iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67795

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 III Mar 2025- Available at www.ijraset.com

StegoFace - Deep Learning-Based ID Image Security

Bhavya M[1], Sai Dhanush VR[2], Mukunda M[3], Surya J[4]
[1, 2, 3]*Students,* [4]*Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India*

Abstract: ***Identity verification processes predominantly depend on photo ID cards, which are at risk of fraudulent modifications and photo substitution methods. Conventional security techniques such as watermarks, microtext, and biometric verification exhibit limitations, rendering ID images vulnerable to tampering. To tackle this challenge, we introduce StegoFace, a steganographic model based on deep learning that improves the security of ID images by embedding concealed authentication data within facial images. The system utilizes Deep Convolutional Neural Networks (CNNs), Binary Error-Correcting Codes (BECC), and an autoencoder-decoder framework to ensure the secure embedding and retrieval of data while maintaining the integrity of the image. The Recurrent Proposal Network (RPN) effectively identifies facial areas for accurate message embedding, improving tamper detection and resilience against noise and compression. Experimental findings indicate that StegoFace successfully hides and retrieves concealed messages with minimal visual distortion, offering a strong, scalable, and cost-effective approach for secure identity verification in government-issued IDs, travel documents, and access control systems.***
Keywords: Steganography, Deep Learning, ID Verification, CNN, Binary Error-Correcting Codes, Autoencoder.

I. INTRODUCTION

Identity verification is a critical aspect of modern security systems, with government-issued ID cards serving as primary proof of identity across various sectors, including travel, banking, and access control. However, these ID images are increasingly vulnerable to fraud, including photo substitution attacks, where an unauthorized individual replaces the original ID photo with a counterfeit image. Traditional security measures such as watermarks, microtext, and biometric features provide some level of protection but remain susceptible to duplication, tampering, or expensive implementation costs. To address these challenges, we propose StegoFace, a novel deep learning-based steganography system designed to enhance the security of ID facial images. Unlike conventional methods, StegoFace embeds hidden authentication data within ID images using deep convolutional neural networks (CNNs) and binary error-correcting codes (BECC). This approach ensures that any unauthorized modification of the ID image is easily detectable while preserving the visual integrity of the image.

II. OBJECTIVE

The main goal of StegoFace is to create a secure and effective steganography-based system that improves the protection of printed ID facial images against photo substitution attacks. This system utilizes deep convolutional neural networks (CNNs) along with an autoencoder-decoder mechanism to hide and retrieve authentication data within ID images, ensuring tamper detection while preserving visual quality. By incorporating binary error-correcting codes (BECC), StegoFace increases resilience against noise, compression, and unauthorized alterations. The proposed approach aims to deliver a quick, dependable, and scalable authentication framework that can easily integrate with current identity verification systems. By embedding security features directly into ID images, StegoFace guarantees enhanced security standards for government-issued identification and travel documents, decreasing the likelihood of fraudulent modifications and bolstering trust in identity verification procedures.

III. LITERATURE SURVEY

Over time, numerous security strategies have been developed to improve ID verification and mitigate photo substitution attacks. Conventional methods like watermarks, microtext, and biometric authentication have seen extensive use. Watermarks, which can be either visible or hidden, are incorporated during the production of ID cards to deter duplication; nonetheless, they remain vulnerable to replication and require specific conditions for visibility. Microtext, composed of very tiny printed letters, adds an additional layer of security but is ineffective if individuals are not aware of its existence.

Biometric authentication methods, such as fingerprints and digital signatures, offer a more secure approach but necessitate specialized equipment, making their deployment expensive and complicated. Despite these improvements, photo substitution attacks continue to be a significant concern, as ID images can still be modified without impacting other security features. Recent research has examined novel approaches to enhance document security and image verification. Ferreira et al. (2021) introduced VIP Print, a validation technique aimed at identifying artificial photo modifications and source linking in printed documents. Bazarevsky et al. (2019) presented BlazeFace, a neural network that can detect faces in real-time on mobile GPUs, showcasing the efficacy of deep learning in image processing. Deng et al. (2019) created ArcFace, a deep learning facial recognition model that incorporates an additive angular margin loss to boost facial authentication precision. Jiménez Rodríguez et al. (2018) applied steganography to images captured by drones using chaotic encryption techniques, emphasizing the increasing importance of steganography in secure image transmission. Building upon these advancements, we propose StegoFace: a deep learning-based model for ID image security, which implements a deep convolutional neural network (CNN) steganography framework to elevate ID image security. By embedding concealed authentication information within facial images, StegoFace guarantees tamper detection while preserving the integrity of the image. Utilizing Binary Error-Correcting Codes (BECC) and an autoencoder-decoder framework, this model provides a robust and scalable solution for identity verification, thwarting unauthorized alterations and strengthening document security against fraudulent changes.

