J. C. Bose Journal of Engineering, Technology and Sciences
Vol. 2, Issue No. 1, October 2026

Assessment of Multilevel Security Mechanisms under Prevalent Invasion

Vyoma Vaish*[1], Kakoli Dutt[1], Ashutosh Dixit[2]

[1] Department of Life Sciences, J.C. Bose University of Science and Technology, YMCA, Sector-6, Faridabad, Haryana - 121006, India
[2] Department of Computer Engineering, J.C. Bose University of Science and Technology, YMCA, Sector-6, Faridabad, Haryana - 121006, India

Abstract: Multilevel Security (MLS) is a layered approach designed to protect data from unauthorized access, ensuring confidentiality, integrity, and robustness against diverse threats. Several surveys have explored multilevel security techniques typically combining cryptography and steganography but most remain largely theoretical and lack comprehensive experimental validation. In addition, many existing reviews overlook critical parameters such as resistance to noise attacks, robustness, execution time, and practical implementation. These gaps are particularly concerning in sensitive domains like medical image protection, where both confidentiality and diagnostic fidelity must be preserved. To address these issues, this study systematically evaluates multilevel security approaches across multiple metrics, including qualitative and quantitative analysis, robustness, and computational efficiency, while offering comparative insights across different methods. The findings reveal that multilevel security frameworks strengthen protection overall, yet no single mechanism consistently outperforms others across all evaluation criteria, underscoring the need for adaptive and hybrid strategies.
Keywords: *Multi-Level Security, Noise Attacks, Steganography, Cryptography*

1. Introduction

In the modern era of rapid advancements in communication and computing technologies, internet usage has expanded significantly, transforming personal and professional interaction over open networks. The transmission of data/images across such channels increased the risk of unauthorized access, potential threats that result in time loss, resources, and finances. To counter these risks, early approaches relied on single-layer security mechanisms. Although these methods provided a certain level of protection, their reliance on a single line of defense made them relatively easy to breach. Moreover, these approaches also exhibited several limitations, including vulnerability to cryptanalysis, lack of robustness against non-cryptographic attacks, high latency and resource consumption and the inherent weakness of relying on just one defensive barrier. These weaknesses highlighted the inadequacy of a single line of defense, thereby motivating the shift towards multilayer security mechanisms, which integrate complementary techniques to strengthen confidentiality, integrity, and resilience against diverse threats, thus strongly protecting digital data against various attacks, especially in sensitive domains such as medical imaging. Many existing surveys of MLS show that combining cryptography (for strong confidentiality and integrity guarantees) with steganography (for covert transmission and added secrecy) yields stronger protection than either approach alone. To assess the effectiveness of MLS systems, the four key parameters are commonly evaluated, which are given below:

Qualitative Security Analysis (QSA): Visual inspection is commonly employed to identify perceptual differences between the original image and the stego-image. Although this method is subjective, it remains an essential step because it helps detect noticeable distortions that may expose the presence of hidden information to human observers.

. *Corresponding author
Email address: vyoma873@gmail.com

Received 20 April 2026; Accepted 22 May 2026
Published online 11 October 2026

©2026 JCBJETS

Quantitative Security Analysis (QnSA): These metrics are employed to objectively evaluate imperceptibility, similarity, and randomness in encrypted or stego-images. To further assess the efficiency and security of images, several objective metrics are commonly employed, including Correlation Coefficient (CC), Peak Signal to Noise Ratio (PSNR), Embedding Capacity, Universal Image Quality Index (UIQI), Structural Similarity Index Metric (SSIM), Robustness, Number of Pixel Change Rate (NPCR) and Entropy.

Robustness Analysis (RA): This refers to the capability of a secured image to resist distortions and intentional attacks while preserving both image quality and data integrity. In an MLS scheme, a robust system ensures that hidden information remains recoverable or encrypted images remain decryptable even after manipulations. Different attacks used to evaluate robustness include quantitative analysis, noise attacks (Gaussian, salt-and-pepper), and geometrical attacks (cropping, rotation). The robust MLS mechanism thus effectively withstands these challenges, ensuring reliable protection with minimal quality loss.

Computational Efficiency (CE): It reflects the computational resources required for processes such as encryption, embedding, extraction, and related pre- or post-processing steps.

This paper presents an experimental survey of MLS mechanisms using the above-explained evaluation parameters. Unlike most existing reviews that remain theoretical or offer limited validation, overlooking practical evaluation factors such as qualitative analysis, quantitative analysis, noise attacks and runtime performance, this paper addresses those gaps systematically, which assess MLS schemes using these evaluation parameters.

The rest of the paper is organized as follows: Section 2 gives the literature about the other survey papers that have worked on the above-mentioned security parameters. Section 3 provides the details of technologies used by these multilevel techniques to provide security. The details of the simulation setup parameters are given in Section 4, followed by Section 5, which discusses results and overall conclusions.

2. Literature Survey

Table 2 given below summarizes the literature survey and research works that have investigated security mechanisms on image protection. The comparison highlights whether the studies were theoretical (T) or experimental (E), the number of techniques analyzed, and the extent to which core security properties confidentiality, integrity, and imperceptibility were addressed. In addition, the table identifies whether robustness against practical attacks such as noise, geometric transformations, or occlusion was considered.

From the comparison, it can be observed that a majority of the earlier works are theoretical in nature (Taha et al., 2019; Almuhammadi & Al-Shaaby, 2017; Joseph Raphael & Sundaram, 2010; Baby & Krishnan, 2017; Jan et al., 2021; Patil et al., 2021; Mustafa et al., 2019; Wajgade & Kumar, 2013; Rahmani et al., 2014), focusing primarily on conceptual discussions without practical validation. Only a smaller subset (Chaudhary et al., 2015; Joseph Raphael & Sundaram, 2010; Bansal et al., 2016) carried out experimental evaluations, often with a limited number of techniques.

