iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68656

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Secure Video Steganography using ChaCha20 Encryption and Adaptive LSB

Keerthana Balli[1], Dr. Ch.D.V. Subba Rao[2]
[1]*M.Tech student,* [2]*Professor, Department of Computer Science and Engineering, Sri Venkateswara University College of Engineering, Tirupati, A.P*

Abstract: ***Video steganography is a robust method for concealing confidential information within video files, ensuring data privacy, and safeguarding against unauthorized access. This study presents a secure video steganography technique incorporating the ChaCha20 encryption algorithm to bolster data security before embedding. ChaCha20, recognized for its agility and resilience to cryptographic threats, encrypts the hidden data before it is inserted into chosen video frames using the Least Significant Bit (LSB) method. This ensures minimal misrepresentation and preserves the perceptual quality of the video while providing a strong layer of security. In this proposed system, once input files are selected, the ChaCha20 algorithm automatically generates a key file. This key file is then used to retrieve the concealed information, ensuring a smooth and secure decryption process. The concealed data is extracted and decrypted accurately at the receiver's end. Experimental results demonstrate that the proposed method achieves high noiselessness, low computational overhead, and vigorous security, making it a reliable solution for secure video-based communication.***

Keywords: ***video steganography, chacha20 encryption, least significant bit (LSB), data hiding, secure communication, cryptographicsecurity, steganography techniques, data confidentiality, information hiding, imperceptibility, robust security, low computational overhead.***

I. INTRODUCTION

In today's digital world, securing private information on the internet has become a crucial challenge. As modern communication relies heavily on digital platforms such as emails, chats, and online transactions, the risk of data breaches and cyber threats is ever-increasing[1]. The fundamental question is ensuring our confidential data remains protected from hackers and cybercriminals. To address these security concerns, encryption techniques alone are not sufficient. Instead, an advanced approach that not only transforms the data into an unreadable format but also conceals its very presence is required [2]. This is where video steganography plays a vital role in ensuring a secure digital environment. Steganography is a sophisticated technique that embeds hidden information within a multimedia file in such a way that it remains undetectable to unauthorized users. Unlike cryptography, which focuses on encrypting data, steganography ensures that the existence of the secret message remains unnoticed[3]. This dual-layer security enhances the protection of private information, making it difficult for attackers to alter or misuse the hidden content. Among various forms of digital steganography—text, image, audio, video, and protocol-based—video steganography stands out due to its capability to store a large volume of data. Video files, with their high redundancy and multiple frames, offer a vast medium for embedding confidential information without noticeable distortion [4] [5]. As a result, organizations and enterprises leverage this technique to safeguard sensitive data from cyber threats. However, existing video steganography methods face multiple challenges, including vulnerability to detection, poor embedding capacity, and susceptibility to cryptographic attacks. Previous approaches predominantly relied on symmetric encryption algorithms such as XOR Transformation, DES, 3DES, and AES, which, despite their effectiveness, can be compromised by advanced decryption techniques [6]. To overcome these limitations, the ChaCha20 algorithm emerges as a highly secure and efficient solution. ChaCha20 is a stream cipher encryption method known for its speed, resistance to cryptanalysis, and ability to provide robust security. By integrating ChaCha20 encryption into video steganography, this approach enhances data security while maintaining the imperceptibility of the hidden information[7] [8]. This ensures that although the steganography process is detected, the encrypted data remains indecipherable without the correct decryption key. The proposed system focuses on leveraging ChaCha20-based video steganography to create a highly secure and resilient method for protecting confidential information in video files. Through this novel approach, we aim to achieve[9][10] enhanced security, higher embedding capacity, and improved resistance against unauthorized access, making video steganography a reliable solution for modern digital communication.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

In the cyber world, the growing danger of cyber threats, securing digital communication is more important than ever. Steganography is a method used to conceal the secret data inside digital files, such as images, audio, and videos making it invisible to unauthorized users[11][12]. Among these, video steganography is considered more effective because it offers more storage capacity and better security than image-based techniques. However, many traditional steganography techniques face security vulnerabilities, limited data-hiding capacity, and computational inefficiencies [13] [14]. To address these limitations, researchers have combined encryption techniques with steganography, improving security and robustness. This section reviews existing research on video steganography techniques**,** highlighting their strengths, weaknesses, and the need for a more secure and efficient approach [15]**.**

