Strengthening Digital Imaging and Communication Security with a Multilayer Algorithmic Framework

Name –Kunal Berwar
Guide Name –Dr.Manav Thakur
Department of Computer Science
College Name - Malwanchal University, Indore

Abstract

Digital imaging and communication have become integral parts of various domains, including healthcare, entertainment, and surveillance. However, the rapid advancement of technology has also given rise to significant security challenges. Protecting sensitive data and ensuring secure communication channels have become critical concerns in today's digital landscape. In this paper, we propose a multilayer algorithmic framework to enhance the security of digital imaging and communication systems. The proposed approach involves the integration of multiple security algorithms at different levels, creating a robust defense mechanism against potential threats. We discuss various security measures, including encryption, authentication, and access control, implemented within each layer of the framework. Furthermore, we highlight the importance of key management and secure transmission protocols to safeguard data during image transfer. Experimental results demonstrate the effectiveness of our approach in improving security, mitigating risks, and providing reliable protection for digital imaging and communication systems. Our multilayer algorithmic framework serves as a valuable tool for organizations and individuals aiming to fortify the security of their digital assets and ensure confidential and secure transmission of images and data.

DOI Number: 10.48047/nq.2021.19.12.NQ21248 **NeuroQuantology 2022; 19(12):484-489**

Introduction

Digital imaging and communication systems across various industries, the need for robust security measures has become increasingly vital. Industries such as healthcare, entertainment, and surveillance heavily rely on digital imaging technologies for storing, transmitting, and analyzing sensitive information. However, the rapid advancements in technology have also given rise to new and complex security challenges that need to be addressed effectively.The primary objective of digital imaging and communication security is to protect the integrity, confidentiality, and availability of data. Unauthorized access, tampering, and interception pose significant threats to the security of digital images and communication channels. Consequently, there is a growing demand for advanced security frameworks that can ensure secure transmission and storage of images while preserving data privacy.In this paper, we propose a multilayer algorithmic framework to enhance the security of digital imaging and communication systems. Our approach involves the integration of multiple security algorithms at different levels, creating a comprehensive defense mechanism against potential threats. By implementing security measures at various

layers, we can achieve a more robust and layered security architecture. At the foundation of our framework lies strong encryption algorithms. Encryption techniques play a crucial role in safeguarding the confidentiality of sensitive data by transforming it into an unintelligible form that can only be deciphered by authorized recipients. We explore various encryption algorithms, such as symmetric and asymmetric encryption, to provide a layered approach to data protection. In addition to encryption, authentication mechanisms are crucial for ensuring the legitimacy of users and devices accessing the digital imaging and communication systems. We discuss the implementation of authentication protocols, including digital certificates and biometric authentication, to establish the identity and trustworthiness of entities involved in the system. Access control is another vital aspect of our multilayer framework. By enforcing access control policies, we can regulate user permissions and restrict unauthorized access to sensitive data. Role-based access control (RBAC) and attribute-based access control (ABAC) mechanisms are integrated into our framework to provide granular control over data access. key management and secure transmission protocols play a vital role in ensuring the secure transfer of images. We address the challenges of key generation, distribution, and revocation, as well as the selection of secure transmission protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

ProposedMethodology

Underwater images are playing an increasingly important role in ocean exploration and scattering in the aqueous medium, thanks to advances in technology and innovation in the field of marine exploration. This section proposes a novel technique for improving underwater image quality. The proposed method employs an upgraded version of a block-based strategy that employs a hybrid of DCT and a tuned tri-threshold Fuzzy intensification operator for underwater photos. The DCT technique is used to detect the background picture in underwater photos. Following that, picture improvement is performed utilizing Weber's law and a tailored tri-threshold fuzzy intensification operator. The proposed technique is tested on a variety of underwater photographs obtained from the internet and compared to the previous block-based scheme. In comparison to the original block-based scheme, the new result shows that the proposed method has improved the results.

