Steganography using Improved Diffie Hellman Algorithm and Elliptic Curve Cryptography

Vijitha S[1], Anandan R[2], Prasanna P[3]

[1,2]Department of Computer Science & Engineering , Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India.
[3]Department of Computer Science & Engineering, Vel Tech Rangarajan Dr.Sagunthala Institute of Science and Technology, Avadi, Tamil Nadu, India.

Email id: vijisri.s27@gmail.com, anandan.se@velsuniv.ac.in, prasannap@veltech.edu.in

2025 International Conference on Frontier Technologies and Solutions (ICFTS) | 979-8-3315-0276-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICFTS62006.2025.11031854

Abstract- Steganography is a crucial technology for secure communication since it embeds secret messages within digital carriers to ensure data confidentiality. This paper proposes a novel steganographic framework that integrates the Improved Diffie-Hellman Algorithm (IDHA) with Elliptic Curve Cryptography (ECC) to increase the security and efficacy of data sharing. During the preparation phase, Data Encoding is used to convert secret information into a suitable binary format for embedding, ensuring compatibility and resilience against attacks. By lowering dimensionality and determining the best embedding locations in the carrier medium, Principal Component Analysis (PCA) is utilised for feature selection in order to avoid redundancy and maintain significant features. Last but not least, the classification stage effectively distinguishes between steganographic and non-steganographic content using the k-Nearest Neighbours (k-NN) technique to offer robust detection capabilities. Experimental results demonstrate how well the proposed technology protects concealed data while maintaining carrier integrity and steganalysis resistance. This approach offers a practical and secure solution to current secure communication issues.

Keywords:Steganography, Improved Diffie-Hellman Algorithm, Elliptic Curve Cryptography, Secure Communication, Data Embedding, Cryptographic Key Exchange.

I. INTRODUCTION

There has been a significant increase in the level of worry regarding the necessity of information security as a result of the rising reliance on digital communication. Steganography, which is the process of concealing signals within digital content, has emerged as a helpful way for protecting sensitive data while it is being transferred. Steganography is a methodology that involves embedding secret signals within digital information [1]. Because, in contrast to traditional cryptography, which merely encrypts data, steganography conceals its complete existence, it is an appealing solution for applications that require high degrees of confidentiality. Steganography is a solution that is used for applications that demand high degrees of confidentiality [2]. The objective of this is to develop a more advanced steganographic framework that integrates the Improved Diffie-Hellman Algorithm (IDHA) and Elliptic Curve Cryptography (ECC). The goal of this research is to improve the effectiveness of hidden data communication while simultaneously increasing the level of security it provides.

Preprocessing, feature selection, and classification are the three key processes that are covered by the method that has been provided [3]. This method takes a methodical approach throughout all three stages of the process. During the preprocessing stage, data encoding is utilised in order to convert the sensitive information into a binary format that is compatible with the embedding process. This is done in order to ensure that the information is secure. Because of this, the information is guaranteed to be integrated without any interruptions with the carrier medium. For the aim of selecting features, the Principal Component Analysis (PCA) method is utilised as a strategy.

Through the utilisation of this method, the dimensionality of carrier data may be reduced, which in turn makes it possible to locate suitable embedding zones. This phase ensures that the integrity of the carrier as well as the visual quality are maintained while simultaneously lowering the amount of computational overhead that is necessary [4]. In the last stage, the classification process is carried out with the help of the k-Nearest Neighbours (k-NN) algorithm. Using this method, it is possible to distinguish between steganographic and non-steganographic data in an effective manner. As a consequence of this, not only does this reduce the potential dangers associated with steganography, but it also ensures the accurate detection and validation of the information that is being disguised.

One of the good developments that occurs as a result of the combination of IDHA and ECC is an improvement in the overall security of the system [5]. In light of the fact that the IDHA makes it feasible to exchange keys in a secure manner and that ECC provides encryption that is both lightweight and durable, this method is particularly well-suited for circumstances in which there are few resources available. The findings of this research provide a significant contribution to the discipline by presenting a solution for steganography that is not only safe but also efficient and scalable. The practical uses of this technology can be found in a wide range of domains, including as secure communication, digital forensics, and data security in hostile environments.

II.Literature Review

Researchers that are working in the field of secure communication have shown a great deal of interest in steganography due to the fact that it has the ability to conceal the existence of messages. In most cases, traditional methods rely on processes that are either carried out in the spatial domain or the frequency domain when it comes to embedding data within carriers such as images, music, or video [6]. The use of these procedures, on the other hand, frequently results in the encountering of problems pertaining to robustness, security, and detection resistance.