With respect to the security parameters, imperceptibility, a critical factor in multimedia applications, was less consistently emphasized. More importantly, robustness against attacks (noise, geometric distortions, or occlusion) is absent across most surveys, leaving a gap in practical assessment. This gap justifies the need for systematic, experimental evaluations as presented in this paper, which consider both qualitative and quantitative parameters under realistic attack conditions. No one discussed computational efficiency.

Table 1: Literature Survey

Reference	Comparison Type (T/E)	No. of Tech. Compared	Q_nSA	QSA	RA	CE
Taha et al., 2019	T	22	N	N	N	N
Almuhammadi & Al-Shaaby, 2017	T	19	Y	Y	N	N
Chaudhary et al., 2015	E	5	Y	Y	N	N
Joseph Raphael & Sundaram, 2010	T	19	Y	N	N	N
Maryoosh et al., 2021	E	12	N	N	N	N
Baby & Krishnan, 2017	T	9	N	N	N	N
Jan et al., 2021	T	26	P	Y	N	N
Patil et al., 2021	T	-	N	N	N	N
Bansal et al., 2016	E	4	Y	Y	N	N
Mustafa et al., 2019	T	10	P	N	N	N
Wajgade & Kumar, 2013	T	-	N	N	N	N
Rahmani et al., 2014	T	19	N	N	N	N

Where T represents Theoretical, E represents Experimental, N represents No, Y represents Yes, P represents Partial.

3. Available Multilevel Security Mechanisms

Various research works have combined steganography, cryptography, and compression to enhance secure data hiding, forming a multi-level protection framework, which has been illustrated in Figure 2 and Table 2 given below. Figure 2 given below shows a secure image hiding system that combines compression, encryption, and steganography to hide a text or image securely within another image to produce a stego-crypto image. The process begins with the hiding of an image or data, where compression is done to minimize data size, followed by encryption of the compressed data with a secret key, which secures access to the data. Finally, steganography embeds the encrypted data within a cover image to protect it from visibility or detection by a third party. The resultant stego-crypto image after applying the multilevel security mechanism looks like a normal image. This approach enhances both data security and confidentiality, imperceptibility, and robustness, making it suitable for secure communication and data protection through open channels.

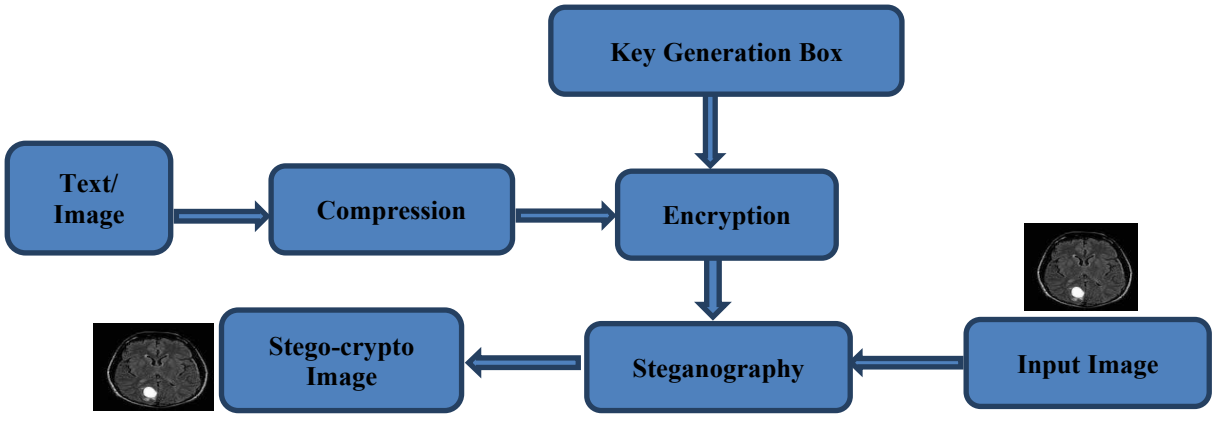


Figure 1: Block Diagram of Multi-Level Security

Table 2a represents the abbreviation table and Table 2 b shows the comparative overview of various research works that combine steganography, cryptography, and compression for secure data hiding. Each row represents a different reference, outlining which techniques were used in each of the three domains. In steganography, spatial domain techniques such as LSB and its variants (e.g., pseudorandom LSB and pixel selection) are widely used for simplicity and imperceptibility, while frequency domain methods like DWT, DCT, and BPCS, along with improved BPCS (IBPCS), offer greater robustness and invisibility. On the cryptography side, traditional algorithms such as DES, AES, RSA, RC4, and the Vigenère cipher are commonly applied, while chaos-based approaches (e.g., Logistic Map) introduce unpredictability, and more advanced schemes such as quantum cryptography and visual cryptography provide emerging alternatives. Compression, mainly through Huffman coding, is often integrated to reduce data size before or after encryption and embedding, ensuring storage efficiency and quality preservation. Together, these techniques define a secure image hiding process where the original message (text or image) is first compressed, then encrypted with a chosen cryptographic scheme, and finally embedded into a cover image using spatial, frequency, or hybrid steganography methods. A proposed security mechanism should have all the features given above.

Table 2a: Abbreviation table

AES	Advanced Encryption Standard
BPCS	Bit Plane Complexity Segmentation
CNN	Convolutional Neural Network
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DWT	Discrete Wavelet Transform
DWT-2L	Discrete Wavelet Transform – Two Level
DWT-IL	Discrete Wavelet Transform – Integer Lifting
IBPCS	Improved Bit Plane Complexity Segmentation
LSB	Least Significant Bit
RC4	Rivest Cipher 4
RSA	Rivest–Shamir–Adleman
SVD	Singular Value Decomposition