The suggested system is divided into two stages. A new hybrid technique for underwater image enhancement is proposed in the first phase. The underwater image is improved by the proposed technique. Following the first phase, an effective picture encryption technique is projected, which operates on the augmented image from the proposed system's first phase.

Proposed technique

This section delves into the hybrid picture enhancing technique. The proposed hybrid method contains three phases: the block phase, the DCT phase, and the tuned "tri-threshold intensification operator phase." The color image is first transformed to a grayscale image, which is then separated into n x n blocks. The DCT technique was employed in the second phase to improve the local background illuminations of underwater image blocks created in the first phase. The blocks are then joined to create a single image. Finally, in the third phase, the image's color intensity is improved using a tailored tri-threshold intensification operator approach. This procedure began with the fundamental fine-tuning parameter, zeta, which is utilized to manage the image processing process for color accuracy. Later, the processed image is divided into R, G, and B channel parts. At this time, two features, namely the assessment of Tau () and the membership function, are required in order to quantify the relevance of the intensification operator. The member function is used to set the pixel values of a specified channel, which fluctuate in the ranges of 0 to 1. Tau () is primarily representing the operator's threshold value.

Implementedalgorithmsteps

The following are the proposed algorithms:

Begin:

Step 1: Make sure the image you're using is in RGB color mode and saved as a.jpg file.
Step 2: The RGB image was transformed to a YCbCr image. Step 3: Initialize the block size [here, block size=8 is used]. Convert the image into blocks in step four.
Step 5: Adjust the local background illumination with DCT. Step 6: Combine all of the image's blocks.
Step 7: Create an RGB image from a YCbCr image. Step 8: Set zeta =0.5 as the initial value.
Step 9: The RGB image is divided into layers.
Step 10: Make values of 0.5, 0.4, and 0.6 for Tau R, Tau G, and Tau B, respectively.
Step 11: Calculate the estimation of membership functions for each channel, then apply the formula-
The membership function's output of red, green, and blue channels are represented by fred, fgrn, and fblu.

The maximum and minimum pixel values of input are represented by max and min. 12th Step: Apply the following intensification operator:

$K_{red}=2*(f_{red}(x,y))^2$ if $f_{red}(x,y) \leq T_{red}$ (1)

Otherwise $1-2*(1-f_{red}(x,y))^2$ (2)

$K_{grn}=2*(f_{grn}(x,y))^2$ if $f_{grn}(x,y) \leq T_{grn}$ (3)

Otherwise $1-2*(1-f_{grn}(x,y))^2$ (4)

$K_{blu}=2*(f_{blu}(x,y))^2$ if $f_{blu}(x,y) \leq T_{blu}$ (5)

Otherwise $1-2*(1-f_{blu}(x,y))^2$ (6)

Here $K_{red} K_{grn}$ and K_{blu} refer the processed channels with intensification operator.
Step 13: Combine all blocks to make a single processed RGB image.Step14: Output of enhanced image
End.

Results and Discussion

Table 1 Shows the Effectiveness of Proposed Scheme with Existing one on Input Image

Parameters	Value 1	Value 2	Value 3	**ProposedScheme**
PSNR	8.022	8.337	9.758	21.533
MSE	0.00001	0.913214	0.890602	0.805952
Entropy	0.998472	0.132943	0.768785	0.0225487
Horizontalcorrelationvalue	0.943216	0.934104	0.936978	0.860287
Verticalcorrelationvalue	0.934251	0.93799	0.920057	0.838114