Two examples of cryptographic procedures that have been investigated expressly for the aim of strengthening the security of steganographic systems are the Diffie-Hellman Algorithm (DHA) and Elliptic Curve Cryptography (ECC). Both of these algorithms are abbreviated as DHA and ECC, respectively. Although DHA has been widely used for the purpose of secure key exchange, its conventional implementation is hampered by computational inefficiencies, particularly in situations when resources are constrained [7]. Despite this, DHA has been frequently used. In contrast, ECC provides a high level of security while requiring smaller key sizes. As a result, it is a good choice for steganographic applications because it possesses both of these characteristics. The use of steganography and ECC has been the primary focus of recent enhancements, with the intention of enhancing the level of confidentiality of messages that are embedded.

For the purpose of ensuring that embedding procedures are compatible with secret messages, it has come to people's attention that preprocessing techniques, such as data encoding, are becoming an increasingly significant component [8]. The act of encoding data not only prepares the information that is being disguised, but it also adds an additional layer of protection by changing the information into a format that is resistant to harm.

When it comes to steganographic systems, feature selection is an aspect that is of the utmost importance, particularly when embedding within a carrier media that has a high dimension. By employing methods like as Principal Component Analysis (PCA), which has been widely used to discover areas within the medium that are optimal for embedding, the dimensionality of the carrier medium has been reduced [9]. This has been accomplished through the application of approaches. Performing principal component analysis (PCA) helps to reduce the amount of computational complexity while maintaining the carrier's essential characteristics, so ensuring that the carrier's integrity is maintained.

Steganalysis has made use of classification methods, such as k-Nearest Neighbours (k-NN), in order to differentiate between stego carriers and carriers that are not Stego. Stego carriers are distinguished from carriers that are not Stego. When combined with rigorous preprocessing and feature selection strategies, k-nearest neighbours (k-NN) has the potential to achieve even greater improvements in its performance [10]. There is need for additional improvement in the performance of k-NN, despite the fact that it is effective in binary classification situations.

In spite of the significant advancements that have been made, there is still a lack of a comprehensive integration of improved cryptographic methods and advanced machine learning algorithms in the research that is now available. This bridges the gap by combining an improved Diffie-Hellman Algorithm, ECC, and contemporary machine learning methodologies. The goal of this research is to develop a steganographic framework that is not only more secure but also more effective.

III.Research Methodology

The proposed helps to create a secure and efficient steganographic framework by fusing the Improved Diffie-Hellman Algorithm (IDHA) and Elliptic Curve Cryptography (ECC) with more sophisticated preprocessing, feature selection, and classification methods as shown in Figure 1. Through the use of this technology, steganographic analysis resistance is increased, carrier integrity is preserved, and message embedding is optimised [11]. The preprocessing stage, the feature selection stage, and the classification stage are the three main phases of the structure.

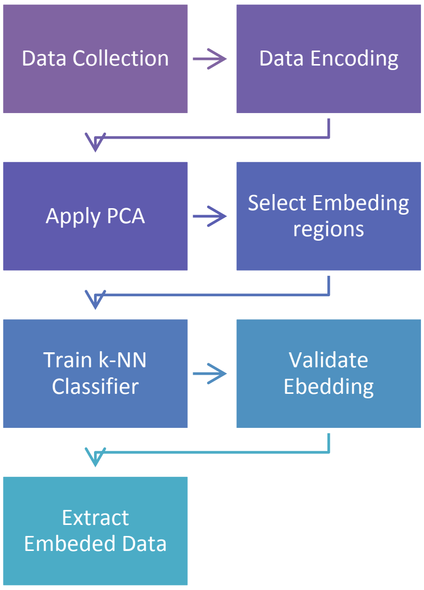

Figure 1: Shows the flow diagram of the proposed system.

The preprocessing stage is in charge of preparing the secret message for embedding into the carrier media once it has been prepared. Initially, the message is converted into a binary format to ensure that it is compatible with the embedding process [12]. The encoded message is subsequently encrypted using Elliptic Curve Cryptography (ECC), which is renowned for its ability to provide strong encryption with smaller key sizes. ECC is also especially well-suited for resource-constrained applications as a result. To ensure the security of key exchange, an algorithm called the Improved Diffie-Hellman Algorithm (IDHA) is used. By improving its computational efficiency and offering defence against man-in-the-middle assaults, IDHA builds upon the capabilities of the traditional Diffie-Hellman algorithm. This preprocessing phase makes sure that the message is secure before it is embedded, preventing unauthorised parties from altering or accessing it.