Table 2b: Available Multilevel Security Mechanisms

Reference	**Steganography / Watermarking Technique**	**Cryptography Technique**	**Compression / Additional Technique**
Nivedhitha et al., 2012	LSB	DES	–
Gupta et al., 2012	LSB	RSA / Diffie-Hellman	–
Nain et al., 2013	Pseudorandom LSB	RC4	–
Dhall et al., 2016	Pseudorandom LSB	Vigenère Cipher	Huffman Compression
Tayal et al., 2016	DWT + BPCS	Logistic Map	–
Tayal et al., 2017	IBPCS	Hierarchical Encryption	Huffman Compression
Bansal et al., 2018	IBPCS	Chaos-Based Encryption	Huffman Compression
Banharnsakun, 2018	ABC	–	–
Elhoseny et al., 2018	DWT-1L / DWT-2L	RSA + AES	–
Bal et al., 2021	LSB Watermarking	Symmetric Key	–

		Cryptography	
Jain et al., 2018	DCT Steganography	Visual Cryptography	–
Rawat et al., 2018	IBPCS	Chaotic-Based Hierarchical Encryption	Huffman Compression
Tauhid et al., 2019	DCT + LSB	AES	–
Jain et al., 2019	DWT	Hierarchical Visual Encryption	Huffman Compression
Paul et al., 2020	LSB (Pixel Selection)	AES	–
Dhall & Gupta, 2021	IBPCS + LWT Watermarking	Quantum Scrambling Encryption	Huffman Compression
Islam et al., 2014	LSB Steganography (Status Bits)	Visual Encryption	Huffman Compression
Khandelwal et al., 2022	Adaptive LSB Steganography	AES	Pixel Locator Sequence
Khalifa & Guzman, 2022	DWT-SVD	Threshold Value Encryption	Image Scrambling
Li et al., 2022	CNN-Based Deep Steganography	Deep Learning Security	Symmetry Adaptation
Zhang et al., 2022	Coverless Image Steganography	CNN Face Recognition	Morphing Technique
Nezami et al., 2022	Wavelet Transform Steganography	Multi-Region Encryption	Double Matrix Decomposition
Hu et al., 2022	Hash-Based LSB Steganography	Hash Function Encryption	Secure Random Embedding

4. Simulation Setup Parameters

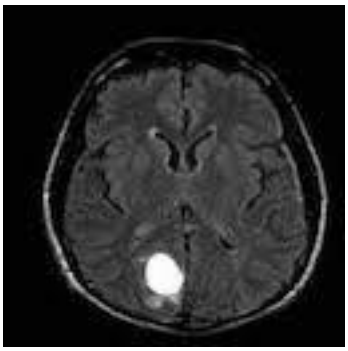
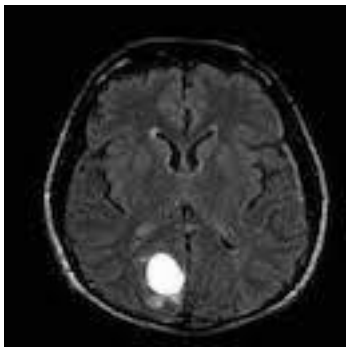
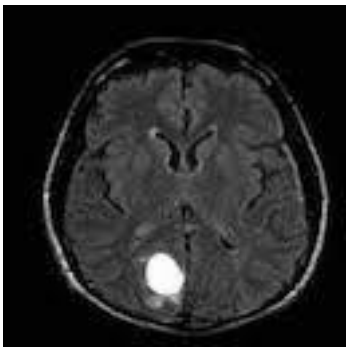
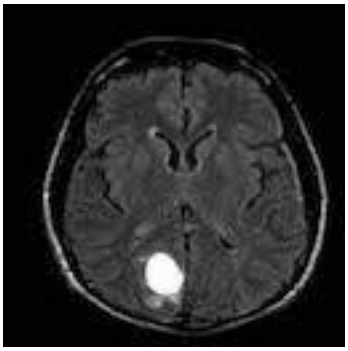
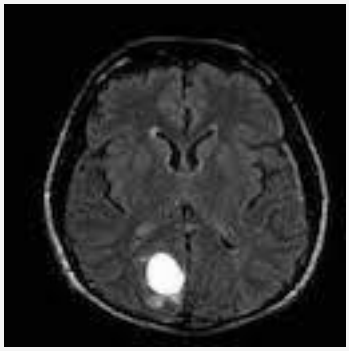
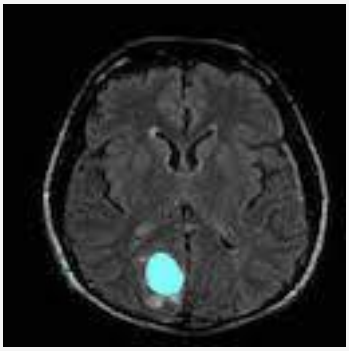
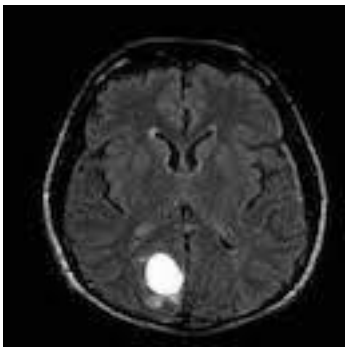
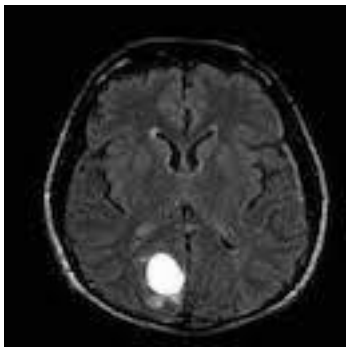
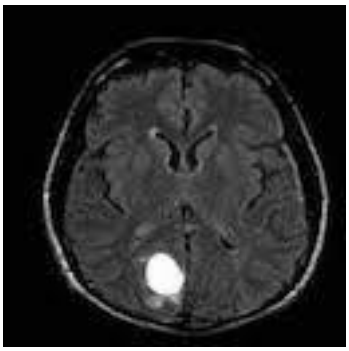
Table 3 below shows the simulation setup parameters used to tune the system to perform the experiments.