IV. EXISTING SYSTEM

The existing security protocols for ID verification mainly incorporate watermarks, microtext, and biometric authentication. Watermarks, which can be either overt or covert, are integrated into ID cards during manufacturing to deter counterfeiting. Nevertheless, they are not completely secure, as they can be duplicated or altered. Likewise, microtext, which features extremely small printed characters on ID cards, is challenging to detect and reproduce without specialized tools, but its effectiveness diminishes if individuals are unaware of its existence. Another widely used security mechanism is biometric authentication, including fingerprints and digital signatures, which offers an additional layer of security by confirming that the ID card belongs to its legitimate owner. Although biometric security is very effective, it necessitates costly verification systems and specialized devices, making widespread implementation difficult. In spite of these conventional security features, photo substitution attacks continue to pose a substantial problem, as perpetrators can change the ID photo without altering other security aspects, resulting in fraudulent identity exploitation.

V. CHALLENGES IN EXISTING SYSTEM

Even with several security layers in place, current ID verification techniques encounter significant issues. Watermarks and microtext can be easily replicated, and their effectiveness relies on visual examination, which makes them prone to advanced forgery methods. While biometric authentication offers greater security, its high implementation costs and requirement for specialized infrastructure limit its accessibility across various industries. Moreover, photo substitution attacks remain a significant risk, as conventional security features target document authenticity instead of image integrity. Attackers have the ability to substitute the facial image on an ID card without altering other verification components, resulting in identity theft. The lack of a solid, automated system for identifying image modifications renders ID verification systems open to unauthorized changes. Therefore, there is an urgent necessity for a sophisticated security solution that provides tamper-proof identity verification while being both cost-efficient and scalable.

VI. PROPOSED SYSTEM

The StegoFace system presents a novel approach to steganography based on deep learning, aiming to improve the security of ID images and guard against photo substitution attacks. In contrast to conventional techniques, StegoFace conceals hidden authentication data within facial images through the use of deep convolutional neural networks (CNNs), making it possible to detect any unauthorized alterations to the ID image. The system is made up of two primary components: an encoder that securely embeds authentication information within the image, and a decoder that extracts the hidden data to confirm its authenticity. To bolster security further, StegoFace incorporates Binary Error-Correcting Codes (BECC), enhancing its resilience to noise, compression, and tampering. Moreover, Recurrent Proposal Networks (RPNs) are employed to precisely locate and handle facial areas for message insertion. The autoencoder-decoder mechanism ensures that visual distortion is kept to a minimum, allowing the original image quality to be preserved while achieving a high level of security. Through these sophisticated methods, StegoFace provides a strong, scalable, and cost-efficient solution for secure identity verification, effectively tackling the weaknesses found in current ID security systems.

VII. ADVANTAGES

1) Improved Security Measures – StegoFace offers enhanced protection by incorporating concealed authentication data within identification images, allowing for the detection of any unauthorized alterations.
2) Superior Steganography Technique – The system guarantees that the embedded information remains imperceptible to the human eye while maintaining the quality of the original image.
3) Dependable Decoding System – The deep learning-based decoder proficiently retrieves the concealed authentication message, ensuring consistent verification.
4) Effectiveness in Practical Applications – StegoFace is crafted for use in a range of ID verification systems, such as government-issued identification, passports, and access control cards, thereby enhancing security in practical contexts.

