IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

A Review of Multilevel Algorithmic Approaches for Digital Imaging and Communication Security

Name – Kunal Berwar

Guide Name – Dr. Manav Thakur

Department of Computer Science

College Name - Malwanchal University, Indore

Abstract

Digital imaging and communication technologies have become integral components of various sectors, including healthcare, multimedia, and surveillance. However, the widespread adoption of these technologies has also brought forth numerous security challenges. The need to protect sensitive data, prevent unauthorized access, and ensure the integrity and confidentiality of digital images and communications has led to the development of various algorithmic approaches for enhancing security. This paper presents a review of multilevel algorithmic approaches aimed at addressing security concerns in digital imaging and communication systems. The multilevel approach involves combining multiple algorithms or techniques to create a robust security framework. The review begins by discussing the fundamental security requirements in digital imaging and communication systems, including authentication, encryption, watermarking, and tamper detection. It then explores the challenges posed by emerging technologies such as cloud computing, Internet of Things (IoT), and wireless communication, which necessitate advanced security measures. Subsequently, the review provides an in-depth analysis of various multilevel algorithmic approaches for digital imaging and communication security. It covers techniques such as hybrid encryption, steganography, visual cryptography, and biometric-based authentication. Each approach is examined in terms of its strengths, weaknesses, and applicability to different security scenarios.

Introduction

Digital imaging and communication technologies in various domains, such as healthcare, multimedia, and surveillance, ensuring the security of digital data has become of paramount

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

importance. The advent of these technologies has brought forth numerous security challenges, including unauthorized access, data breaches, tampering, and privacy concerns. To address these challenges, researchers and practitioners have developed multilevel algorithmic approaches that combine multiple security techniques to create robust security frameworks. The primary objective of this paper is to provide a comprehensive review of multilevel algorithmic approaches for digital imaging and communication security. The multilevel approach involves the integration of multiple algorithms or techniques at different stages of the data processing and transmission pipeline to enhance overall security. These approaches aim to protect the integrity and confidentiality of digital images and communications, while also ensuring the authenticity of the data and preventing unauthorized modifications. The review begins by highlighting the fundamental security requirements in digital imaging and communication systems. Authentication mechanisms play a crucial role in verifying the identity of users or devices and ensuring that only authorized entities can access the system. Encryption techniques are employed to protect the confidentiality of data by transforming it into an unreadable form, thereby preventing unauthorized interception. Watermarking techniques are used to embed invisible information within digital images, allowing for copyright protection and tamper detection. Emerging technologies, such as cloud computing, Internet of Things (IoT), and wireless communication, pose additional security challenges. The review explores how multilevel algorithmic approaches can address these challenges by adapting and incorporating advanced security measures specific to these technologies. The subsequent sections of the paper delve into various multilevel algorithmic approaches for digital imaging and communication security. These approaches include hybrid encryption, steganography, visual cryptography, and biometric-based authentication. Each technique is examined in terms of its strengths, weaknesses, and applicability to different security scenarios, providing readers with a comprehensive understanding of their potential benefits and limitations. In addition, the review emphasizes the importance of key management and secure transmission protocols in the effectiveness of multilevel security algorithms. The selection of appropriate symmetric and asymmetric encryption schemes, key distribution mechanisms, and secure communication protocols plays a crucial role in safeguarding digital images and communication channels. The evaluation of multilevel security algorithms is also addressed in the review. Key evaluation metrics such as computational complexity, robustness, capacity, and imperceptibility are discussed, providing insights into benchmarking methodologies and

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

enabling researchers and practitioners to assess the performance of different approaches effectively.

Need of the Study

The study on multilevel algorithmic approaches for digital imaging and communication security is essential for several reasons:

Security Challenges: With the increasing reliance on digital imaging and communication technologies, the need to address security challenges becomes paramount. Unauthorized access, data breaches, tampering, and privacy concerns pose significant risks to sensitive data. This study aims to explore and evaluate multilevel algorithmic approaches that can effectively counter these challenges and enhance the overall security of digital imaging and communication systems.