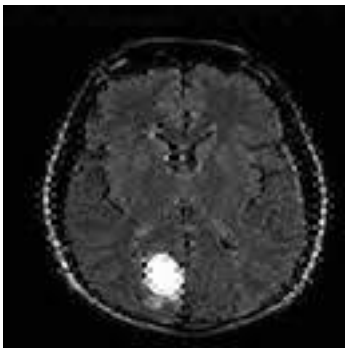
Table 3: Simulation Setup Parameters

Parameter	**Specification**
System	Apple MacBook Pro (Apple Silicon- M1/M2/M3)
Processor	Apple M2 Pro Chip, 10-core CPU (6 Performance, 4 Efficiency)
RAM	16 GB Unified Memory
Operating System	Mac OS Sonoma 14.0
Programming	Python 3.11 (via Anaconda or Pyenv)
Image Processing	OpenCV 4.9, scikit-image, PIL
Medical Image	CT, MRI scans (256X256, 512x512, 1024X1024, 2048X2048 and 4K
Visualization	Matplotlib, Seaborn, TensorBoard

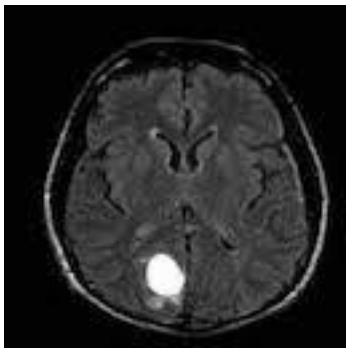
5. Results and Discussions

The investigation of image quality (before and after embedding) evaluates the confidentiality of the diverse mechanisms. The results section is divided into four parts as mentioned previously. Figure 3 shows the original and the image obtained after the proposed mechanism by different researchers. These results can be used for comparisons to verify the visual quality and imperceptibility of secret data in the cover image.

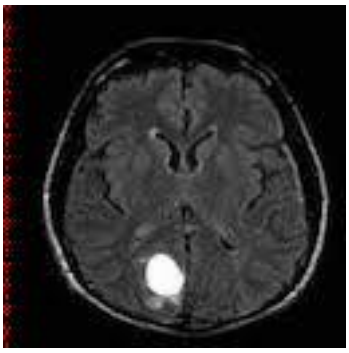
Original Image	Stego Images 1 (Nivedhitha et al., 2012)	Stego Images 2 (Gupta et al., 2012)
		
Stego Images 3 (Nain et al., 2013)	Stego Images 4 (Dhall et al., 2016)	Stego Images 5 (Tayal et al., 2016)
		
Stego Images 6 (Tayal et al., 2017)	Stego Images 7 (Bansal et al., 2018)	Stego Images 8 (Banharnsakun, 2018)
		
Stego Images 9 (Elhoseny et al., 2018)	Stego Images 10 (Bal et al., 2021)	Stego Images 11 (Jain et al., 2018)



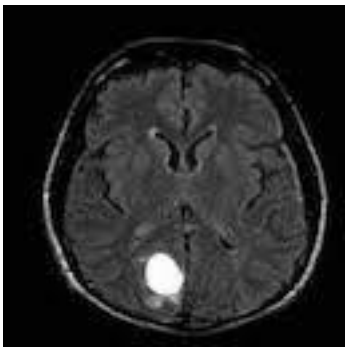
Stego Images 12 (Rawat et al., 2018)



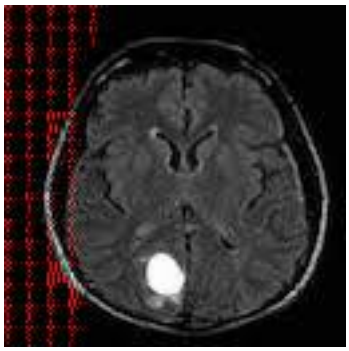
Stego Images 13 (Tauhid et al., 2019)



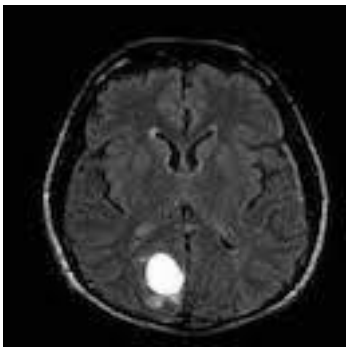
Stego Images 14 (Jain et al., 2019)



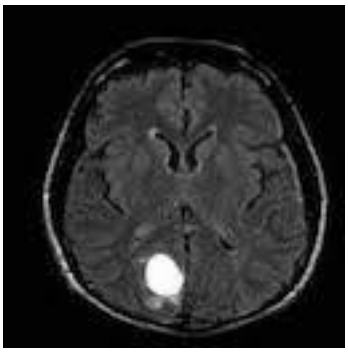
Stego Images 15 (Paul et al., 2020)

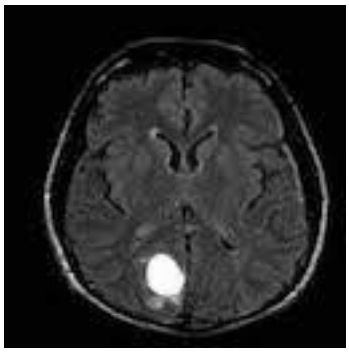


Stego Images 16 (Dhall & Gupta, 2021)



Stego Images 17 (Islam et al., 2014)





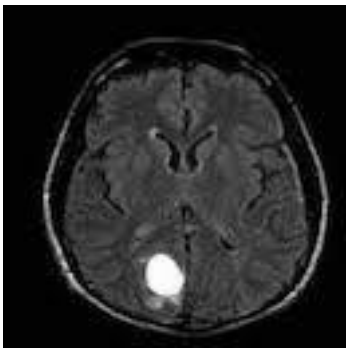


Figure 2: Perceptual Quality

As the results show, it is not easy to differentiate between all the images. This means most of the implemented mechanisms provide excellent visual quality. Several mechanisms, like (Jain et al., 2019) and (Dhall & Gupta, 2021), indicate the presence of secret information in the cover image. The amount of information to be stored also impacts the image's perceptibility**.**

Figure 4, on the other hand, shows noise attack analysis by evaluating and comparing the respective values of diverse algorithms.