VIII. SYSTEM ARCHITECTURE

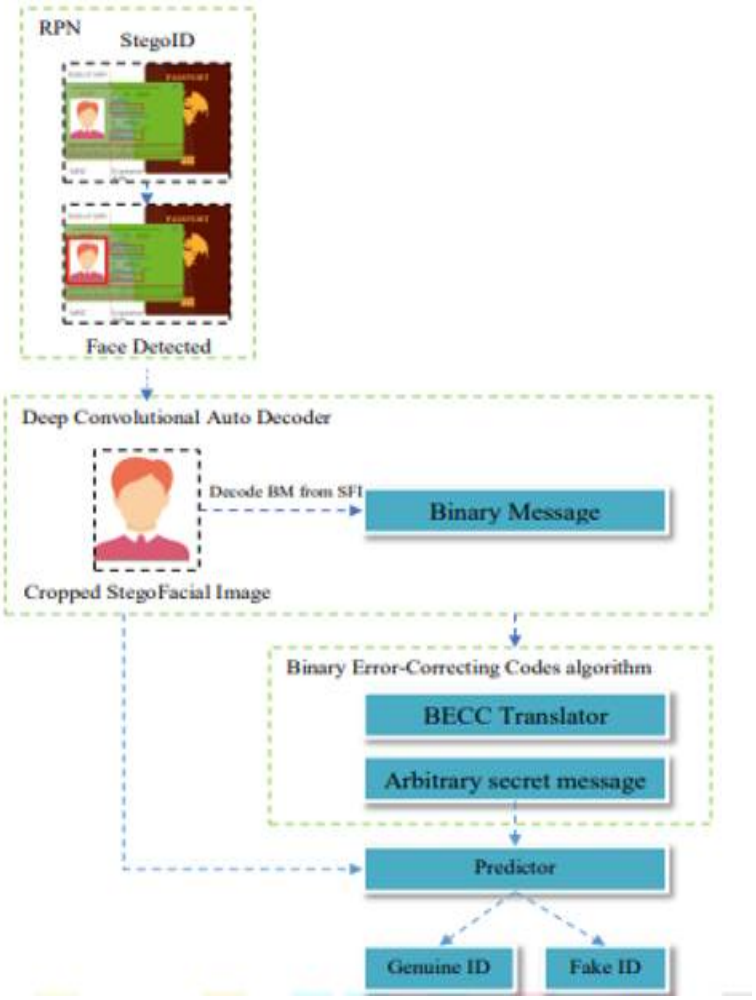


Fig. 1: A deep learning-based framework for embedding and verifying hidden authentication data in ID images.

The architecture of the StegoFace system is composed of an encoder and a decoder that collaborate to enhance the security of ID images through steganography based on deep learning. The Preprocessing Module improves image quality and identifies key facial features for precise encoding. The StegoFace Document Distributor oversees the embedding of data and its verification, while the BECC Translator utilizes Binary Error-Correcting Codes (BECC) to bolster resilience against noise and compression. The Deep Convolutional ID Face Steganography module features an Autoencoder that embeds concealed authentication data and an Auto Decoder that retrieves and confirms this data. Furthermore, the Recurrent Proposal Network (RPN) identifies and processes facial areas, ensuring accurate and secure message embedding while preserving the integrity of the image.

IX. MODULES

The StegoFace system is made up of several essential components that collaborate to securely embed and retrieve authentication information within identity images. Each component is vital for ensuring strong, tamper-proof identity verification while preserving the integrity of the image.

1) Preprocessing Module: The preprocessing module improves image quality and identifies key facial characteristics needed for encoding. It prepares the ID image by implementing noise reduction, contrast enhancement, and feature extraction, creating optimal conditions for data insertion.

2) StegoFace Document Distributor: This component oversees the secure distribution and verification of ID images that have steganographically embedded data. It ensures that encoded images can be accurately verified without sacrificing their original quality.

3) BECC Translator: The Binary Error-Correcting Codes (BECC) Translator enhances the resilience of data by encoding authentication messages in a manner that protects against noise, compression, and possible distortions. It guarantees that the concealed data remains retrievable even in challenging circumstances.

4) Deep Convolutional ID Face Steganography: This component is made up of two primary parts:

Encoder: Embeds authentication data within ID images while preserving visual quality.

Auto Decoder: Extracts and validates the hidden message to detect unauthorized alterations.

5) Recurrent Proposal Network (RPN): The RPN is tasked with locating and identifying facial areas within ID images, ensuring that the authentication data is embedded accurately and securely, thus preventing tampering without detection. These components work together to bolster ID security, offering a deep learning-based steganography solution that delivers effective, scalable, and tamper-proof identity verification.