The Least Significant Bit (LSB) substitution is a simple and widely used technique in video steganography. It works by hiding secret data in the least significant bits of pixel values in selected video frames [16]. This method is easy to implement and allows a large amount of data to be embedded. However, it has some major weaknesses [17]. It can be easily detected through statistical analysis, making it less secure [18]. It is also highly vulnerable to video compression techniques like MP4 and H.264, which can distort or remove the hidden data. Additionally, it is not strong enough to resist steganalysis attacks, which are designed to detect hidden information. To improve security, Koumal Kaushik and Suman (2015) developed a hash-based round LSB technique that randomly selects LSBs for embedding data. This made the hidden data harder to detect and improved imperceptibility [19]. However, the method still struggled with compression artefacts and statistical attacks, making it less effective for real-world use.

To make video steganography more secure, researchers have developed transform domain techniques, which hide data in the frequency components of a video instead of directly changing pixel values. This makes the hidden data more resistant to compression and detection [21]. One common method is Discrete Cosine Transform (DCT), which embeds data in compressed formats like MP4 and H.264, making it harder to detect. Another technique, Discrete Wavelet Transform (DWT), divides the video into different frequency layers, improving resistance to attacks. Some advanced methods combine both DCT and DWT to create hybrid techniques, balancing security and efficiency [22]. The biggest advantages of transform domain techniques are that they can better withstand video compression and steganalysis, making the hidden data harder to detect. However, the main drawback is that these methods require more computing power, which makes them difficult to use in real-time applications.

With advancements in artificial intelligence, video steganography has become more secure and flexible using deep learning techniques. Chong Mou et al. (2023) introduced a Neural Network-based method that can hide multiple secret videos inside a single cover video. This AI-driven method makes it much harder for attackers to detect conceal data. It also allows receivers to extract specific hidden videos using unique keys, adding an extra layer of security [23]. However, the biggest challenge is that this method requires a lot of computational power, which makes it difficult to use in real-time applications.

Motion vector-based steganography is a smart way to hide data in videos by modifying motion estimation data instead of directly changing pixels. This technique takes advantage of motion vectors, which help predict movement between frames in compressed formats like MP4 and H.264. Subramanian N. et al. **(2023)** reviewed this method and found that it has some great advantages. Since it works within the motion data, it is more resistant to video compression, meaning the hidden information is less likely to be lost [24]. Also, because the modifications are subtle, it reduces the chances of detection by steganalysis tools. However, this method does have some downsides. The biggest limitation is that it can't store as much hidden data compared to more advanced techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). While it provides better security and remains undetectable, its lower data-hiding capacity makes it less useful for embedding large amounts of secret information [25].

Using encryption in steganography makes hidden data even more secure by scrambling it before embedding it into a video or image. Ayush Balodi et al. (2023) compared two popular encryption methods: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) to see how they perform in steganography [26]. Their study found that AES is much more secure than DES because DES has a shorter key length, making it easier to crack using brute-force attacks.However, AES also comes with some challenges [27]. It requires a lot of processing power, which slows down encryption and decryption. Another issue is that image steganography has limited space, meaning only a small amount of data can be hidden. Additionally, because AES uses a block cipher structure, it takes more time to process, making it less efficient for large-scale applications like video steganography [28] [29]. While AES provides stronger security, its heavy processing requirements make it difficult to use in real-time or high-volume steganography.

While AES is a strong encryption method, its high processing requirements make it less suitable for real-time applications like video steganography [30]. ChaCha20 is a more efficient alternative that offers both speed and security. It is significantly faster than AES, making it ideal for real-time video processing. Additionally, it requires lower computational power, which reduces processing time and makes it more practical for devices with limited resources.

Despite being lightweight, ChaCha20 still provides strong security, effectively resisting brute-force and cryptographic attacks. These advantages make it a more suitable encryption method for modern steganography applications where both efficiency and security are crucial.

III. PROPOSED SYSTEM

In this proposed system, the chacha20 stream cipher is used to securely hide datawithin video files for the purpose of video steganography. The system leverages chacha20's efficiency and strong encryption capabilities to embed hidden information in video frames without significantly altering the video's content or quality.