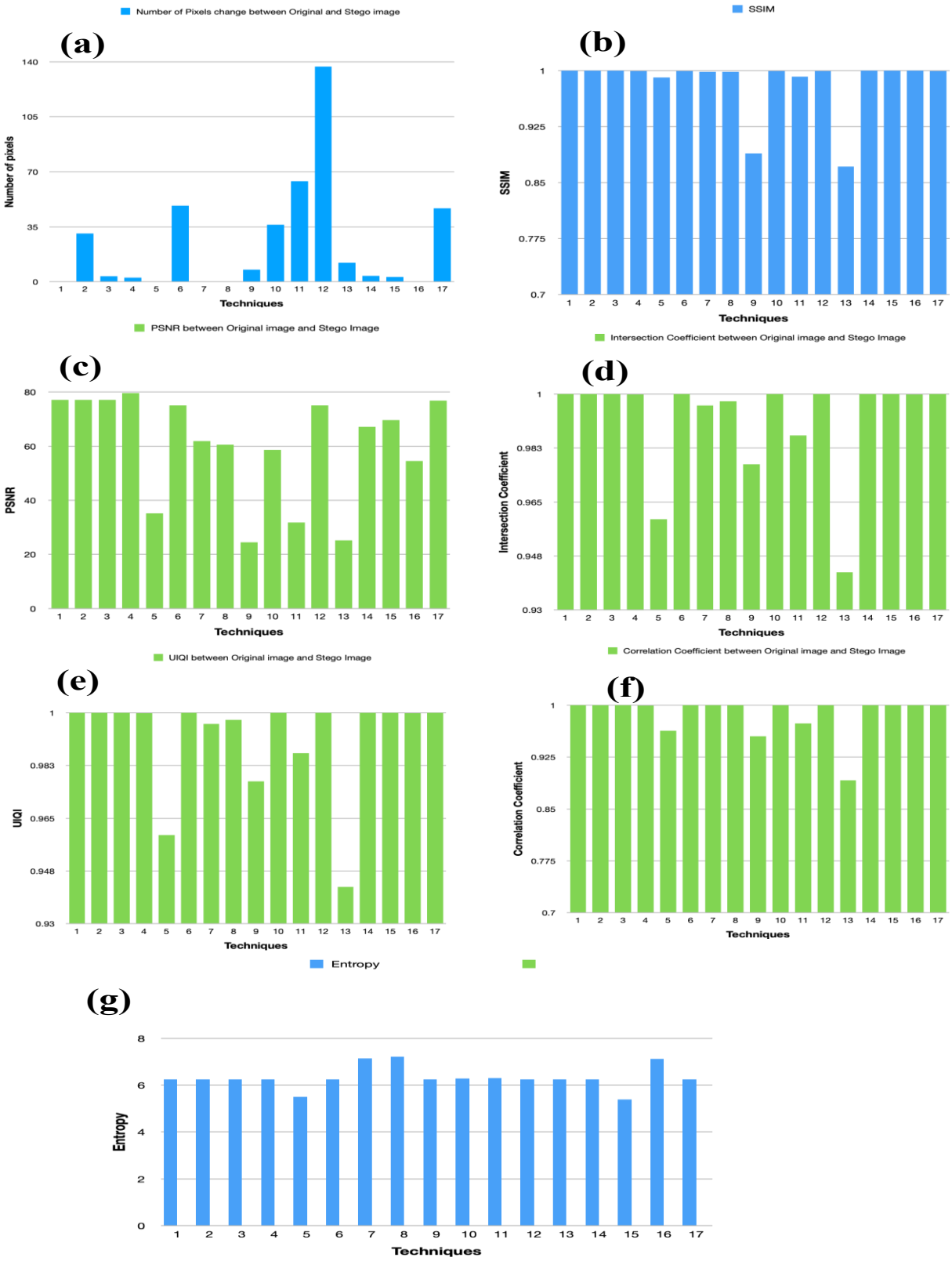


Figure 3: Results of Quantitative Security Analysis: (a) Number of pixels change between Original and Stego- Image; (b) Structural Similarity Index; (c) Peak Signal-to-Noise Ratio; (d) Intersection Coefficient; (e) Universal Image Quality Index; (f) Correlation Coefficient; (g) Entropy

