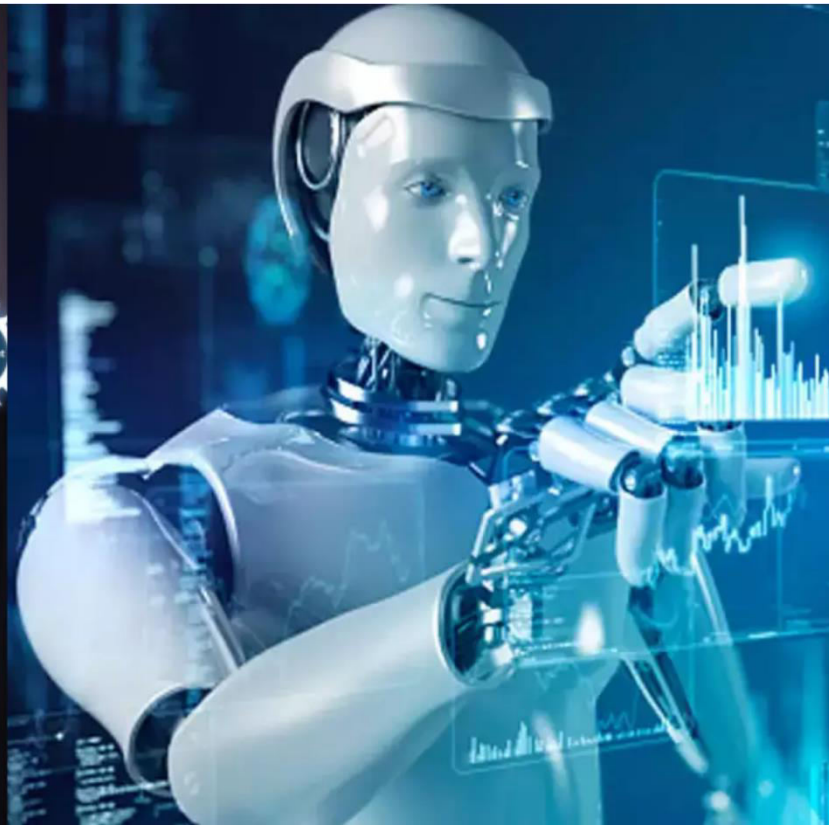
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

Key Generation for Zero Steganography using DNA Sequence

Indudhara J, Mr. Musheer Ahmed

Student, Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India

Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: Zero steganography is a novel technology that eliminates detectable artifacts and greatly improves security by enabling covert communication without changing the cover medium. In this work we present a novel DNA-based key generation model that generates robust cryptographic keys for zero-steganography systems by utilizing the intrinsic complexity unpredictability and biological characteristics of DNA sequences. The process starts with raw DNA sequences which are then pre-processed to standardize nucleotide patterns and eliminate noise. Before being integrated into a zero-modification steganography framework the hidden message is encrypted using these DNA-derived keys. DNA is a great source of cryptographic material because it shows naturally. The four nucleotides A T C and G make up DNA.

I. INTRODUCTION

In the modern era communication has greatly benefited from technology. The development of cell phones the internet cloud computing and other cutting-edge technologies has made people more connected. Consequently there is a risk to the security of data transferred across networks. Data security is starting to take precedence. Steganography and cryptography are two widely used approaches for protecting data. Most studies on coverless steganography use image databases and analyze image properties. These investigations demonstrated the resistance of coverless steganography to steganalysis techniques. However further development is still possible.

II. LITERATURE SURVEY

[1] J. P. Bhoge and P. N. Chatur, "Avalanche Effect of AES Algorithm,"
According DNA-based key generation for zero-steganography, as it highlights the significance of producing random, high-entropy keys. The overall resilience of the steganographic system is increased by a powerful avalanche effect, which guarantees that keys derived from DNA sequences will yield secure and unpredictable encrypted outputs. Through experimental investigation, the authors show that even a single-bit change in the encryption key or plaintext results in a substantial and unanticipated change in the final ciphertext.