X. RESULTS OBTAINED

The StegoFace model effectively hid and recovered concealed messages without significant visual changes, ensuring image quality while following stringent security measures. The Recurrent Proposal Network (RPN) efficiently identified facial regions for precise message integration, and Binary Error-Correcting Codes (BECC) enhanced the resilience of messages to noise and compression. The Deep Autoencoder proficiently converted messages into high-resolution images, while the Deep Auto Decoder consistently extracted them with excellent accuracy and minimal data loss. The results confirm the system's efficacy in secure document verification, particularly for ID authentication and Machine-Readable Travel Documents (MRTDs). By employing RPN for feature identification, BECC for strength, and deep autoencoder-decoder methods, the system ensures seamless message embedding while maintaining image fidelity. The aim is to attain high accuracy in both encoding and decoding, safeguarding against distortions, noise, and compression artifacts, thereby positioning StegoFace as a highly trustworthy solution for secure identity verification.

Fig. 2: The project showcase page, introduction to the StegFace project.

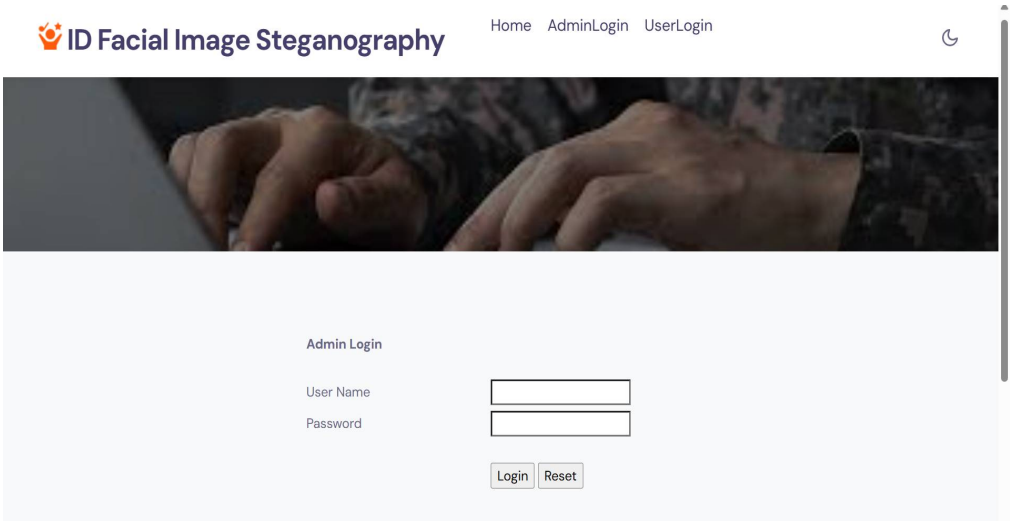


Fig. 3: Admin login page for accessing the encoding system.

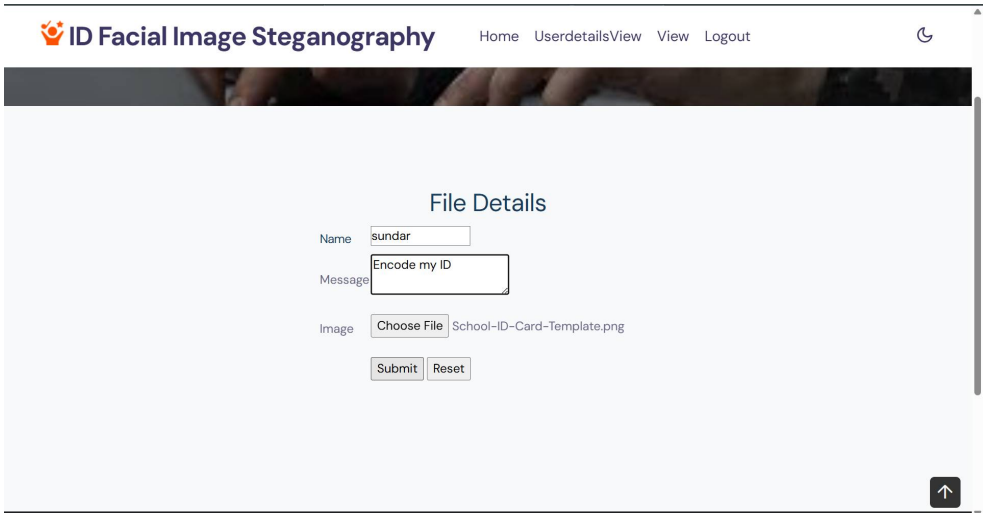


Fig. 4: Admin panel where images are uploaded and encoded with the required text.