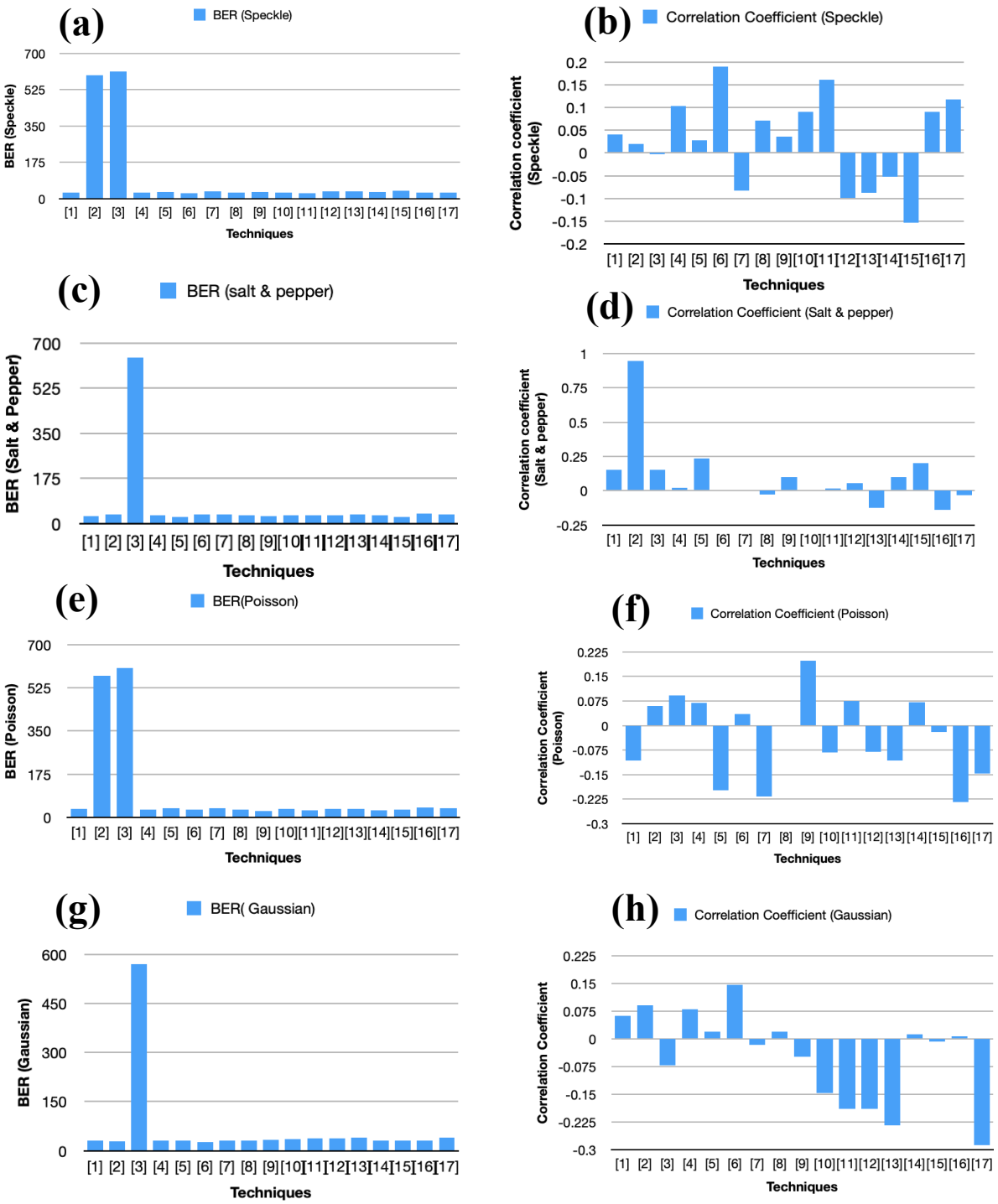


Figure 4: Robustness Analysis (a) BER for Speckle noise; (b) Correlation Coefficient for Speckle noise; (c) BER for Salt & Pepper; (d) Correlation Coefficient for Salt & Pepper; (e) BER for Poisson; (f) Correlation Coefficient for Poisson; (g) BER for Gaussian; (h) Correlation Coefficient for Gaussian

Figure 4 shows the attack results. From the Figures, it can be observed that the impact of all the noises on the Melenli & Topkaya, 2020 and Mihalj et al., 2020 proposals is quite significant in comparison to others due to the employment of the most straightforward spatial domain steganography technique (LSB) and traditional encryption schemes.

Execution Time Analysis: Time restrictions are very prominent in many data communication and security applications, so prompt data is required for further action. That is why all the implemented mechanisms are compared based on execution time requirements.

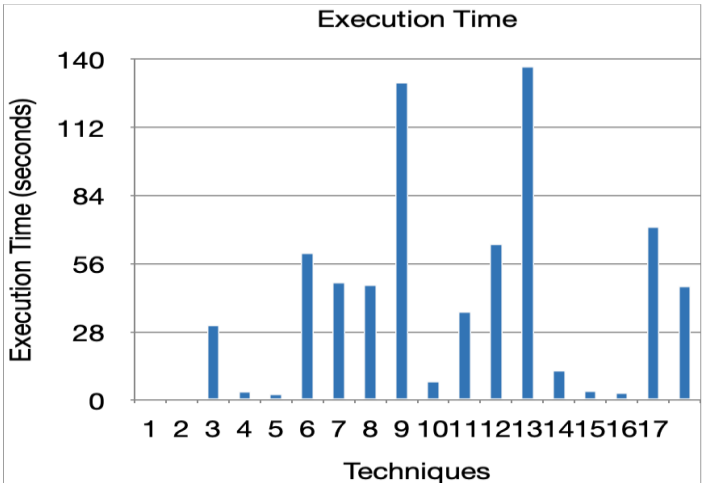


Figure 5: Execution Time (in seconds)

Figure 5 shows the execution time results. Elowen, M. et al. (Elhoseny et al., 2018) and Tauhid, A. (Rawat et al., 2018) show high execution time due to the employment of multiple levels of encryption techniques. At the same time, Nivedhitha, R. takes the least time due to the employment of LSB and 64-bit DES encryption.

6. Conclusion

This paper analyzes various multilevel security mechanisms in terms of Qualitative, Quantitative Robustness Analysis and Execution time. From all the above results obtained experimentally, the following inferences can be drawn:

- The technique proposed by Paul (Paul et al., 2020) is the best in terms of Quantitative analysis and execution time. Also, it is robust against various noise attacks
- The technique proposed by Tauhid (Tauhid et al., 2019) is the most fragile among all in terms of Quantitative parameters
- The technique proposed by Nain (Nain et al., 2013) is not resistant to noise attacks
- Since the execution time of technique proposed by Rawat (Rawat et al., 2018) is very high, it is not recommended for real-life usage.

References

Abd El-Latif, A. A., Li, L., Wang, N., Han, Q., & Niu, X. (2013). A new approach to chaotic image encryption based on a quantum chaotic system, exploiting color spaces. *Signal Processing, 93*(11), 2986–3000. https://doi.org/10.1016/j.sigpro.2013.03.031

Akhshani, A., Akhavan, A., Lim, S.-C., & Hassan, Z. (2012). An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation, 17*(12), 4653–4661. https://doi.org/10.1016/j.cnsns.2012.05.033

Almuhammadi, S., & Al-Shaaby, A. (2017). A survey on recent approaches combining cryptography and steganography. *Computer Science & Information Technology (CS & IT)*.