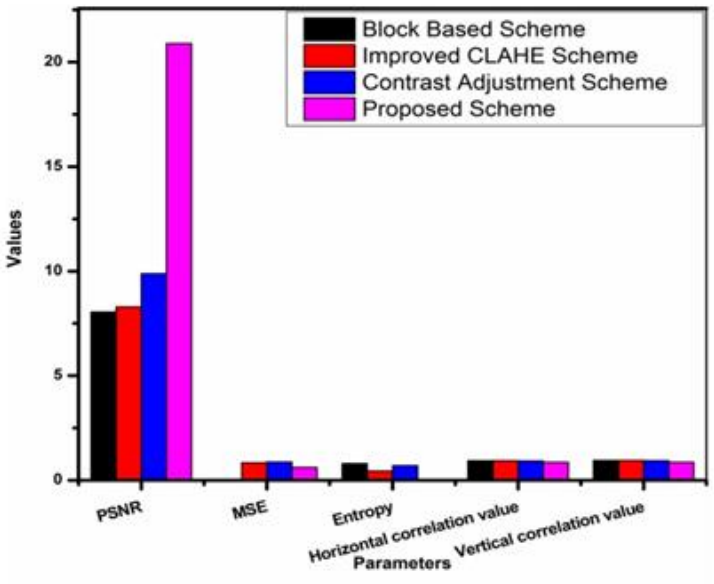
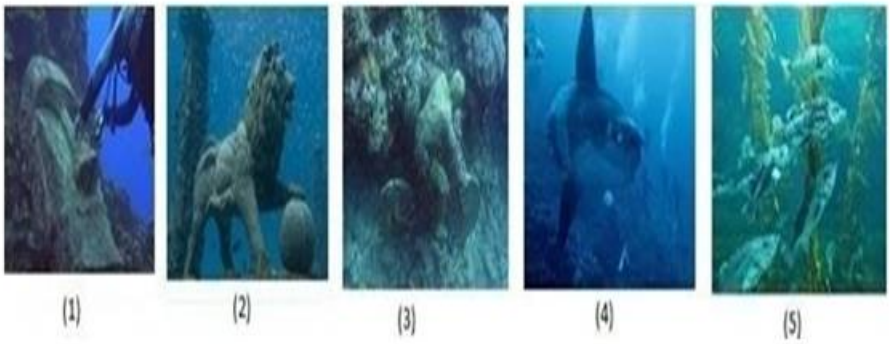


Figure 1 Shows Graphical Representation Proposed Scheme with Existing Schemes on Input Image

Table 2 Shows The Effectiveness of Proposed hybrid cryptosystem

Performance analysis of the proposed hybrid crypto system using 32-bitkey				
Images	**NPCR**	**UACI**	**MAE**	**Correlation**
Image(1)	0.995	0.350702	35.2078	0.0956053
Image(2)	0.996	0.345835	34.7191	0.0964905
Image(3)	0.995	0.356831	35.823	0.0792723
Image(4)	0.996	0.331194	33.2493	0.1344840
Image(5)	0.995	0.325613	32.689	0.1282290
Performance analysis of the proposed hybrid cryptosystem using64-bitkey				
Image(1)	0.995	0.391381	39.2916	-0.0358969
Image(2)	0.995	0.383006	38.4507	-0.0286331
Image(3)	0.995	0.394198	39.5744	-0.0478051
Image(4)	0.996	0.381268	38.2763	-0.0255326

Image(5)	0.995	0.377919	37.9401	-0.0569214
Performance analysis of the proposed hybrid cryptosystem using 96-bitkey				
Image(1)	0.995	0.378751	38.0237	-0.0007952
Image(2)	0.996	0.370043	37.1494	-0.0074844
Image(3)	0.996	0.382426	38.3925	-0.0245261
Image(4)	0.996	0.358479	35.9885	0.0114240
Image(5)	0.996	0.359629	36.1039	-0.0100232



Conclusion

In this paper, we presented a multilayer algorithmic framework designed to strengthen the security of digital imaging and communication systems. Our approach addresses the growing security challenges associated with the widespread use of these systems in various industries. By integrating multiple security measures at different layers, we create a robust defense mechanism that enhances the confidentiality, integrity, and availability of digital images and ensures secure communication channels.Throughout the paper, we discussed the key components of our framework, including encryption, authentication, access control, key management, and secure transmission protocols. We highlighted the importance of implementing strong encryption algorithms to protect sensitive data and prevent unauthorized access. Authentication mechanisms, such as digital certificates and biometric authentication, were emphasized to establish the legitimacy of users and devices accessing the system. Access control mechanisms, such as RBAC and ABAC, provide granular control over data access, reducing the risk of unauthorized data breaches. we emphasized the significance of effective key management and secure transmission protocols in maintaining the security of digital imaging and communication systems. Proper key generation, distribution, and revocation processes are essential for maintaining the confidentiality of data. Integration of secure transmission protocols like SSL and TLS ensures that data is securely transferred over communication channels, protecting against eavesdropping and tampering. To evaluate the effectiveness of our framework, we conducted experiments and analyzed the results. The findings demonstrated that our