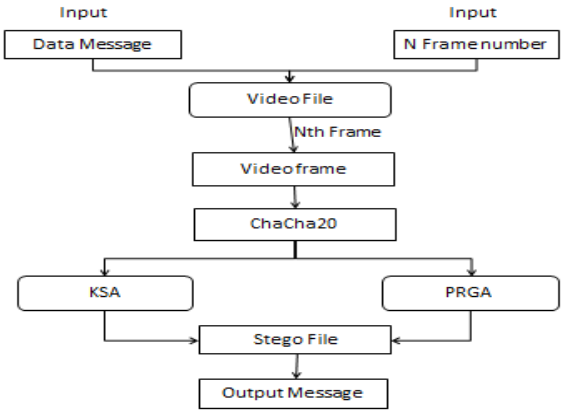


Fig. 1 Block diagram for proposed method

The main purpose of this figure 1 is to demonstrate a secure method for hiding data inside the video frames, ensuring both steganographic concealment and cryptographic protection of the hidden data. It can be used for secure communication or data hiding. Itrepresents a video steganography method for hiding a data message within a video file using cryptographic principles.
The chacha20 is afast and secure encryption algorithm used to protect data. It is a stream cipher; meaning is it encrypts information continuously rather than in fixed blocks and making it highly efficient. A chacha20 algorithm was created by Daniel J. Bernstein as an improved version of the Salsa20 cipher algorithm**.** It is widely used because of its speed, simplicity, and strong security features. It is also designed to resist common attacks like differential and linear cryptanalysis, ensuring that encrypted data remains safe. One of its biggest advantages is that it works well on multi-core processors and high-performance systems, making it ideal for modern applications. It generates acontinuous stream of random bits (keystream), which is then XORed with the original data to produce the encrypted message. This method ensures fast and efficient encryption while maintaining strong security. The following methodology shows, how to works the proposed algorithm:

1) Select a cover video file in MP4 or AVI or FLV format and extract necessary secret information from the video.
2) Convert the video into individual frames and identify specific frames for data hiding while keeping other frames unchanged.
3) Encrypt the secret message using a ChaCha20 algorithm.
4) Append a unique password for additional security before embedding.
5) Embed the encrypted message into the least significant bits of the selected frames, ensuring minimal distortion to maintain video quality.
6) Replace the modified frames in the original sequence and then reconstruct the video with the stego frames to generate the final stego video.
7) Send the stego video securely to the receiver.
8) Receive the stego video and extract the data.
9) Divide the frames from the video and then identify the frames that contain hidden data while keeping other frames are unchanged.
10) Extract the hidden information from the selected frames using the adaptive LSB extraction technique.
11) Validate the password to ensure the integrity of the extracted data.
12) If the password is incorrect, discard the extracted data to prevent decryption errors.

13) Decrypt the extracted information using the decryption algorithm and retrieve the original secret message by using ChaCha20 algorithm.
14) Merge the extracted frames with the remaining frames and reconstruct the original video to restore its initial state.

A. *ChaCha20 Encryption*

The ChaCha20 encryption process(figure 2) ensures that the confidential message is first securely converted into ciphertextusing a keystream. Once encrypted, the binary data is secretlyhidden within the RGB(Red, Green, Blue)components of a video frame for creating astego Video. A video that secretly carries hidden information .This technique combines chacha20 encryption (to keep the message safe) with steganography (to keep it hidden), making sure that the hidden message remains both secure andundetectable. Even if someone extracts the hidden data, they won't be able to read it without the correct decryption key, ensuring strong security. This method is widely used in secure communication, digital forensics, and data protection, where secrecy is essential. ChaCha20 is also known for its speed and efficiency, making it a great choice for real-time encryption in video processing. Additionally, since the message is spread across the video frame's pixels, it becomes difficult to detect or extract without proper knowledge of the algorithm.