Baby, A., & Krishnan, H. (2017). Combined strength of steganography and cryptography—A literature survey. *International Journal of Advanced Research in Computer Science, 8*(3).

Banharnsakun, A. (2018). Artificial bee colony approach for enhancing LSB-based image steganography. *Multimedia Tools and Applications, 77*(20), 27491–27504.

Bansal, R., Hediayti, A., Aggrawal, J., Sorlan, B., & Gupta, S. (2016). Comparison of hybrid security schemes: A survey. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 9*(8), 169–180.

Bansal, R., Nagpal, C. K., & Gupta, S. (2018). An efficient hybrid security mechanism based on chaos and improved BPCS. *Multimedia Tools and Applications, 77*(6), 6799–6835.

Chaudhary, D., Gupta, S., & Deswal, S. (2015). Origin of hybrid security mechanisms and ways of improvement. *International Journal of Big Data Security and Intelligence*.

Chauhan, B., Dhall, S., & Gupta, S. (2015). A comparison of various hashing techniques. *International Journal of Computer Networks and Applications, 2*(6).

Dhall, S., Bhushan, B., & Gupta, S. (2016). An improved hybrid mechanism for secure data communication. *International Journal of Computer Network and Information Security, 8*(6), 67.

Dhall, S., & Gupta, S. (2021). Multilayered highly secure authentic watermarking mechanism for medical applications. *Multimedia Tools and Applications, 80*(12), 18069–18105. https://doi.org/10.1007/s11042-021-10531-w

Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access, 6*, 20596–20608.

El-Zoghdy, S. F., Nada, Y. A., & Abdo, A. A. (2011). How good is the DES algorithm in image ciphering. *International Journal of Advanced Networking and Applications, 2*(5), 796–803.

François, M., Grosges, T., Barchiesi, D., & Erra, R. (2012). A new image encryption scheme based on a chaotic function. *Signal Processing: Image Communication, 27*(3), 249–259. https://doi.org/10.1016/j.image.2011.11.003

Gao, X., Yu, J., Chang, Y., Wang, H., & Fan, J. (2022). Checking only when it is necessary: Enabling integrity auditing based on the keyword with sensitive information privacy for encrypted cloud data. *IEEE Transactions on Dependable and Secure Computing, 19*(6), 3774–3789. https://doi.org/10.1109/TDSC.2021.3106780

Gupta, S., Goyal, A., & Bhushan, B. (2012). Information hiding using least significant bit steganography and cryptography. *International Journal of Modern Education and Computer Science, 4*(6), 27.

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors International, 2*, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Hu, D., Zhang, Y., Yu, C., Wang, J., & Wang, Y. (2022). *Image steganography based on style transfer*. arXiv. https://doi.org/10.48550/arXiv.2203.04500

Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014). An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography. In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)* (pp. 1–6). IEEE.

Jain, Y., Dhall, S., & Gupta, S. (2019). A robust multilevel security mechanism against geometric attacks. In *2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)* (pp. 220–226). IEEE.

Jain, Y., Sharma, G., Anand, G., & Dhall, S. (2018). A hybrid security mechanism based on DCT and visual cryptography for data communication networks. In *Cyber security* (pp. 131–142). Springer.

Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2021). Double layer security using crypto-stego techniques: A comprehensive review. *Health and Technology*, 1–23.

Joseph Raphael, A., & Sundaram, V. (2010). Cryptography and steganography—A survey. *International Journal of Computer and Technology Applications, 2*(3), 626–630.

Khalifa, A., & Guzman, A. (2022). Imperceptible image steganography using symmetry-adapted deep learning techniques. *Symmetry, 14*(7), 1325. https://doi.org/10.3390/sym14071325

Khandelwal, J., Sharma, V. K., Singh, D., & Zaguia, A. (2022). DWT-SVD-based image steganography using threshold value encryption method. *Computers, Materials & Continua, 72*(2), 3299–3312. https://doi.org/10.32604/cmc.2022.023116

Khandhar. (n.d.). *Telemedicine*

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making, 20*(1), 106. https://doi.org/10.1186/s12911-020-01145-7

Kumari, M., & Gupta, S. (2021). Performance comparison between chaos and quantum-chaos based image encryption techniques. *Multimedia Tools and Applications, 80*, 33213–33255. https://doi.org/10.1007/s11042-021-11178-3

Li, Y.-H., Wang, C.-C., & Chen, C.-Y. (2022). Coverless image steganography using morphed face recognition based on convolutional neural network. *EURASIP Journal on Wireless Communications and Networking, 2022*, 28. https://doi.org/10.1186/s13638-022-02107-5

Liu, H., & Jin, C. (2017). A novel color image encryption algorithm based on quantum chaos sequence. *3D Research, 8*(1). https://doi.org/10.1007/s13319-016-0114-7

Maryoosh, A. A., Dhaief, Z. S., & Mustafa, R. A. (2021). Subject review: Information steganography based on different methods.

Melenli, S., & Topkaya, A. (2020). Real-time maintaining of social distance in COVID-19 environment using image processing and big data. In *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)* (pp. 1–5). IEEE. https://doi.org/10.1109/ASYU50717.2020.9259891

Mihalj, M., Carrel, T., Gregoric, I. D., Andereggen, L., Zinn, P. O., Doll, D., Stueber, F., Gabriel, R. A., Urman, R. D., & Luedi, M. M. (2020). Telemedicine for preoperative assessment during a COVID-19 pandemic: Recommendations for clinical care. *Best Practice & Research Clinical Anaesthesiology, 34*(2), 345–351.

Nain, A. K., Gupta, S., Bhushan, B., & Chawla, R. (2013). An adaptive pseudorandom STEGO-CRYPTO technique for data communication. *International Journal of Computer Networks and Communications, 5*, 173–188.