[2] X. Zhang, F. Peng, and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification".
This study proposes an unchanging coverless image steganography method to make the secret communication very resistant to steganalysis attacks pixel values. The technique combines Latent Dirichlet Allocation (LDA) topic modelling in combination with the DCT (Discrete Cosine Transform (DCT) features to describe images as high-level semantic characteristics rather than explicitly inserting hidden material into an image. In contrast to.conventional embedding-based steganography, the writers demonstrate this approach.method offers superior security, stability under picture alterations, and great resistance to attacks.

[3] X. Duan and H. Song, "Coverless information hiding based on Generative Model".
The writers create visuals that naturally convey the secret message using a generative model, usually based on deep learning. The model is taught to produce visually natural images with no direct modifications from particular inputs (representing message segments), making it very challenging to discover the communication using conventional steganalysis. The authors demonstrate that this generative method offers great steganalysis resistance, coverless transmission, and good security. The method improves stealth and robustness by switching from embedding-based steganography to generation-based concealment.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

[4] Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval".
A distinct visual characteristic pattern is linked to each communication block or secret message. To send a message the system searches the database for an image (or group of images) whose partial-duplicate properties match those mapped message patterns. Since the image is only selected based on the message and not modified there are no statistical indications of steganography. By applying the same feature extraction and retrieval method to the shared database the recipient can use the recovered images visual characteristics to decode the message.

III. PROPOSED METHODOLOGY

Unlike traditional steganography methods which physically embed hidden information into digital content zero steganography uses cryptographic keys to control concealment and retrieval reducing the likelihood of discovery. By offering a bio-inspired approach that can be used in domains like digital communication biomedical data transfer and military systems the goal goes beyond immediate security. By fusing digital cryptography with biological randomization the research ultimately aims to provide a novel way for safeguarding sensitive data in an increasingly interconnected digital world. This method guarantees that the generated keys are distinct unpredictable and impervious to pattern-based or brute-force exploitation. The system aims to overcome the drawbacks of current steganography and key generation methods by offering a reliable scalable and user-friendly architecture that permits secure communication.

Proposed Model Diagram
The diagram shows DNA-based zero-steganography architecture for secure image concealment without altering the cover medium. It begins with a secret image that is altered into a fake secret image most likely through encryption or obfuscation in order to prevent direct disclosure of sensitive content. This fictional image and a cover image undergo a DNA-inspired transformation process symbolized by double helix icons which suggests that nucleotide mapping shifting and flipping operations are used to create sequences rich in entropy. This technique ensures that the cover medium is unaffected but the security of the hidden message depends only on the DNA-derived key and shared transformation parameters between sender and recipient.