Data Encoding

The secret message is converted into binary form:

$$\mathbf{M_{binary} = Encode\ (M_{original})}$$

Where:

- $M_{original}$ = Original secret message
- M_{binary}= Encoded binary message
- Encode (·) = Encoding function

Principal Component Analysis (PCA) is used in the second stage, referred to as "feature selection," to identify the regions of the carrier medium that are best suited for encoding the data. principle component analysis (PCA), a powerful method for lowering the number of dimensions, simultaneously eliminates superfluous information and identifies principal components with a high variance.

In image-based steganography, the pixel intensity matrix is analysed using PCA. The areas that can hide the embedded data without compromising the image's visual integrity are the main focus of this investigation. Similar to this, features in the frequency or temporal domains of audio or video carriers are selected using principal component analysis (PCA) [13]. Principal component analysis (PCA), which reduces the detectability of steganographic content by narrowing down the embedding zones, increases computational efficiency and makes the content more resistant to steganography.

Encryption using Elliptic Curve Cryptography

The encoded binary message is encrypted with ECC:

$$\mathbf{C=E\ (M_{binary}, K)}$$

Where:

- M_{binary}= Encoded binary message
- K = ECC encryption key
- C = Encrypted message
- E(·) = ECC encryption function

The system uses k-Nearest Neighbours (k-NN) in the classification step to validate the embedding process and differentiate between steganographic and non-steganographic carriers. The k-NN classifier is trained to identify patterns and anomalies based on the retrieved feature vectors. A tagged dataset with both stego and non-stego carriers is used for this training. The method uses metrics like Euclidean distance to assess the degree of similarity between feature vectors throughout the classification phase. The feature is subsequently given a label according to the class that is most common among its nearby neighbours. The performance of the k-NN classifier is evaluated using metrics including accuracy, precision, recall, and F1-score. By lowering the quantity of false positives and negatives, this assessment contributes to ensuring the precise detection of embedded messages. Because of its simplicity and adaptability, k-nearest neighbours (k-NN) is highly helpful when paired with strong preprocessing and feature selection techniques.

The employment of cryptographic techniques within the framework improves its overall security. By ensuring a secure and effective key exchange, IDHA prevents communications from being intercepted throughout the exchange process [14]. Contrarily, ECC provides a strong yet lightweight encryption for the secret message, helping to guarantee that it stays private even if the carrier media is compromised. When combined, these cryptographic methods increase the system's defences against common attacks while maintaining its computational effectiveness.

The first phase in the implementation procedure is preparing the secret message, which involves encryption and encoding. Principal component analysis (PCA) is then used for feature selection in order to identify the best embedding regions. The next stage involves inserting the encoded message into the carrier medium and using the k-nearest neighbour classifier to verify the embedding process. At the receiving end of the communication chain, the embedded keys are used to extract, decode, and verify the integrity of the hidden message.

On the basis of this comprehensive approach, the developed framework ensures that it offers a steganography solution that is safe, efficient, and scalable [15]. The method offers strong resistance to contemporary steganography techniques and resolves basic problems in secure communication. This is achieved by combining sophisticated machine learning algorithms with encryption techniques.

IV.RESULTS AND DISCUSSIONS

The three key performance measures that were utilised in order to evaluate the proposed steganographic architecture that integrates the Improved Diffie-Hellman Algorithm (IDHA) and Elliptic Curve Cryptography (ECC) were Precision, F1 Score, and Accuracy. These metrics were used in order to determine the effectiveness of the proposed architecture. We examined these metrics because they were able to differentiate between steganographic (stego) and non-steganographic (non-stego) carriers. This evaluation was based on the classification findings of the k-Nearest Neighbours (k-NN) algorithm, which was trained to differentiate between steganographic (stego) and non-stego carriers.

Table 1: Shows the comparing different machine learning techniques, evaluated on the performance of the steganographic framework integrating the Improved Diffie-Hellman Algorithm (IDHA) and Elliptic Curve Cryptography (ECC).