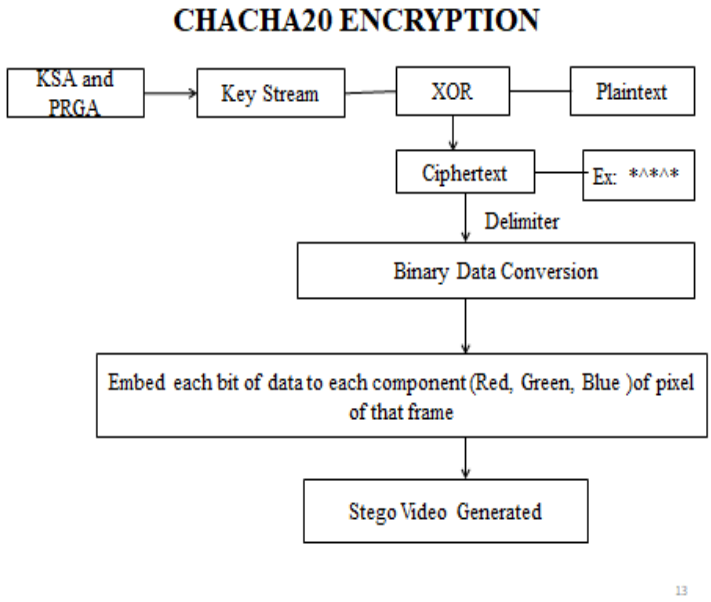


Fig 2 ChaCha20 Encryption

B. *ChaCha20 Decryption*

The process of extracting and decrypting a secret message from a stego video is simple yet highly secure. It begins by selecting a specific Nth frame from the video, where the LSB (Least Significant Bit) extraction method retrieves the hidden binary data embedded within the pixel values. Since this extracted data is encrypted, it needs to be decrypted using the ChaCha20 algorithm. The decryption process uses a key and a keystream to convert the encrypted data back into its original secret message, ensuring that only authorized users can access it. Even if someone extracts the hidden data, they won't be able to read it without the correct decryption key, maintaining a high level of security. ChaCha20 is widely trusted for its speed, efficiency, and resistance to attacks**,** making it a strong choice for secure communication, digital forensics, military intelligence, and covert data storage. One major advantage of this method is that the video quality remains unaffected, ensuring that the presence of hidden data goes undetected. Additionally, since the message is embedded at the pixel level, it is nearly impossible to identify or remove without proper decryption knowledge. The figure 3 visually explains this step-by-step process, making it easier to understand how ChaCha20 decryption helps extract and restore secret messages from a stego video.

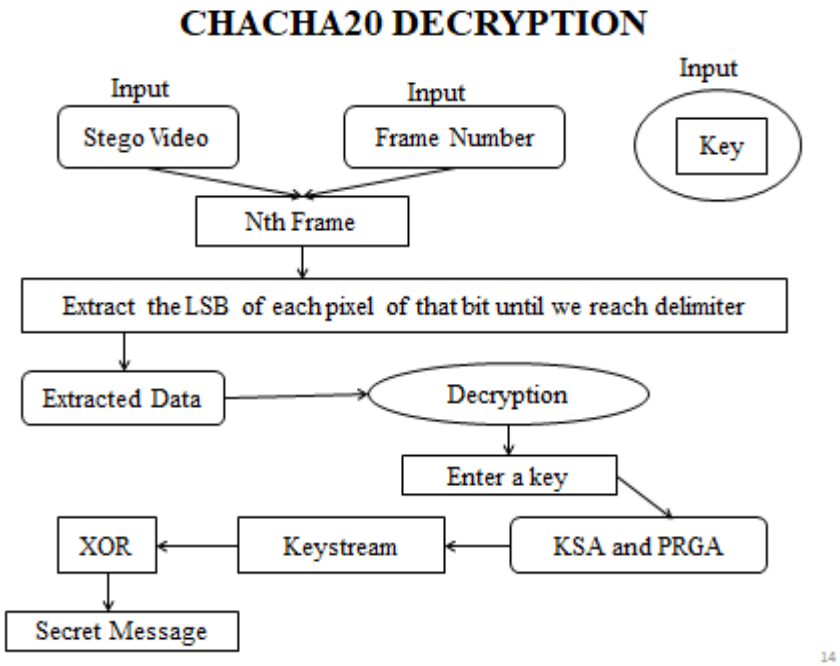


Fig 3 ChaCha20 Decryption

IV. RESULTS

The following result shows that the complexity of video quality is judged according to the quartile deviation of video complexity. Those metrics are used to shows the part of original video and encoded video generated by stegavideo and the proposed method respectively.