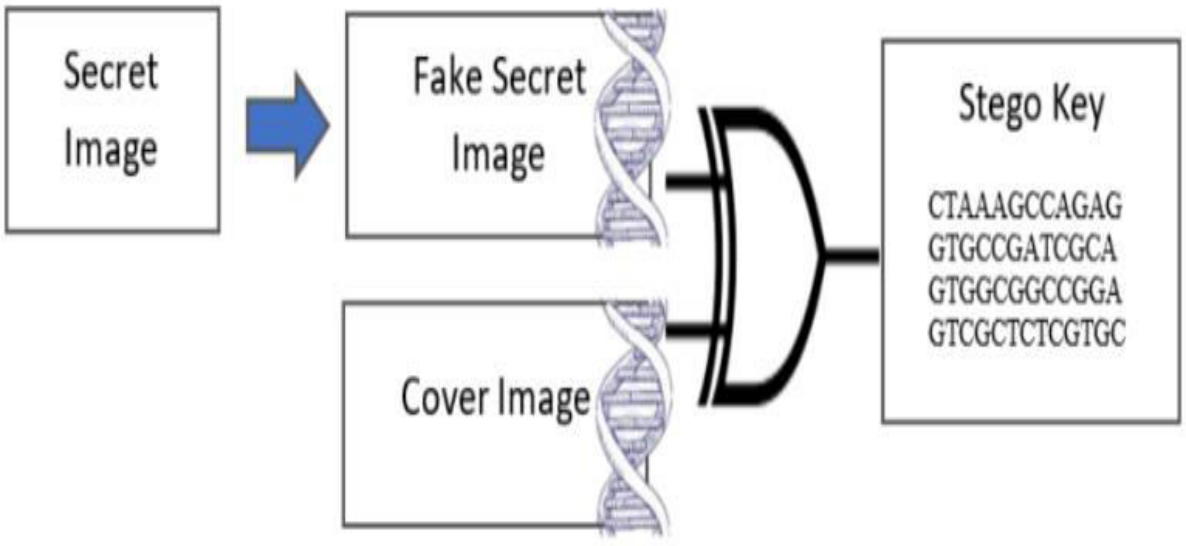


Figure 2.1.1: *Block Diagram of Proposed System*

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

IV. RESULTS

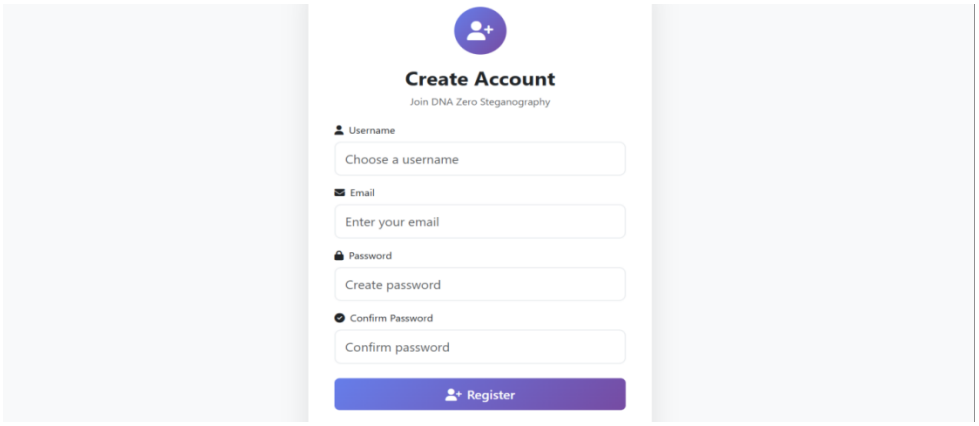


Fig: Register Page

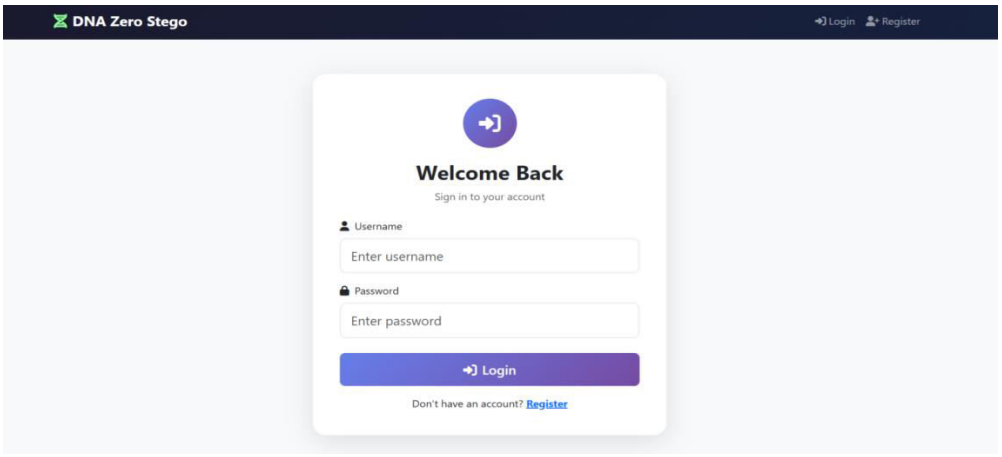


Fig: Login/ Signup page

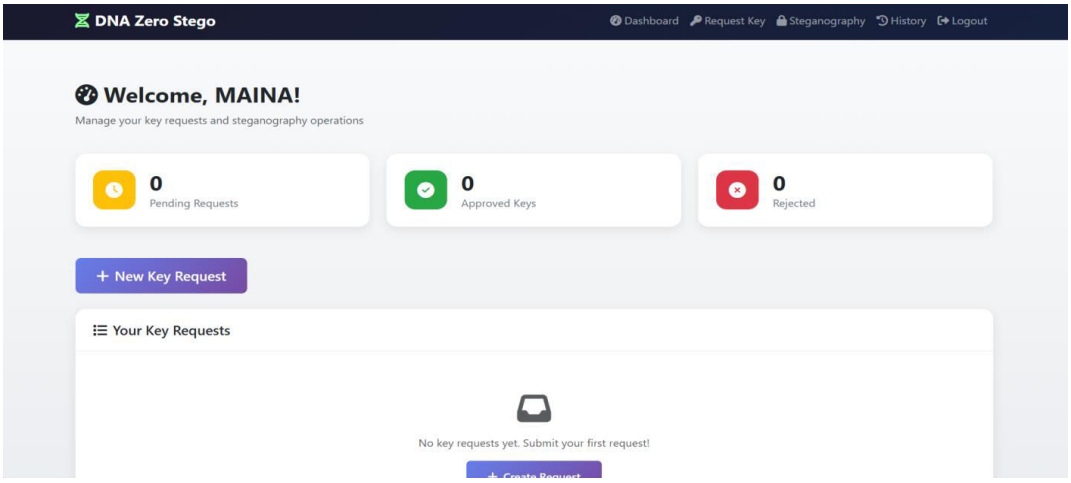


Fig: Dashboard Page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

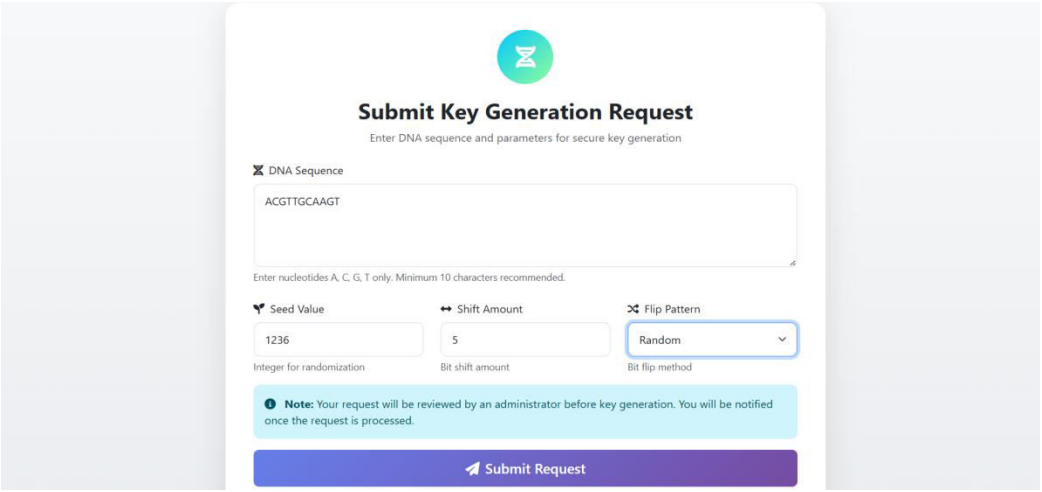


Fig: Request Page

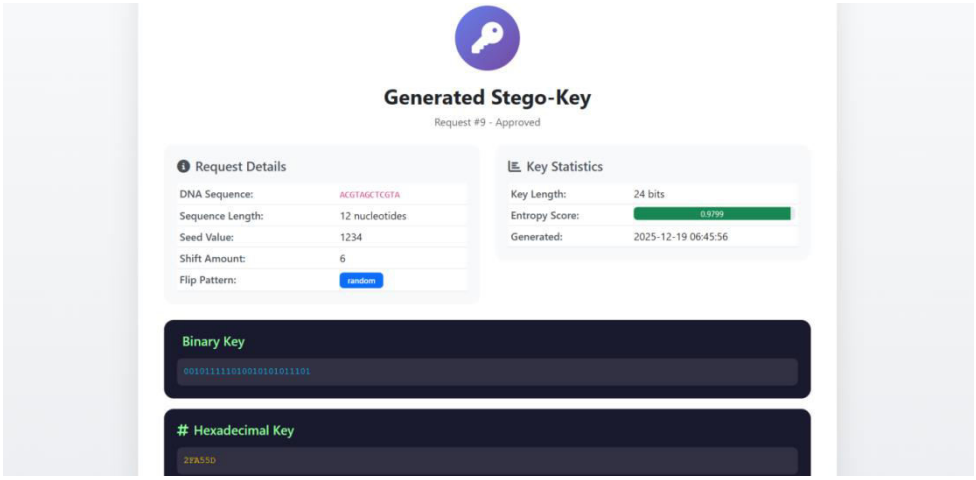


Fig: Generated Key Page

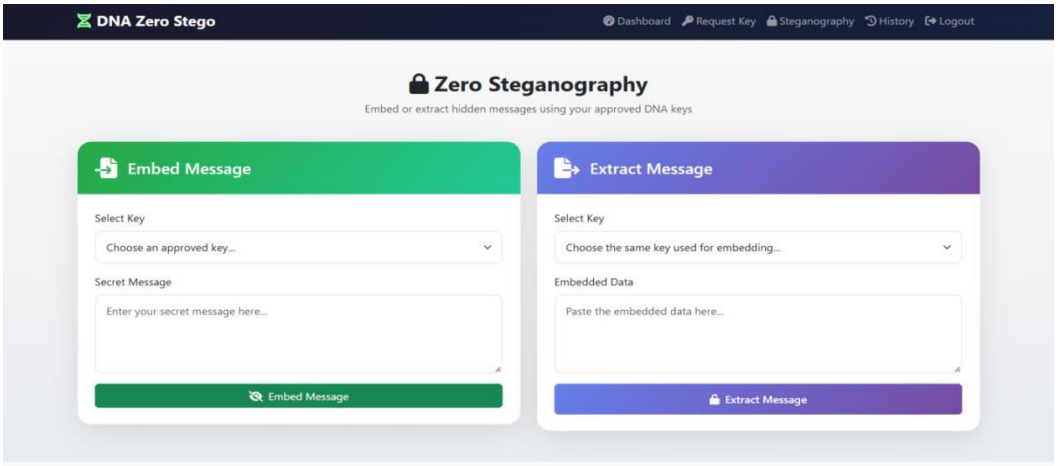


Fig: Embed and Extract Page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

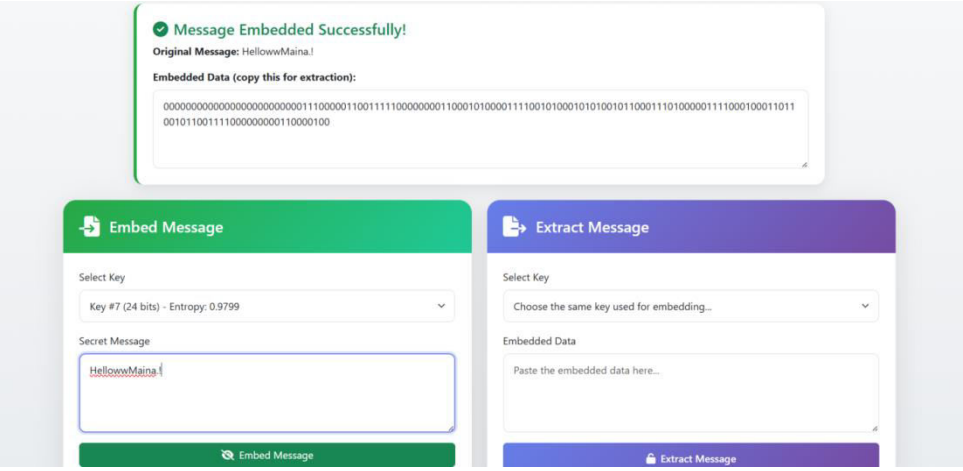


Fig: Message Embedded Page

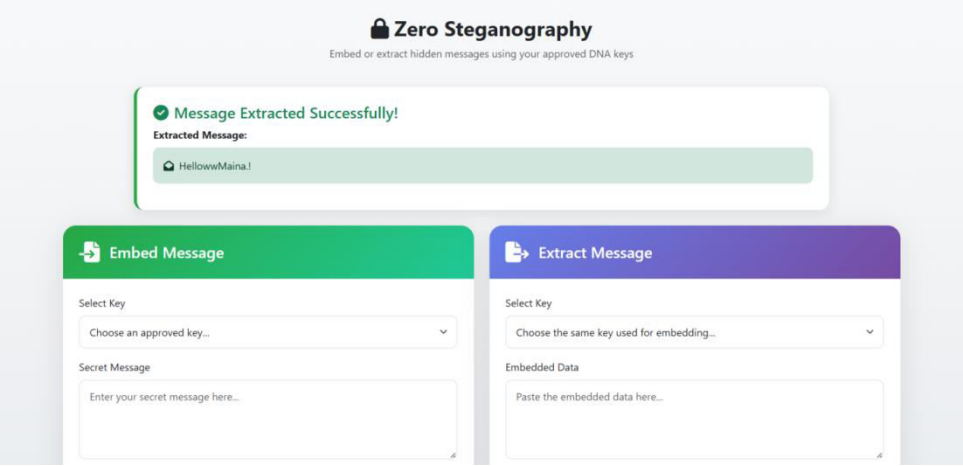


Fig: Message Extracted Page

V. CONCLUSION

A method for generating zero steganography keys using DNA sequences is presented in this paper. The transmission of the cover image and key must be considered in order to prevent the scheme from being compromised. DNA sequences were used to ensure security especially in schemes with a low cracking risk. Additionally the use of DNA simplified