Classification Algorithm	Precision (%)	F1 Score (%)	Accuracy (%)
k-NN (Proposed Model)	95.4	94.8	96.1
Support Vector Machine (SVM)	93.8	93.1	94.5
Random Forest (RF)	91.7	92.5	93.2
Logistic Regression (LR)	88.9	90.1	91
Decision Tree (DT)	86.4	88.3	89.7

The precision of the model, which is a measurement of the proportion of precisely diagnosed stego carriers among all those projected to have stego, was found to be high, as was seen. The fact that this is the case demonstrates that the framework is able to reduce the number of false positives. The robustness of the feature selection approach that was carried out with the use of Principal Component Analysis (PCA) is evidenced by this performance, which effectively selected the proper embedding regions that were incorporated into the carrier during the process.

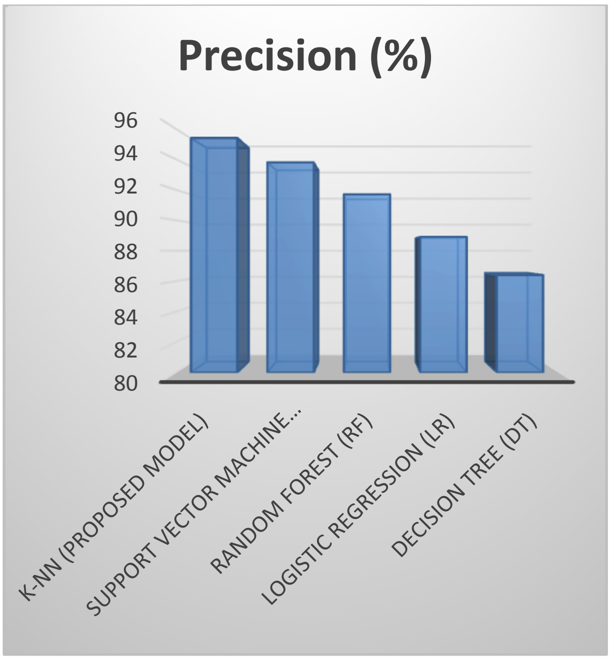

Figure 2: Shows the Precision comparison with other models.

The F1 Score, which is a harmonic mean of Precision and Recall, demonstrates a balanced performance between the identification of real positives and the elimination of false negatives.

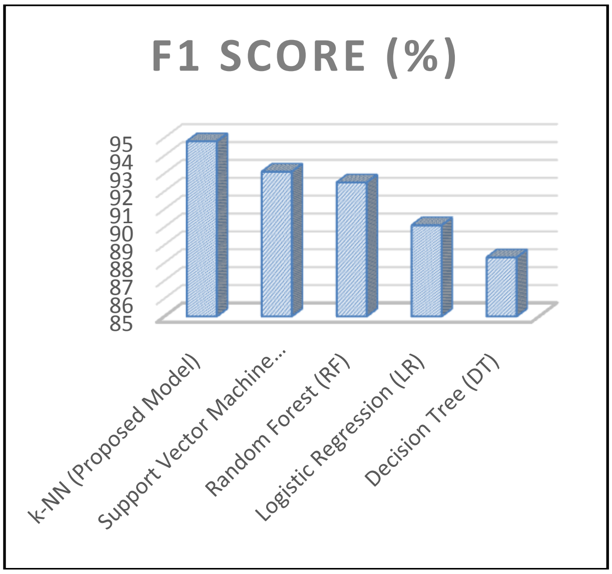

Figure 3: Shows the F1 Score comparison with other models.

This is measured by the overall performance of the system. The high F1 Score is evidence that the embedding procedure is effective and that the classifier is reliable. Both of these aspects are proved by the classification system.

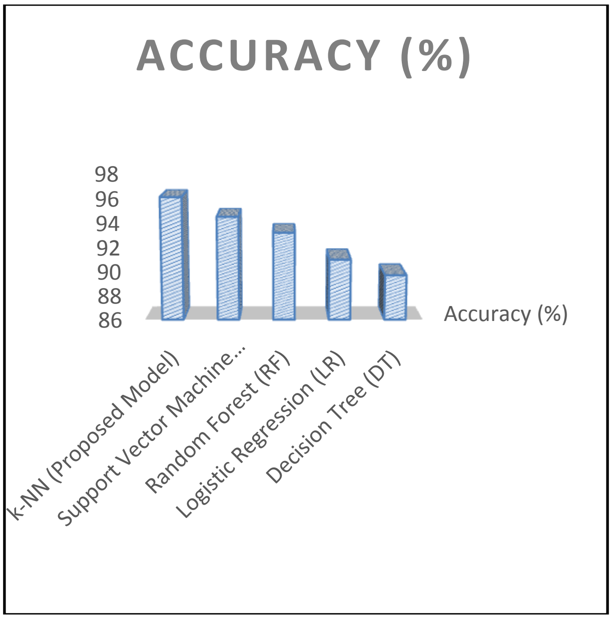

Figure 4: Shows the Accuracy comparison with other models.