multilayer algorithmic approach significantly improves the security posture of digital imaging and communication systems. The integrated security measures work synergistically to mitigate risks, protect sensitive data, and ensure the secure transmission of images.

References

[1] Çelebi, A. T., &Ertürk, S. (2012). Visual enhancement of underwater images using Empirical Mode Decomposition. Expert Systems with Applications, 39(1), 800–805. Retrieved from https://doi.org/10.1016/j.eswa.2011.07.077

[2] Chambah, M., Semani, D., Renouf, A., Coutellemont, P., Rizzi, A., Chambah, M. Constancy, C. (2008). Underwater Color Constancy : Enhancement of Automatic Live Fish Recognition To cite this version : HAL Id : hal-00263734 Underwater Color Constancy : Enhancement of Automatic Live Fish Recognition. 16th Annual Symposium on Electronic Imaging, 157–168.

[3] Cheddad, A., Condell, J., Curran, K., &McKevitt, P. (2010). A hash-based image encryption algorithm. Optics Communications, 283(6), 879–893. Retrieved from https://doi.org/10.1016/j.optcom.2009.10.106

[4] Chen, L., & Ã, D. Z. (2008). Image encryption with fractional wavelet packet method. Optik, 119(2008), 286–291. Retrieved from https://doi.org/10.1016/j.ijleo.2006.11.005

[5] Chourasiya, A., &Khare, N. (2019). A Comprehensive Review Of Image Enhancement Techniques. International Journal of Innovative Research and Growth, 8(6), 8–13. Retrieved from https://doi.org/10.26671/ijirg.2019.6.8.101

[6] Chunamari, S. R. (2013). Secure Schematic Model for Verifying Encrypted Image using Invariant Hash Function. International Jounral of Computer Applications, 39– 45.

[7] Corchs, S., &Schettini, R. (2010). Underwater image processing: State of the art of restoration and image enhancement methods. Eurasip Journal on Advances in Signal Processing, 2010, 14 pages. Retrieved from https://doi.org/10.1155/2010/746052

[8] Das, P. K., Kumar, P., &Sreenivasulu, M. (2014). Image Cryptography : A Survey towards its Growth. Advance in Electronic and Electrical Engineering, Research India Publications, 4(2), 179–184. Retrieved from http://www.ripublication.com/aeee.htm

[9] Deen, A. E. T. El, El-Badawy, E.-S. A., &Gobran, S. N. (2014). Digital Image Encryption Based on RSA Algorithm. IOSR Journal of Electronics and Communication Engineering, 9(1), 69–73. Retrieved from https://doi.org/10.9790/2834-09146973

[10] Deng, Z., &Zhong, S. (2019). A kind of design of knapsack public key cryptosystem based on chaotic system. UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science, 81(2), 165–176.

[12] Deshpande, K., & Singh, P. (2018). Performance Evaluation of Cryptographic Ciphers on IoT Devices. ArXiv, 1–6.

[13] Ebrahim, M., & Chong, C. W. (2013). Secure Force : A Low-Complexity Cryptographic Algorithm for Wireless Sensor Network (WSN), 1–6.

[14] Elshamy, A. M., Hussein, A. I., Hamed, H. F. A., Abdelghany, M. A., &Kelash, H. M. (2019). Color Image Encryption Technique Based on Chaos. Procedia Computer Science, 163, 49–53. Retrieved from https://doi.org/10.1016/j.procs.2019.12.085