A. PSNR Metric

The following figure 4 shows thePSNR (peak signal-to-noise ratio) metric, which helps measure the quality difference between a stego video (a video with hidden data) and the original video when using ChaCha20-based video steganography. The X-axis represents two PSNR metric values: PSNR_AVG(average quality measurement) and GLOBAL_PSNR(overall quality measurement), while the y-axisshows the PSNR values in decibels (dB), ranging from about 40 to 50. The blue bars represent the PSNR values of thestego video**,** and the red bars represent the values of the original video before embedding any data. From this figure 4, we can see that the PSNR values of the stego video are slightly lower than the original video, meaning that embedding the hidden message has caused a small drop in quality. However, the PSNR values remain high, which means the difference is so small that the video still looks the same to the human eye. This proves that ChaCha20-based video steganography is effective, as it keeps the video looking almost identical while securely hiding the encrypted data. One of the biggest advantages of this method is that it combines encryption with steganography, making the hidden message almost impossible to detect and decryptwithout the correct key. This makes it useful for secure communication, digital forensics, business confidentiality, and military applications. Even if someone suspects that data is hidden in the video, they cannot access the original message without the proper decryption key. Compared to other encryption techniques, ChaCha20 is fast, efficient, and highly secure. The high PSNR values indicate that the video quality is preserved well, meaning the hidden data does not cause major distortions. Factors like video resolution, frame rate, and embedding capacity also affect the quality. In the future, improvements such **as** better video compression and AI-driven encryption methods can help make this technique even more secure and efficient. Overall, this PSNR analysis confirms thatChaCha20-based video steganography is a great way to hide sensitive datawhile keeping the video quality almost unchanged, making it an excellent choice for safe and secret communication**.**

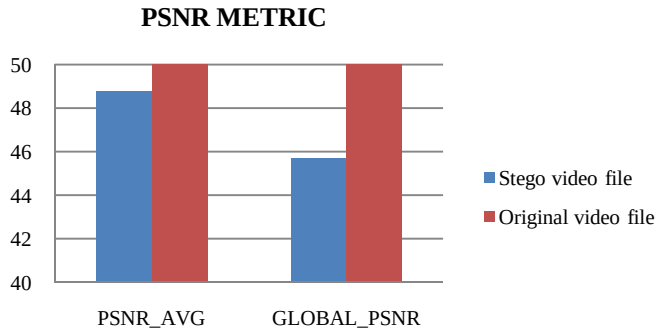


Fig 4 PSNR Metric

B. SSIM Metric

The following figure 5 shows, the SSIM (structural similarity index metric), which measures how much the stego video (a video with hidden data) resembles the original video when using ChaCha20-based video steganography. The X-axis represents two key SSIM metricvalues: SSIM_AVG(average similarity across frames) and GLOBAL_SSIM(overall similarity of the entire video). The Y-axis shows SSIM values ranging from 0.9 to 1, where a value closer to 1 means better quality. The blue bars represent the stego video, and the red bars represent the original video before hiding any data.From the chart, we can see that the SSIM_AVG values for both videos are nearly the same, meaning that the stego video looks almost identical to the original video. However, for GLOBAL_SSIM, the stego video has a slightly lower value, indicating a small quality change across the entire video after embedding the hidden message. Despite this minor drop, the high SSIM values prove that the visual quality of the video is well-preserved, and the difference is barely noticeable to the human eye.This method ensures that the hidden message remains secure while keeping the video looking natural**.** Even if someone examines the video, they won't easily detect the hidden data. This makes ChaCha20-based video steganography a powerful technique for secure and secret communication. Future improvements, like better embedding techniques or AI-based optimization**,** can help further improve video quality while keeping the hidden data even safer.In short, thisSSIM analysis confirms that ChaCha20-based video steganography is a reliable way to hide sensitive data without affecting video quality, making it a great option for secure and discreet data transmission**.**

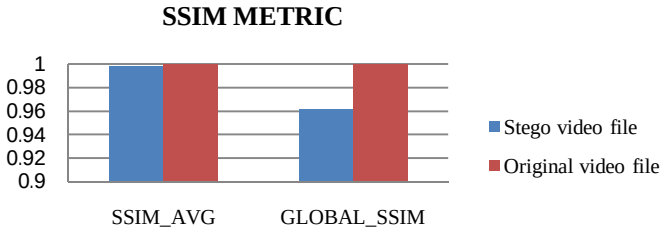


Fig 5 SSIM metric

The comparison of ChaCha20 (table1) shows that, DES, and LSBin video steganography highlights key differences in security, video quality, and file size**.** Among the three, ChaCha20 stands out as the most secure option, offering the highest PSNR (48.76 dB) and SSIM (0.998444), meaning the hidden message remains well-protected while keeping the video quality almost unchanged. However, this strong encryption results in a significantly larger file size. ContrarilyDES provides a balance between security and file size**,**offering moderate video quality (PSNR: 45.02 dB, SSIM: 0.899675) with a smaller file size compared to ChaCha20**.** LSB (least significant bit) is the simplest and most lightweight method**,** but it has the lowest video quality (PSNR: 40.15 dB, SSIM: 0.908765), making it easier to detect and less secure for confidential applications. Overall, if security and quality are the main priorities, ChaCha20 is the best choice.However, if a balance between size and encryption is needed, DES can be a suitable alternative.For scenarios where file size is the biggest concern and security is less critical, LSB may be used, but with caution due to its weaker protection.