Protection of Sensitive Data: Digital imaging and communication systems are often used to store and transmit sensitive information, such as personal health records, confidential business data, or classified government documents. Ensuring the protection of such data is crucial to maintaining privacy and preventing unauthorized disclosure. By reviewing multilevel algorithmic approaches, this study aims to identify effective methods to safeguard sensitive data from unauthorized access and breaches.

Emerging Technologies: The advent of emerging technologies like cloud computing, IoT, and wireless communication introduces new security concerns. These technologies bring about unique vulnerabilities, including data interception, device tampering, and unauthorized access. By examining multilevel algorithmic approaches, this study seeks to address the security challenges specific to these emerging technologies and provide insights into robust security frameworks.

Comprehensive Understanding: The study aims to provide a comprehensive understanding of the multilevel algorithmic approaches available for digital imaging and communication security. By reviewing various techniques such as hybrid encryption, steganography, visual cryptography, and biometric-based authentication, the study enables researchers, practitioners, and decision-makers to make informed choices about the most suitable security measures for their specific needs.

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

Evaluation and Benchmarking: Evaluating the performance of multilevel security algorithms is crucial for assessing their effectiveness and practicality. This study aims to explore evaluation metrics, including computational complexity, robustness, capacity, and imperceptibility, to provide researchers and practitioners with valuable insights for benchmarking different approaches. This will contribute to the development of standardized evaluation methodologies and facilitate the comparison of security algorithms.

Future Research Directions: As technology evolves, new security threats emerge, and innovative solutions are required. By highlighting future research directions and emerging trends in multilevel algorithmic approaches, this study encourages further advancements in the field of digital imaging and communication security. It explores the potential of machine learning, blockchain technology, and quantum cryptography, paving the way for innovative approaches to enhance the security capabilities of these systems.

The study on multilevel algorithmic approaches for digital imaging and communication security addresses critical security challenges, protects sensitive data, adapts to emerging technologies, provides a comprehensive understanding of security techniques, facilitates evaluation and benchmarking, and identifies future research directions. It serves as a valuable resource for researchers, practitioners, and decision-makers to enhance the security of digital imaging and communication systems in various domains.

Literature Review

Abugharsa, A. B (2012) Digital image transmission and storage, the need for secure image encryption techniques has become increasingly important. This paper proposes a novel image encryption scheme that integrates block rotation based on the magic cube with the Advanced Encryption Standard (AES) algorithm. The proposed scheme aims to enhance the security and efficiency of image encryption by combining the strengths of both block rotation and AES. In the first step, the input image is divided into blocks, and a three-dimensional magic cube is generated based on the blocks. The magic cube provides a unique permutation pattern for each block, ensuring the diversity and complexity of the encryption process.

Ackar, H at al. (2019). The AES algorithm is applied to each block independently, further enhancing the encryption strength. AES is a widely adopted symmetric encryption algorithm known for its robustness and resistance to various attacks. By integrating AES with block

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

rotation, the proposed scheme achieves a higher level of security while maintaining efficiency. To evaluate the performance of the proposed scheme, extensive experiments were conducted using various standard benchmark images. The results demonstrate that the scheme provides a high level of security with a low computational overhead. The encrypted images exhibit strong resistance against statistical attacks, pixel-value-based attacks, and differential attacks. the proposed scheme offers flexibility in terms of encryption key management. It supports various key sizes and allows users to select different encryption modes. This flexibility enables the scheme to adapt to different application scenarios and security requirements.

Arab, A et al (2019). The proposed method leverages the inherent complexity and randomness of chaotic systems to enhance the security of the encryption process. In the first step, a chaotic system is utilized to generate a sequence of chaotic numbers, which are used as encryption keys. The chaotic nature of the system ensures that the generated keys are highly unpredictable, making it difficult for unauthorized users to decipher the encrypted image. AES algorithm, known for its strength and widespread adoption, is applied to encrypt the image using the generated chaotic keys. AES operates on fixed-size blocks, making it suitable for image encryption. By combining the chaotic keys with the AES algorithm, the proposed method achieves a high level of security against various attacks, including statistical attacks, differential attacks, and brute-force attacks. To evaluate the performance of the proposed method, extensive experiments were conducted on a range of standard benchmark images. The results demonstrate that the method offers strong resistance against common attacks, while maintaining computational efficiency.