Nezami, Z. I., Jamzad, M., & Rezaei, M. (2022). An efficient and secure technique for image steganography using a hash function. *PeerJ Computer Science, 8*, e1157. https://doi.org/10.7717/peerj-cs.1157

Nivedhitha, R., Meyyappan, D. T., & Phil, M. (2012). Image security using steganography and cryptographic techniques. *International Journal of Engineering Trends and Technology, 3*(3), 366–371.

Patil, A., Mulik, S., Pathak, P., & Raut, K. (2021). Review paper on data security using cryptography and steganography. *VIVA-Tech International Journal for Research and Innovation, 1*(4), 1–6.

Paul, G., Saha, S. K., & Burman, D. (2020). A PVD-based high-capacity steganography algorithm with embedding in non-sequential position. *Multimedia Tools and Applications, 79*(19), 13449–13479.

Priya, S., & Santhi, B. (2019). A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-019-01213-x

Rahmani, M. K. I., Arora, K., & Pal, N. (2014). A crypto-steganography: A survey. *International Journal of Advanced Computer Science and Applications, 5*(7).

Rawat, P., Gupta, N., & Dagar, S. (2018). Data security by a hybrid mechanism. *International Journal of Advanced Research in Computer and Communication Engineering*, 144–151.

Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In R. Anderson (Ed.), *Fast software encryption: FSE 1993*. Springer.

Singh, A. K., Kumar, B., Dave, M., & Mohan, A. (2015). Robust and imperceptible dual watermarking for telemedicine applications. *Wireless Personal Communications, 80*, 1415–1433. https://doi.org/10.1007/s11277-014-2091-6

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of steganography and cryptography: A short survey. *IOP Conference Series: Materials Science and Engineering, 518*(5), 052003.

Tayal, N., Bansal, R., Dhal, S., & Gupta, S. (2017). A novel hybrid security mechanism for data communication networks. *Multimedia Tools and Applications, 76*(22), 24063–24090.

Tayal, N., Dhall, S., & Gupta, S. (2016). A robust hybrid steganography mechanism for security in data communication networks. *International Journal of Computer Networks and Applications, 3*(3).

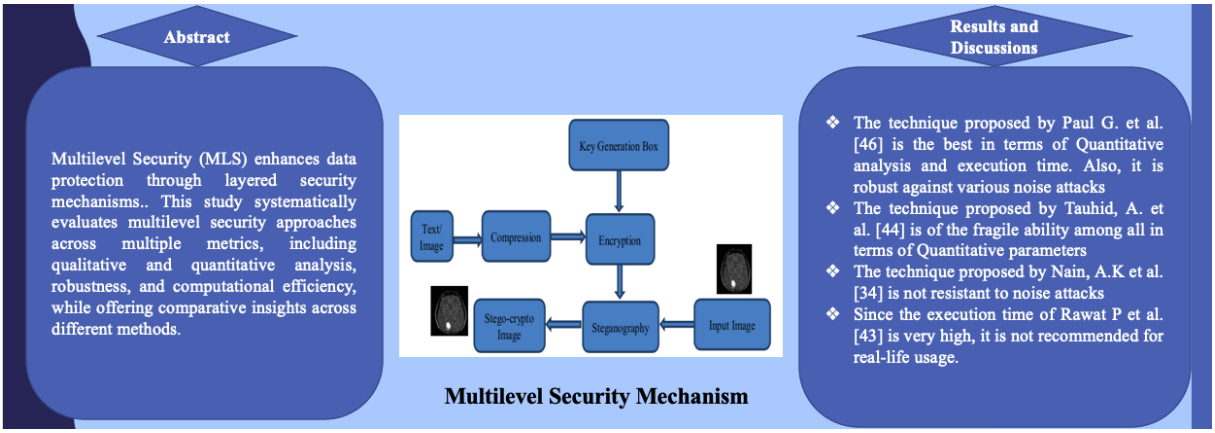
Tauhid, A., Tasnim, M., Noor, S. A., Faruqui, N., & Yousuf, M. A. (2019). A secure image steganography using advanced encryption standard and discrete cosine transform. *Journal of Information Security, 10*(3), 117–129.

Wajgade, V. M., & Kumar, S. (2013). Stegocrypto—A review of steganography techniques using cryptography. *International Journal of Computer Science & Engineering Technology, 4*, 423–426.

Yan, Y., & Dong, Z. (2000). An approach to integer wavelet transform for medical image compression in PACS. *Wuhan University Journal of Natural Sciences, 5*, 204–206. https://doi.org/10.1007/BF02827928

Zhang, X., Liu, Y., & Han, J. (2022). Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage. *Entropy, 24*(2), 246. https://doi.org/10.3390/e24020246

Graphical Abstract





Vyoma Vaish is a PhD Scholar in the Interdisciplinary Department at J.C. Bose University of Science and Technology, YMCA, Faridabad. Her research interests span the domains of Life Sciences and Computer Engineering, with a special focus on Cryptography, Image Security, Medical Image Encryption, and Cybersecurity applications. She is actively engaged in interdisciplinary research integrating advanced computational techniques with scientific and healthcare applications. Her work reflects a strong inclination toward innovative and secure solutions in emerging technological fields.



Dr. Kakoli Dutt is an Associate Professor and Chairperson of the Department of Life Sciences at J.C. Bose University of Science and Technology, YMCA, Faridabad. She has extensive expertise in the field of Life Sciences and has contributed significantly to academic research through numerous research publications in reputed journals. With rich teaching and research experience, she is actively involved in guiding students and promoting scientific innovation in the domain of biological sciences.



Dr. Ashutosh Dixit is Professor and Chairman of the Department of Computer Engineering and Dean of the Faculty of Management Studies at J.C. Bose University of Science and Technology, YMCA, Faridabad. With over 21 years of academic experience, he has published more than 85 research papers and supervised 9 PhD scholars. He has also held several key administrative positions, including Dean of Academic Affairs and Director of IQAC. Dr. Dixit has completed an AICTE-funded research project and secured two national and one international patent. His research areas include Machine Learning, Web Technologies, Computer Networks, and Mobile Communications.