TABLE 1
Comparison table for existing algorithms and Proposed Algorithm

Algorithm	File Size	PSNR Metric	SSIM Metric
ChaCha20	941824 bytes	48.76 dB	0.998444
DES	32768 bytes	45.02 dB	0.899675
LSB	512 bytes	40.15 dB	0.908765

V. CONCLUSION

In conclusion, video steganography using the ChaCha20 encryption algorithm provides a secure and efficient way to hide sensitive data inside a video files. It ensures that strong data protection while keeping the video quality almost unchanged by embedding information in the least significant bits of video frames. Experimental results including PSNR and SSIM metrics confirm that this method works well with only a slight drop in video quality that's mostly impossible to notice. This method enhances security by making sure that even if someone intercepts the video, they can't access the hidden data without the correct key. It is also fast and efficient making it suitable for real time applications. Compared to older methods like DES and simple LSB steganography, ChaCha20 algorithm offers stronger protection against hacking and detection of secret message. However, challenges such as capacity limitations, vulnerability to lossy compression, and potential detection by steganalysis tools highlight areas for further improvement.

REFERENCES

[1] Anastasiia, H., Oleksandr, K., Yuliia, N., Alla, N., Veronika, S., & Tetiana, D. (2024). Management of Strategies for Shaping the Innovative and Investment Potential of Enterprises as a Factor Ensuring Their Economic Security. Indian Journal of Information Sources and Services, 14(3), 16–22. https://doi.org/10.51983/ijiss-2024.14.3.03.

[2] Anderson, R.,Biham, E.,& Knudsen, L.(2000).Serpent and smartcards. In Smart Card Research and Applications: Third international conference, CARDIS'98, Louvain-la-Neuve, Belgium, September 14-16, 1998. Proceedings 3(pp.246-253). Springer Berlin Heidelberg. https://doi.org/10.1007/10721064_23.

[3] Arman, M.S., Al Mamun, S., & jannat, N.(2024, April). A modified AES based approach for data integrity and data origin authentication. In 2024 3rd international conference on Advancement in electrical and electronic engineering (ICAEEE) (pp. 1-6) IEEE.https://doi.org/10.1109/ICAEEE62219.2024.10561750.

[4] Azeez, R. A., Abdul-Hussein, M. K., Mahdi, M. S., & ALRikabi, H. T. S. (2021). Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique. Periodicals of Engineering and Natural Sciences (PEN), 10(1), 178-187. https://doi.org/10.21533/pen.v10i1.2577.

[5] Azeez, R. A., Jamil, A. S., & Mahdi, M. S. (2023). A Partial Face Encryption in Real World Experiences Based on Features Extraction from Edge Detection. International Journal of Interactive Mobile Technologies, 17(7), 69-81. https://doi.org/10.3991/ijim.v17i07.3875.

[6] Bashier, E., & Jabeur, T. B. (2021). An Efficient Secure Image Encryption Algorithm Based on Total Shuffling, Integer Chaotic Maps and Median Filter. Journal of Internet Services and Information Security, 11(2), 46-77. https://doi.org/10.22667/JISIS.2021.05.31.046 .

[7] Biham, E., Dunk Elman, O., & Keller, N. (2001, April). Linear cryptanalysis of reduced round serpent. In International Workshop on Fast Software Encryption (pp. 16-27). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45473-X_2.

[8] Hassan, N. F., Al-Adhami, A., & Mahdi, M. S. (2022). Digital speech files encryption based on Hénon and gingerbread chaotic maps. Iraqi Journal of Science, 830-842. https://doi.org/10.24996/ijs.2022.63.2.36.

[9] Hoobi, M. M. (2024). Multilevel Cryptography Model using RC5, Two fish, and Modified SerpentAlgorithms. Iraqi Journal of Science, 65(6), 3434-3450. https://doi.org/10.24996/ijs.2024.65.6.37

[10] Hussein, M. K., Hassan, K. R., & Al-Mashhadi, H. M. (2020). The quality of image encryption techniques by reasoned logic. Telkomnika (Telecommunication Computing Electronics and Control), 18(6), 2992-2998. https://doi.org/10.12928/TELKOMNIKA.v18i6.14340.