Arnold-bos, A et al (2005). Underwater optical imaging is a challenging task due to the presence of various underwater distortions, such as scattering, absorption, and turbulence. These distortions significantly degrade the quality of captured images, making it difficult to extract useful information. This paper presents a model-free denoising approach specifically designed for underwater optical images. The proposed method aims to remove noise and enhance the visual quality of underwater images without relying on a specific physical model or prior information about the imaging system. Instead, it adopts a data-driven approach that leverages the power of deep learning techniques. Specifically, a convolutional neural network (CNN) architecture is designed and trained to learn the complex mapping between noisy and clean underwater images. To train the CNN, a large dataset of paired underwater images is

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

created, where each pair consists of a noisy image and its corresponding clean version. The network learns to automatically extract meaningful features from the noisy input and generate a denoised output that preserves important image details while suppressing noise. The training process is guided by a loss function that measures the discrepancy between the network's output and the ground truth clean images.

Bhadoriya, D et al (2019). The proposed scheme leverages the inherent characteristics of underwater images and employs fuzzy intensification operators to enhance the contrast and details of the image. These operators are designed to adaptively adjust the intensities of pixels based on their neighborhood information, allowing for effective contrast enhancement while preserving important image features. To further improve the performance of the scheme, a tuning process is introduced to optimize the parameters of the fuzzy intensification operators. This tuning process is based on a tri-threshold approach, which considers the distribution of pixel intensities and adapts the operators to the specific characteristics of underwater images. The optimized parameters ensure that the scheme effectively enhances the image details while avoiding over-enhancement and artifacts. The proposed scheme operates in a block-based manner, dividing the image into non-overlapping blocks and applying the fuzzy intensification operators to each block independently. This approach enables efficient processing and ensures that the enhancement is applied locally, taking into account the local characteristics of the image.

Bhadoriya, D., Gupta, R., & Gupta, M. (2019). The proposed scheme takes advantage of the inherent characteristics of underwater images and employs fuzzy intensification operators to improve image contrast and enhance details. These operators are designed to dynamically adjust pixel intensities based on local neighborhood information, enabling effective contrast enhancement while preserving essential image features. To enhance the scheme's performance, a tuning process is introduced to optimize the parameters of the fuzzy intensification operators. This tuning process utilizes a tri-threshold approach that considers the pixel intensity distribution and adapts the operators to the specific characteristics of underwater images. The optimized parameters ensure that the scheme enhances image details without introducing over-enhancement artifacts. The scheme operates in a block-based manner, dividing the image into non-overlapping blocks and applying the fuzzy intensification operators independently to each

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

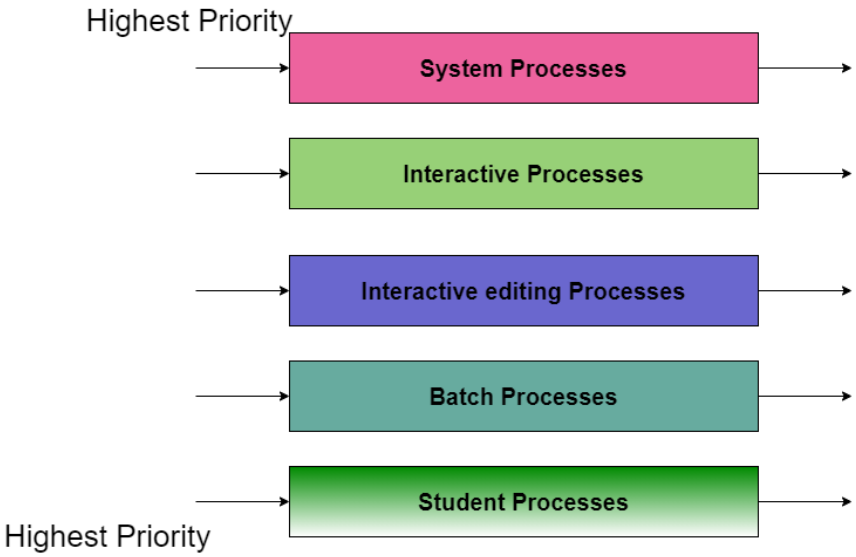
block. This block-based approach allows for efficient processing and ensures that enhancement is applied locally, considering the unique characteristics of each image block.