the system and reduced its computational requirements. Performance at runtime was also improved. The process also created a powerful avalanche effect. The key generation algorithm is generally safe with respect to its avalanche effect runtime and cracking chance. The stego key generated by this method can be improved by transforming the DNA sequences into an image. Further research will develop a stego-key utilizing additional biological properties of DNA like translation and transcription to further enhance the techniques security. Another option is to consider putting the plan into practice in a system or application. Future Improvements Future enhancements to the DNA-based zero-steganography module could focus on making it more efficient adaptable and compatible with state-of-the-art security frameworks. The system could be extended to accept multi-sequence DNA inputs in order to increase entropy and improve key robustness against cryptanalytic attacks. Optimizing hashing algorithms and preprocessing would reduce latency and enhance the modules suitability for real-time applications.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412128|

VI. FUTURE ENHANCEMENT

Future improvements to the DNA-based zero-steganography module may concentrate on increasing its effectiveness, flexibility, and compatibility with cutting-edge security frameworks. In order to increase entropy and boost key robustness against cryptanalytic attacks, the system could be expanded to allow multi-sequence DNA inputs. Pre-processing and hashing algorithm optimization would lower latency and improve the module's suitability for real-time applications. Scalability could be enhanced by parallel processing and cloud-based deployment enabling secure communication over large networks and multiuser environments. Usability improvements that would make the systems more accessible to non-technical users include graphical user interfaces and automated parameter selection. Using machine learning to detect anomalies in audit logs and create adaptive keys could further improve security and reliability. For future secure communication systems these enhancements would ensure that the module grows into a more reliable efficient and user-friendly solution.

REFERENCES

