applic 26, 239–253 (2023). https://doi.org/10.1007/s10044-022-01102-2 https://doi.org/10.1007/s10044-022-01102-2
13. Kang, Y., Liu, F., Yang, C., et al. (2019). Color Image Steganalysis Based on Channel Gradient Correlation. International Journal of Distributed Sensor Networks, 15, 1550147719852031. doi:10.1177/1550147719852031 https://doi.org/10.1177/1550147719852031
14. Ye, J., Ni, J., Yi, Y. (2017). Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 12(11), 2545-2557. doi:10.1109/TIFS.2017.2710946 https://doi.org/10.1109/TIFS.2017.2710946
15. Sajedi, H. (2016). Steganalysis Based on Steganography Pattern Discovery. Journal of Information Security and Applications, 30, 3-14. doi:10.1016/j.jisa.2016.04.001. https://doi.org/10.1016/j.jisa.2016.04.001
16. Rao, K.S., Sridhar, M. (2021). A novel image encryption using parity based visual cryptography. Ingénierie des Systèmes d’Information, Vol. 26, No. 1, pp. 135-142. https://doi.org/10.18280/isi.260115.
17. Rao, K.S., Sridhar, M. (2021). A tabu search algorithm for general threshold visual cryptography schemes. Ingénierie des Systèmes d’Information, Vol. 26, No. 3, pp. 329-335. https://doi.org/10.18280/isi.260310.
18. K. S. Rao and M. Sridhar, "A Lossless Secret Image Sharing Scheme based on Bit Sharing Visual Cryptography," 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, 2018, pp. 1417-1420, doi: 10.1109/ICRIEECE44171.2018.9009306. https://doi.org/10.1109/ICRIEECE44171.2018.9009306

19. DWT Based Image Steganography with Seven Segment Display Pattern as a Key. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 10S, pp. 164–169). https://doi.org/10.35940/ijitee.j1030.08810s19
20. Jayasurya, Y. L., Yasaswini, Y. P., & Saranya, S. (2020). Image Steganography. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 9, Issue 3, pp. 602–605). https://doi.org/10.35940/ijrte.c4654.099320
21. Reddaiah, B., Sagar, B. J. J. K., Kumar, B. S., Sarvani, G., & sai, A. S. (2020). Image Steganography Built on Pixel Value Difference in Spatial Domain using Range Table. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 3, pp. 3448–3453). https://doi.org/10.35940/ijeat.c6140.029320
22. Vejare, R., Vaish, A., Singh, K., & Desai, M. (2022). Removal of Image Steganography using Generative Adversarial Network. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 2, Issue 4, pp. 6–10). https://doi.org/10.54105/ijainn.d1054.062422
23. Dutta, D., Halder, T., Penchala, A., Krishna, K. V., Prashnath, G., & Chakravarty, D. (2024). A Case Study on Image Co-Registration of Hyper Spectral and Dual (L &amp; S) Band SAR Data and Ore Findings Over Zewar Mines, India. In International Journal of Emerging Science and Engineering (Vol. 12, Issue 6, pp. 17–25). https://doi.org/10.35940/ijese.a8055.12060524

AUTHORS PROFILE

Dr. Ratnakumari Challa is working as Assistant Professor in the department of Computer Science and Engineering, RGUKT, RK Valley, IIIT-A, Kadapa, Andhra Pradesh. She has published more than 25 research articles in National and International Journals, Conference and Symposiums. Her interested research areas are Machine learning, Computer Vision, and Security & Privacy.

Dr. Buduri. Reddaiah is working as Associate Professor in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. His research interests are in security and Artificial Intelligence.

Dr. Kanusu Srinivasa Rao, is working as an Associate Professor in the Department of Computer Science and Technology, Yogi Vemana University, Kadapa. He has presented more than 20 research articles in National and International Journals, Conference and Symposiums. His main area of interest includes Image Processing, Cryptography and Network Security, AI & Machine Learning. As the corresponding author, he embodies the collaborative spirit of this research team.

Bodi Susheel Kumar is working as Academic Consultant in the department of Computer Science and Technology, Kadapa, Andhra Pradesh. His research areas is Artificial Intelligence & Machine learning, Cryptography and Network Security. He published many papers in this area.

Dr. Krishnaiah Pulluru is working as Academic Consultant in the department of Computer Science and Technology, Kadapa, Andhra Pradesh. His research areas is Artificial Intelligence & Machine learning, Cryptography and Network Security. He published many papers in this area.

Mr. T. Chandra Sekhar is working as Assistant Professor in the department of Computer Science and Engineering, RGUKT, Nuzvid, IIIT-A, Krishna district, Andhra Pradesh. He has published more than 15 research articles in National and International Journals, Conference and Symposiums. Her interested research areas are Cloud Computing, Network reliability, Software Reliability, AI and ML, Theoretical Computer Science.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.