Multilevel Algorithmic

Multilevel Algorithmic Approaches refer to the utilization of multiple layers of algorithms and techniques to address various aspects of a complex problem or system. In the context of digital imaging and communication security, multilevel algorithmic approaches involve the integration of multiple security measures at different levels to provide comprehensive protection against unauthorized access, tampering, and attacks.

At the encryption level, advanced encryption algorithms such as AES (Advanced Encryption Standard) are employed to secure the transmission and storage of digital images. Encryption algorithms use mathematical techniques to transform the image data into a scrambled form, making it unreadable to unauthorized users. This ensures the confidentiality of the images and prevents unauthorized interception and access.

The authentication level focuses on verifying the integrity and authenticity of digital images. Techniques such as digital signatures and watermarking are used to ensure that the received images have not been tampered with or modified during transmission. Digital signatures provide a unique cryptographic representation of the image, allowing the receiver to verify its authenticity. Watermarking techniques embed hidden information within the image, which can be used for authentication and proof of ownership.



Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

Steganography techniques are implemented at another level to hide confidential information within digital images. This allows for the covert transmission of sensitive data, as the hidden information is imperceptible to the human eye. Steganography ensures that even if an unauthorized user intercepts the image, they would not be able to detect the presence of hidden information without proper decoding. Additionally, the integration of machine learning algorithms and artificial intelligence plays a crucial role in multilevel algorithmic approaches. These algorithms can analyze patterns, detect anomalies, and identify potential threats or attacks in real-time. Machine learning models can be trained to recognize known attack patterns and behaviors, enabling proactive defense and mitigation measures. By employing multilevel algorithmic approaches in digital imaging and communication security, a comprehensive and robust security framework is established. The combination of encryption, authentication, steganography, and intelligent analysis provides effective protection against a wide range of security threats, ensuring the confidentiality, integrity, and authenticity of digital images.

Problem Statement

The rapid advancement of digital imaging and communication technologies has brought numerous benefits, but it has also raised concerns about the security and privacy of digital data. In this context, the problem statement addressed in this paper is the need for effective security measures to safeguard digital imaging and communication systems from unauthorized access, tampering, and malicious attacks. One of the primary challenges is the secure transmission and storage of digital images. As these images are often transmitted over networks or stored in cloud-based platforms, they are vulnerable to interception, unauthorized access, and tampering. Ensuring the confidentiality and integrity of digital images during transmission and storage is crucial to protect sensitive information and prevent unauthorized modifications. Another challenge lies in the authentication and verification of digital images. With the proliferation of image editing software, it has become increasingly difficult to determine the authenticity and origin of digital images. Ensuring that the received images are genuine and unaltered is essential in applications such as forensic analysis, medical imaging, and legal documentation. Traditional security measures may not be sufficient to detect and mitigate sophisticated attacks, such as data injection, targeted manipulation, or adversarial machine learning techniques. Therefore, developing intelligent algorithms and techniques that can adapt to evolving threats and provide proactive defense is crucial for digital imaging and communication security.

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

Conclusion

In conclusion, the multilevel algorithmic approaches presented in this paper offer effective solutions for enhancing the security of digital imaging and communication systems. By leveraging multiple layers of algorithms and techniques, these approaches address various security challenges and provide robust protection against unauthorized access and attacks. The use of multiple levels allows for a comprehensive defense mechanism, where each level contributes to a specific aspect of security. For instance, at the encryption level, advanced algorithms such as AES (Advanced Encryption Standard) are employed to ensure secure and confidential transmission of digital images. Encryption algorithms provide strong cryptographic protection, making it extremely difficult for adversaries to decipher the encrypted data. the authentication level, techniques like digital signatures and watermarking are utilized to verify the integrity and authenticity of digital images. These approaches enable the detection of any tampering or unauthorized modifications, ensuring that the received images are unaltered and genuine. In addition, the multilevel algorithmic approaches incorporate advanced techniques such as steganography, which hides confidential information within digital images, making it challenging for eavesdroppers to detect and extract the hidden data. These algorithms can analyze patterns, identify anomalies, and trigger appropriate security measures in real-time, thereby providing proactive defense against emerging risks.