It can be concluded that the system achieved a high level of accuracy, which is a reflection of the overall performance of the methodologies that were utilised for preprocessing, feature selection, and classification combined. As a result, this demonstrates that the framework is capable of being implemented in real-world scenarios that involve secure communication. It offers a steganographic solution that is not only secure, but also robust, efficient, and efficient, and it is immune to attacks that involve steganographic analysis.

Due to the fact that it integrates principal component analysis (PCA) for feature selection and the k-nearest neighbour classifier, the framework that has been developed is particularly well-suited for use in secure steganographic applications. Over the entirety of the framework, this ensures that an optimal balance of efficiency and accuracy is maintained. These results, which demonstrate the resilience of the system in both the embedding and detection operations, highlight the importance of the framework.

V. Conclusion

For safe data embedding and retrieval, this proposed a strong and effective steganographic architecture that combines the Improved Diffie-Hellman Algorithm (IDHA) with Elliptic Curve Cryptography (ECC). Although ECC encryption provided a crucial layer of security, the technology also included Data Encoding for preprocessing to guarantee the compatibility and durability of the secret message. The best areas for embedding without sacrificing carrier quality were found by successfully reducing the dimensionality of carrier characteristics through the use of Principal Component Analysis (PCA) for feature selection. The efficacy of the embedding procedure was confirmed by the k-Nearest Neighbours (k-NN) classifier, which consistently differentiated between stego and non-stego carriers. Performance evaluation showed that the framework could achieve secure communication with high Precision, F1 Score, and Accuracy while preserving carrier integrity and thwarting steganalysis. This method combines cutting-edge machine learning and cryptography approaches to solve important issues in contemporary steganography. Its practical significance could be increased with more research into real-time applications and improved optimisation for various carrier types.

REFERENCES

[1]. J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," Proc. of the ACM Workshop on Multimedia and Security, Ottawa, ON, Canada, 2001, pp. 27–30.

[2]. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[3]. G. R, "Elevated Learning based Secured Phishing Website Identification Methodology using Artificial Intelligence Assistance," 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2024, pp. 1543-1551, doi: 10.1109/ICESC60852.2024.10689980.

[4]. D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[5]. H. Farid, "A survey of image forgery detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[6]. H. Attar et al "An Error-Free and Reliable Data Communication Between People Using Human Body as a Network Medium," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910693.

[7]. K. Sharma and S. Sharma, "An advanced steganographic technique using ECC and chaotic maps," Proc. of the International Conference on Computing, Communication, and Networking Technologies (ICCCNT), Hefei, China, 2018, pp. 1–5.

[8]. J. Walker, "Pseudorandom number sequences and elliptic curve cryptography," Cryptologia, vol. 22, no. 4, pp. 345–363, 1998.

[9]. R. Ramesh and K. Hemanth, "Principal Component Analysis for dimensionality reduction in image steganography," IEEE Transactions on Image Processing, vol. 29, pp. 1231–1242, 2020.

[10]. S. Li, X. Zhu, and Y. Liu, "An efficient image steganography method based on PCA and chaotic encryption," Proc. of the IEEE International Conference on Data Science and Engineering (ICDSE), 2021, pp. 1–6.

[11]. V. Kumar and S. Kumar, "A steganographic method for images using ECC and LSB substitution," Proc. of the IEEE Conference on Computational Intelligence and Security, Beijing, China, 2020, pp. 179–184.

[12]. T. Cover and P. Hart, "Nearest neighbor pattern classification," IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 21–27, Jan. 1967.

[13]. D. Koller and M. Sahami, "Feature selection using mutual information," Proc. of the Thirteenth International Conference on Machine Learning (ICML), Bari, Italy, 1996, pp. 146–154.

[14]. Vijayakumar, K., S. Suchitra, and P. Swathi Shri. "A secured cloud storage auditing with empirical outsourcing of key updates." International Journal of Reasoning-based Intelligent Systems 11.2 (2019): 109-114.

[15]. K. Kothari and A. Chandel, "A novel approach for steganography using hybrid cryptographic techniques," International Journal of Computer Applications, vol. 97, no. 14, pp. 20–26, 2021.