[11] Kalinin, O., Gonchar, V., Abliazova, N., Filipishyna, L., Onofriichuk, O., & Maltsev, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. Natural and Engineering Sciences, 9(1), 26-45. https://doi.org/10.28978/nesciences.1469858.

[12] Mahdi, M. S., Azeez, R. A., & Hassan, N. F. (2020). A proposed lightweight image encryption using ChaCha with hyperchaotic maps. Periodicals of Engineering and Natural Sciences, 8(4), 2138-2145.

[13] Mahdi, M. S., Hassan, N. F., & Abdul-Majeed, G. H. (2021). An improved chacha algorithm forsecuring data on IoT devices. SN Applied Sciences, 3(4), 429. https://doi.org/10.1007/s42452-021-04425-7.

[14] Najm, H. (2021). Data authentication for web of things (WoT) by using modified secure hash algorithm-3 (SHA-3) and Salsa20 algorithm. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2541-2551.

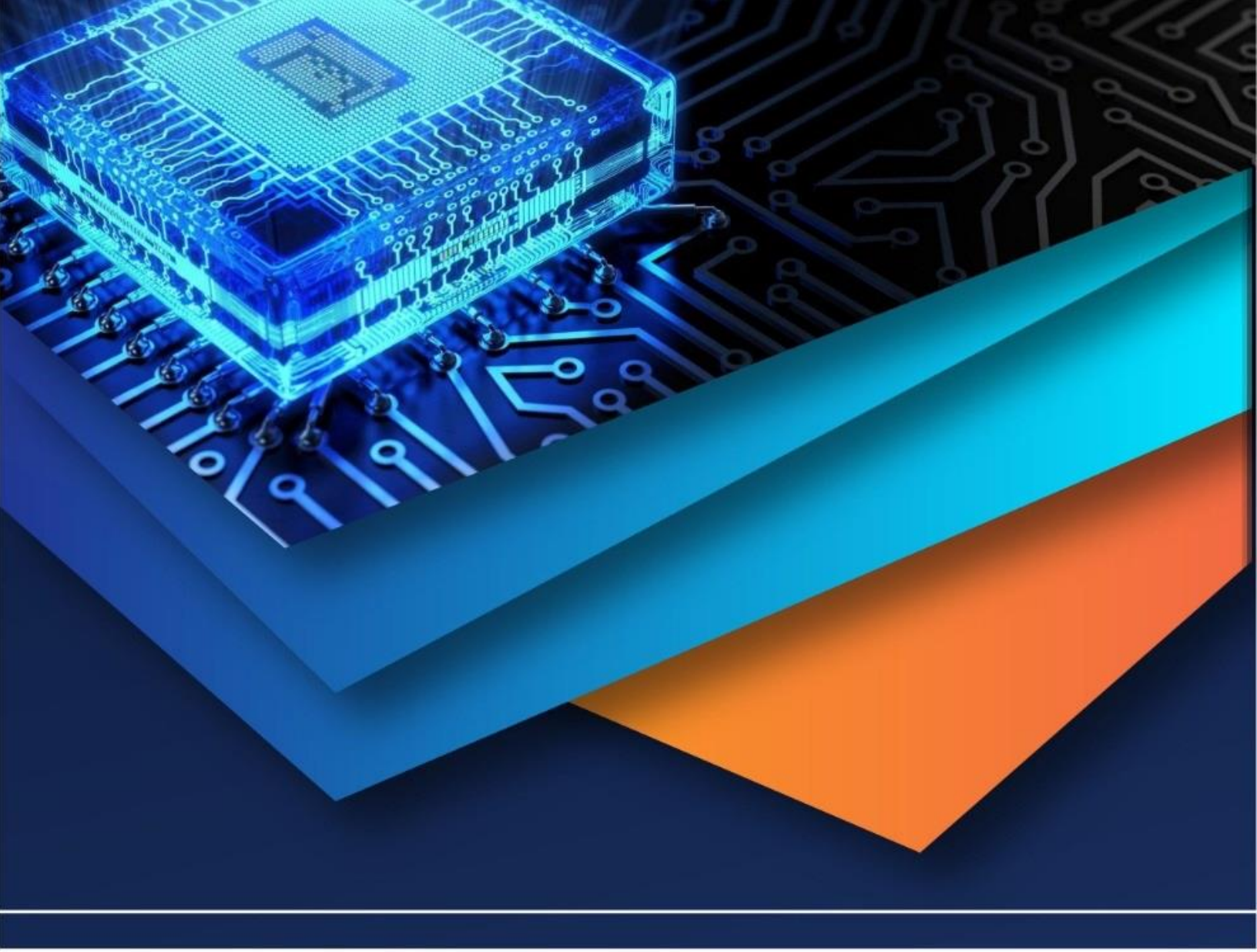
[15] Najm, H., Hoomod, H. K., & Hassan, R. (2020). A proposed hybrid cryptography algorithm based on GOST and salsa (20). Periodicals of Engineering and Natural Sciences (PEN), 8(3), 829-1835.