[1] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali, “Security analysis of DNA based steganography techniques,” SN Appl. Sci., 2020.
[2] Z. Zhou, Y. Mu, and Q. M. J. Wu, “Coverless image steganography using partial-duplicate image retrieval,” Soft Comput., 2019.
[3] M. M. Liu, M. Q. Zhang, J. Liu, P. X. Gao, and Y. N. Zhang, “Coverless Information Hiding Based on Generative Adversarial Networks,” Yingyong Kexue Xuebao/Journal Appl. Sci., 2018.
[4] A. Arya and S. Soni, “A Literature Review on Various Recent Steganography Techniques,” Int. J. Compute. Technol. Appl., 2018.
[5] X. Zhang, F. Peng, and M. Long, “Robust Coverless Image Steganography Based on DCT and LDA Topic Classification,” IEEE Trans. Multimed., 2018.
[6] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, “Coverless image steganography: A survey,” IEEE Access, 2019.
[7] M. S. Rahman, I. Khalil, and X. Yi, “An approach to data authenticity in mobile cloud-based healthcare that uses lossless DNA data hiding,” Int. J. Inf. Manage., 2019.
[8] K. K. Sand and S. Jelavić, “Mineral facilitated horizontal gene transfer: A new principle for evolution of life?,” Front. Microbiol., 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details