Fig. 5: Displays the binary data output after extracting text and detecting a face in the image.

Fig. 6: The User Panel where users can upload an image and verify its encoded data.

Fig. 7: Displays the verification result as "Real", confirming that the uploaded image contains encoded binary data.

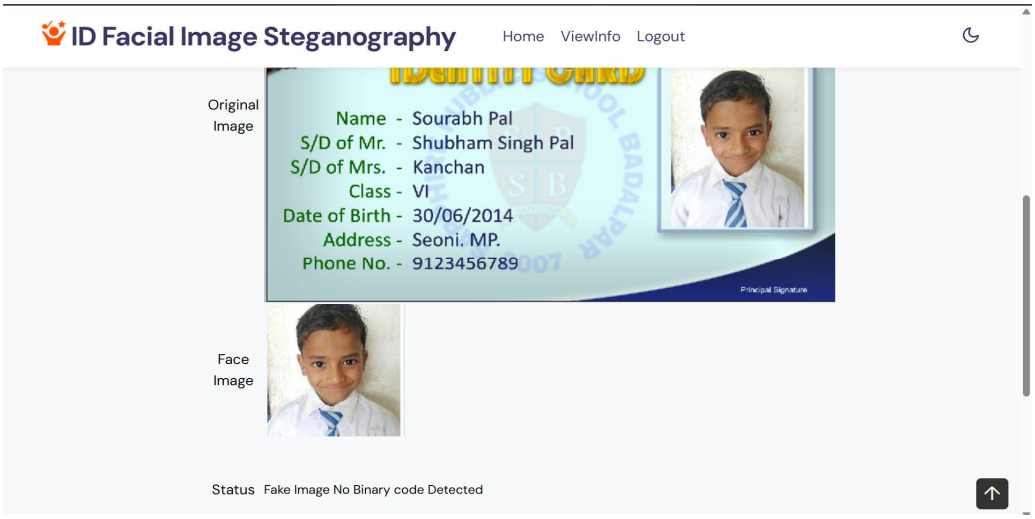


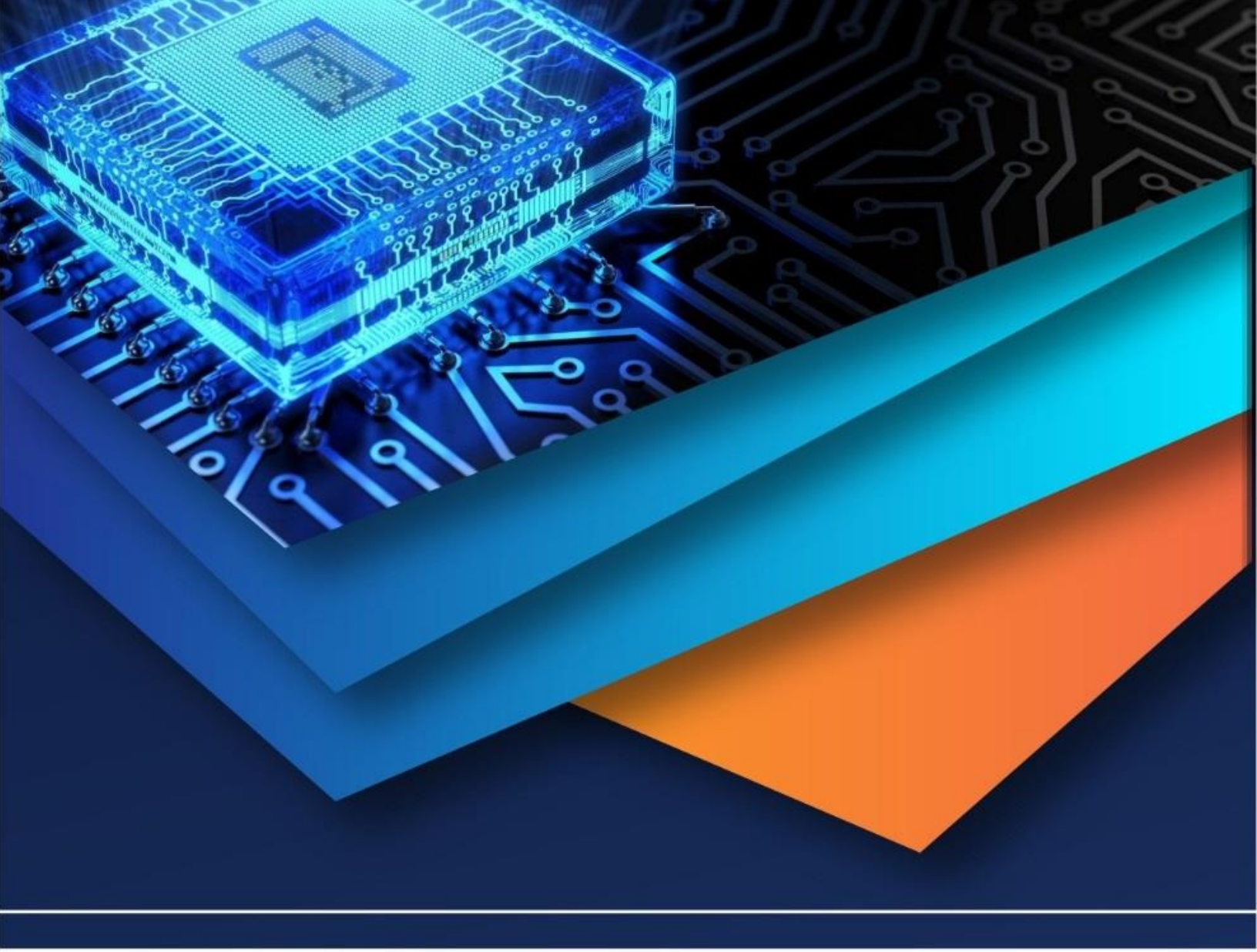
Fig. 8: Displays the verification result as "Fake Image - No Binary Code Data Detected", indicating that the uploaded image does not contain any encoded binary data.