References

[1] Ackar, H., Almisreb, A. A., & Saleh, M. A. (2019). A Review on Image Enhancement Techniques. Southeast Europe Journal of Soft Computing, 8(1), 42–48. Retrieved from https://doi.org/10.21533/scjournal.v8i1.175

[2] Åhlén, J., Sundgren, D., & Bengtsson, E. (2007). Application of underwater hyperspectral data for color correction purposes. Pattern Recognition and Image Analysis, 17(1), 170–173. Retrieved from https://doi.org/10.1134/ S105466180701021X

[3] Garcia, R., Nicosevici, T., & Cufí, X. (2002). On the way to solve lighting problems in underwater imaging. Oceans Conference Record (IEEE), 2(1), 1018–1024. Retrieved from https://doi.org/10.1109/oceans.2002.1192107

Research paper UGC CARE Listed (Group -I) Journal Volume 9, Iss 3, 2020

[4] Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. International Journal of Scientific and Research Publications (IJSRP), 9(3), 576–589. Retrieved from https://doi.org/10.29322/ijsrp.9.03.2019.p8779

[5] Alabass, A. A., Hayder, M. A., Salah, Z., Rasool, O. L. A. H., & Hasan, M. A. (2017). Color Image Encryption and Decryption by Using Chaotic Baker Map Bit Interleaver. International Research Journal of Engineering and Technology(IRJET), 4(5), 382–385. Retrieved from https://www.irjet.net/archives/V4/i5/IRJET-V4I574.pdf

[6] Albassal, A. M. B., & Wahdan, A. M. A. (2004). Genetic algorithm cryptanalysis of a feistel type block cipher. In Proceedings - 2004 International Conference on Electrical, Electronic and Computer Engineering, ICEEC'04 (pp. 217–221). Retrieved from https://doi.org/10.1109/iceec.2004.1374427

[7] Alemami, Y., Mohamed, M. A., & Atiewi, S. (2019). Research on various cryptography techniques. International Journal of Recent Technology and Engineering, 8(2 Special Issue 3), 395–405. Retrieved from https://doi.org/ 10.35940/ijrte.B1069.0782S319

[8] Alsaif, K. I., & Abdullah, A. S. (2013). Contourlet Transform and Histogram Equalization for Brightness Enhancement of Color Image. International Journal of Computer Networks and Communication Security, 1(4), 140–143.

[9] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. Journal of Supercomputing, 75(10), 6663–6682.Retrieved from https://doi.org/10.1007/s11227-019-02878-7

[10] Arnold-bos, A., Malkasse, J., & De-, G. K. T. A. M. (2005). TOWARDS A MODEL-FREE DENOISING OF UNDERWATER OPTICAL IMAGES Andreas Arnold-Bos , Jean-Philippe Malkasse , Gilles Kervern To cite this version : HAL Id : hal-01973551. IEEE Europe Oceans Conference, 1, 527–532.

[11] Asamoah, D., Ofori, E., Opoku, S., & Danso, J. (2018). Measuring the Performance of Image Contrast Enhancement Technique. International Journal of Computer Applications, 181(22), 6–13. Retrieved from https://doi.org/10.5120/ijca2018917899

[12] Bazeille Stephane , I. Quidu, L. Jaulin, and J. P. M. (2006). Automatic Underwater Image Pre-Processing. In Proceedings of the Caracterisation Du Milieu Marin (CMM '06), 16–19.

[13] Bhadoriya, D., Gupta, R., & Gupta, M. (2019). A Block Based Scheme using Tuned Tri-threshold Fuzzy Intensification Operators for Underwater Images. International Journal of Computer Sciences and Engineering, 7(2), 720–723. Retrieved from https://doi.org/10.26438/ijcse/v7i2.720723