[16] Najm, H., Hoomod, H., & Hassan, R. (2021). A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System. International Association of Online Engineering. https://www.learntechlib.org/p/218922/.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[17] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N., & Stay, M. (2000). The Twofish team's final comments on AES Selection. AES round, 2(1), 1-13.
[18] Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT algorithm: design to RGB image encryption implementation. IEEE Access, 8, 52609-52621. https://doi.org/10.1109/ACCESS.2020.2978083
[19] Tian, P., & Su, R. (2022). A Novel virtual optical image encryption scheme created by combining chaotic S-Box with double random phase encoding. Sensors, 22(14), 5325. https://doi.org/10.3390/s22145325
[20] Ullah, A., Shah, A. A., Khan, J. S., Sajjad, M., Boulila, W., Akgul, A.,& Ahmad, J. (2022). An efficient lightweight image encryption scheme using multichaos. Security and Communication Networks, 2022(1), 5680357. https://doi.org/10.1155/2022/5680357
[21] Weinstein, D., Kovah, X., & Dyer, S. (2012). SeRPEnT: Secure remote peripheral encryption tunnel. Technical Report MP120013, the MITRE Corporation.
[22] Karthikeyan, B., Raj, M.M.A., Yuvaraj, D. and Joseph Abraham Sundar, K. (2020) A Hybrid Approach for Video Steganography by Stretching the Secret Data. In: Ranganathan, G., Chen, J. and Rocha, Á. Eds., Inventive Communication and Computational Technologies, Springer, 1081-1087. https://doi.org/10.1007/978-981-15-0146-3_104.
[23] Patil, A., Keshkamat, S.M., Desai, V.V. and Arlimatti, T. (2018) Embedding of Advanced Encryption Standards Encoded Data in Video Using Least Significant Bit Algorithm. 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, 27-28 July 2018, 617-621. https://doi.org/10.1109/icrieece44171.2018.9009202.
[24] Manohar, N. and Kumar, P.V. (2020). Data Encryption & Decryption Using Steganography. 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 13-15 May 2020, 697-702. https://doi.org/10.1109/iciccs48265.2020.9120935.
[25] Qasim Ahmed Alyousuf, F., Din, R. and Qasim, A.J. (2020) Analysis Review on Spatial and Transform Domain Technique in Digital Steganography. Bulletin of Electrical Engineering and Informatics, 9, 573-581. https://doi.org/10.11591/eei.v9i2.2068.
[26] Alam, K., Nushrat, S., Patwary, A.H., Ullah, A. and Robin, K.H. (2023) An Improved Approach of Image Steganography Based on Least Significant Bit Technique for Secure Communication in Cloud. In: Woungang, I., Dhurandher, S.K., Pattanaik, K.K., Verma, A. and Verma, P., Eds., Advanced Network Technologies and Intelligent Computing, Springer, 215-233. https://doi.org/10.1007/978-3-031-28180-8_15.
[27] Canniere, C.D.; Preneel, B. TRIVIUM Specifications. ESTREAM, ECRYPT Stream Cipher Project. 2006. Volume 2006. Available online: https://www.ecrypt.eu.org/stream/e2-trivium.html (accessed on 22 February 2024).
[28] Zhang, B.; Rahmatullah, B.; Wang, S.L.; Liu, Z. A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. Multimed. Tools Appl. **2022**, 82, 15735–15762.
[29] Elashry, I.F.; El-Shafai, W.; Hasan, E.S.; El-Rabaie, S.; Abbas, A.M.; Abd El-Samie, F.E.; El-sayed, H.S.; Faragallah, O.S. Efficient chaotic-based image cryptosystem with different modes of operation. Multimed. Tools Appl. **2020**, 79, 20665–20687.
[30] Sha, Y.; Cao, Y.; Yan, H.; GAO, X.; Mou, J. An image encryption scheme based on IAVL permutation scheme and DNA operations. IEEE Access **2021**, 9, 96321–96336.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)