XI. CONCLUSION

The security of identification verification systems continues to be a significant issue, as conventional techniques such as watermarks, microtext, and biometric validation remain susceptible to photo substitution attacks. The latest developments in deep learning and steganography have led to stronger solutions for protecting ID images, with research like VIP Print, BlazeFace, ArcFace, and steganography-based encryption advancing image verification and document safety. Building upon these advancements, StegoFace employs CNN-based steganography, Binary Error-Correcting Codes (BECC), autoencoder-decoder frameworks, and Recurrent Proposal Networks (RPNs) to integrate authentication information within ID images, guaranteeing tamper detection and resistance against unauthorized alterations. This system provides a scalable, affordable, and secure solution for identity verification in contexts such as government-issued IDs, travel documents, and access control systems. Subsequent research can further refine steganography methods and deep learning frameworks to bolster security against emerging threats in identity fraud.

REFERENCES

[1] Ferreira, A., Nowroozi, E., & Barni, M. (2021) – Proposed VIPPrint, a validation technique for detecting artificial photo modifications and source linking in printed documents.
[2] Deng, J., Guo, N., Xue, N., & Zafeiriou, S. (2019) – Introduced ArcFace, a deep learning-based facial recognition model with an additive angular margin loss, enhancing authentication accuracy.
[3] Jones, L., Wu, Y., Bi, D., & Eckel, R. A. (2019) – Designed a line phase code method for embedding hidden information within images to improve security.
[4] Jiménez Rodríguez, M., Padilla Leyferman, C. E., Estrada Gutiérrez, J. C., González Novoa, M. G., Gómez Rodríguez, H., & Flores Siordia, O. (2018) – Applied steganography techniques to drone-captured images, implementing chaotic encryption for secure data transmission.
[5] V. Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, "BlazeFace: Sub-millisecond neural face detection on cellular GPUs," 2019.
[6] S. Chen, L. Wang, and Y. Zhao**,** "A survey on deep-learning-based image steganography," 2024.
[7] J. Patel, A. Verma, and R. Singh**,** "A deep learning-driven multi-layered steganographic approach for secure information transmission," 2025.
[8] T. Nakamura, H. Lee, and M. Kim**,** "A new approach based on steganography to address facial recognition vulnerabilities against fake identities," 2024.
[9] K. Sharma, P. Gupta, and L. Das**,** "Reversible Face Recognition Using Deep Steganography" 2024.
[10] D. White, J. Roberts, and K. Brown, "Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review," 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY