iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55069

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 11 Issue VIII Aug 2023- Available at www.ijraset.com

Fake Face Detection in Identity Cards Using Stegoface

Sarulatha[1], Sreerambabu[2], Kalidasan[3], Mohammed Riyaz[4]
[1]*PG Scholar,* [2]*Head of the Department,* [3, 4]*Assistant Professor Dept of MCA*

Abstract: ***Identification and Machine-Readable Travel Documents (MRTDs) play a crucial role in verifying and validating identities in various situations, such as international travel, civil applications, online commerce, and access to transaction processing systems. These documents incorporate multiple security features aimed at preventing document forgery. However, criminals have shifted their focus to obtaining genuine documents fraudulently and manipulating facial portraits, as the existing security systems are challenging to bypass. To address this issue and mitigate the risks associated with such fraud, it is imperative for governments and ID/MRTD manufacturers to continually enhance and develop security measures. In this context, we present StegoFace, an innovative and efficient steganography method specifically designed for concealing secret messages within facial images found on common IDs and MRTDs. StegoFace employs an end-to-end approach, consisting of an ensemble of n Deep Convolutional Auto Encoders, which encode the secret message into a stegofacial image, and a Deep Convolutional Auto Decoder, capable of extracting the hidden message from the stegofacial image. Notably, our StegoFace approach outperforms the StegaStamp method in terms of perceptual quality, as evidenced by the results of metrics such as Peak Signal-to-Noise Ratio, hiding capacity, and imperceptibility on the test dataset.***

Keywords: IDs, MRTDs, identification, authentication, national borders, civil applications, sales, purchasing portals, transaction processing systems, security features, document forgery, criminal attacks, ID verification systems, fraudulent obtaining, manipulation, facial portraits, risks .

I. INTRODUCTION

Identity documents, such as ID cards and passports, are used to prove a person's identity. They can be issued in various forms and serve multiple purposes, including identification verification, travel, and accessing government benefits. Some countries have national identification cards, while others rely on regional or informal identification methods. The inclusion of photographs in identity documents, known as photo IDs, helps establish a connection between the document and the individual. However, there are challenges and security issues, such as counterfeit cards and identity theft.

Steganography is a technique used to hide secret information within non-secret documents or media, posing additional security challenges. Deep learning, a subset of artificial intelligence, plays a significant role in various applications, including image recognition and machine translation.

The objective of the project is to develop theft-resistant authentication mechanisms and conceal security-encoded data in identity and travel documents to combat counterfeiting. Additionally, the project aims to propose a facial image steganography method, develop a portable biometric system for document validation, and enhance decoding efficiency from smaller photos.

Overall, the project focuses on enhancing security measures and protecting against identity fraud while utilizing techniques like steganography and deep learning.

II. SYSTEM ANALYSIS

A. Existing System

Watermarks and micro text: These are designs added to ID cards during production to enhance security. Watermarks are customized and only visible when held a certain way, making duplication difficult. Microtext is tiny text printed on the card, hard to replicate if not known.

Laminate and holographic laminate: Holographic laminate adds an extra layer of visual security to ID cards, allowing easy validation. It is difficult to replicate due to customization and requires specific equipment.

Embedded technologies (magnetic stripes, barcodes, etc.): Used in access control systems, embedding technologies restrict access to secure Biometric data (fingerprints, digital signatures, etc.): Including biometric data in ID cards ensures high security. It verifies the cardholder's identity through layers, designs, and embedded technologies, reducing the risk of photo alterations.

Laser engraving: Laser engraving is a secure method of personalizing ID cards by etching features into the card body. It provides tamper-proof and durable personalization, making forgery and manipulation nearly impossible.

StegaStamp: StegaStamp is a steganography model that encodes and decodes hyperlinks in photos captured from real prints. It approximates distortions resulting from printing transmission, contributing to secure information concealment.

B. Proposed System

The proposed system, called StegoFace, is designed as a security method for verifying document portraits in IDs and MRTDs. It utilizes steganography models to encode and decode secret messages in facial images. StegoFace consists of an encoder and a decoder.

Recurrent Proposal Network (RPN): The RPN is a fully convolutional network that simultaneously predicts object bounds and objectless scores. It generates high-quality region proposals efficiently, considering a wide range of scales and aspect ratios using anchor boxes.

Binary Error-Correcting Codes algorithm: This algorithm is used to translate an arbitrary secret message into a binary message during encoding. During decoding, it translates the binary message back to the original secret message.

areas. Magnetic stripes and barcodes enable different security clearances for cardholders and facilitate quick identification.

Deep Convolutional Auto Encoder: The encoder network aims to optimize the trade-off between restoring the perceptual properties of input images and extracting the hidden message. It embeds the message in the cropped face, producing an encoded facial image to be printed on an ID card.

Deep Convolutional Auto Decoder: The decoder recovers the hidden message encoded in the facial image captured by a digital camera. It receives the encoded part, retrieves the message, and validates it using a hash function or checksum verification algorithm, ensuring the integrity of the face portrait.

III. DEVELOPMENT ENVIRONMENT

A. Hardware Requirement

Processor : Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz
RAM : 8GB Hard
Disk : 320GB

B. Software Requirement

Front End : HTML, CSS, JS
Back End : PYTHON
Database : My SQL
IDE : FLACK

IV. MODULE DESCRIPTION

A. StegoFace Document Distributor Dashboard

The StegoFace Document Distributor Dashboard is a web-based security concept that focuses on protecting the integrity of ID holder's portraits in documents. It incorporates an additional laser personalized portrait to prevent subsequent changes. The Generator Control Panel allows government regulators to upload ID cards, where the facial image and secret message are encoded using advanced algorithms. The Verifier Control Panel enables authorized verifiers to upload ID cards and decode the encoded portraits, recovering the secret message and verifying the portrait's integrity. This system utilizes deep learning methods and provides robust document security while maintaining facial recognition capabilities.

B. Preprocessing Module

The system comprises a Preprocessing Module that extracts meaningful features from face images, reducing redundant data and optimizing processing time. It resizes the input secret image to match the cover image size and converts images into useful features through convolutional layers. The Face Detection module utilizes a region proposal network (RPN) and PRnet for accurate face detection and segmentation. The Cropper module crops the face region for encoding. The system employs a Binary Error-Correcting Codes (BECC) algorithm, specifically Hamming codes, for error detection and correction during message transmission.

Overall, these modules enhance the system's ability to preprocess images, detect faces, and encode secret messages with error correction, facilitating secure ID verification.

C. Deep Convolutional ID Face Steganography

The Deep Convolutional ID Face Steganography system includes an Auto Encoder and an Auto Decoder. The Auto Encoder encodes the input face image and secret message into an encoded image using a UNet-based architecture. It preserves the information of the secret message by removing pooling layers. The embedding network, along with the preprocessing module, has an hourglass structure and generates a latent space that reconstructs the stego face resembling the cover image. The Auto Decoder recovers the message encoded in the facial image and incorporates a Region Proposal Network (RPN) for cropping and normalizing the scale. The extraction network, similar to the embedding network, extracts the hidden secret image using convolutional layers. Validation is performed using a convolutional layer to construct the extracted secret image.

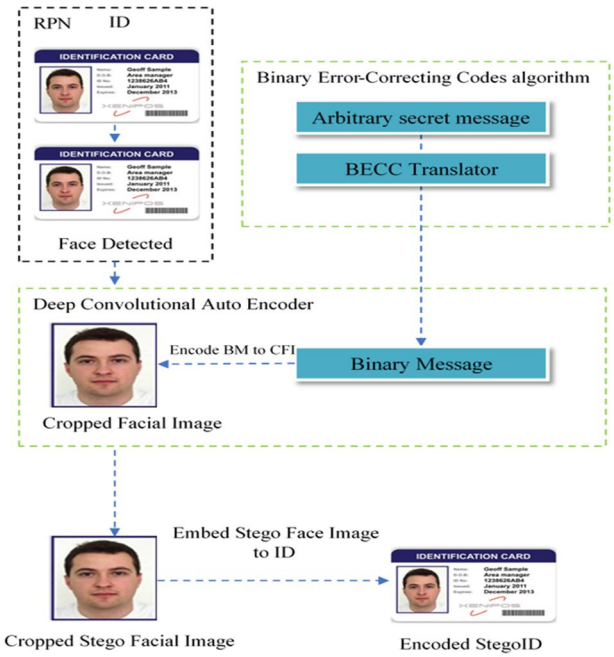
D. Loss Function

The StegoFace system incorporates a customized loss function consisting of an embedding loss and an extraction loss. The embedding loss measures the dissimilarity between the input cover image and the output StegoFace, while the extraction loss measures the dissimilarity between the input secret image and the extracted secret image. By optimizing these losses, the model aims to enhance its performance. The loss function is tailored to provide feedback during training, with the embedding network's loss used to update the embedding network and the overall loss minimizing distortions in the extracted secret image. The error adjustment parameter α is set to 0.3 based on experiments for optimal results.

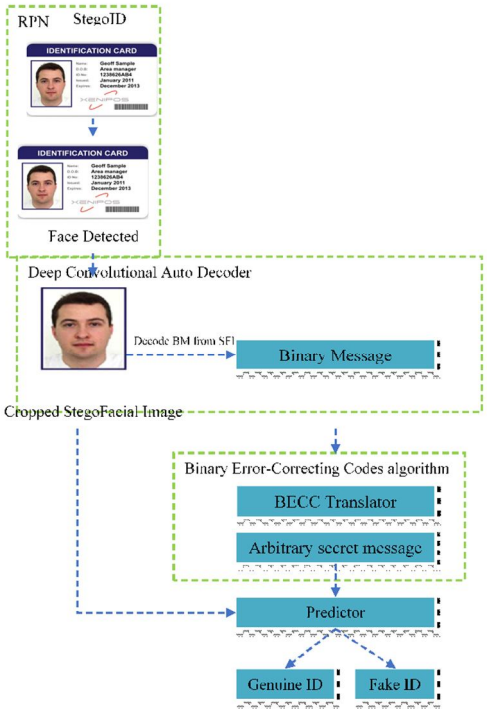
E. Performance Evaluation

Steganographic techniques are evaluated based on imperceptibility, payload capacity, security against statistical attacks, robustness against image manipulation, and peak signal-to-noise ratio (PSNR). Imperceptibility aims to conceal the presence of hidden data to avoid suspicion. Payload capacity refers to the ratio between the cover medium and the secret message, balancing capacity with imperceptibility. Security against statistical attacks ensures that no artifacts or signatures reveal the hidden data. Robustness against image manipulation ensures resistance to corruption during transmission or modifications. PSNR measures the similarity between cover and stego images, with higher values indicating better quality and similarity. These evaluations help assess the effectiveness and performance of steganographic techniques.

V. SYSTEM DESIGN



Deep Convolutional Auto Encoder



Deep Convolutional Auto Decoder

VI. CONCLUSION

In conclusion, this paper presents StegoFace, an efficient steganography method tailored for concealing security encoded data in ID and MRTD documents while ensuring portrait integrity verification. StegoFace utilizes an end-to-end Deep Learning Network comprising a Deep Convolutional Auto Encoder to encode secret messages within facial images, producing the encoded image, and a Deep Convolutional Auto Decoder to decode messages from previously printed and captured images. Unlike existing methods, StegoFace enables image usage in their original context regardless of the background, eliminating photo parameter restrictions. Our approach outperforms StegaStamp in terms of perception quality, demonstrating higher security, robustness, imperceptibility, and information hiding capacity.

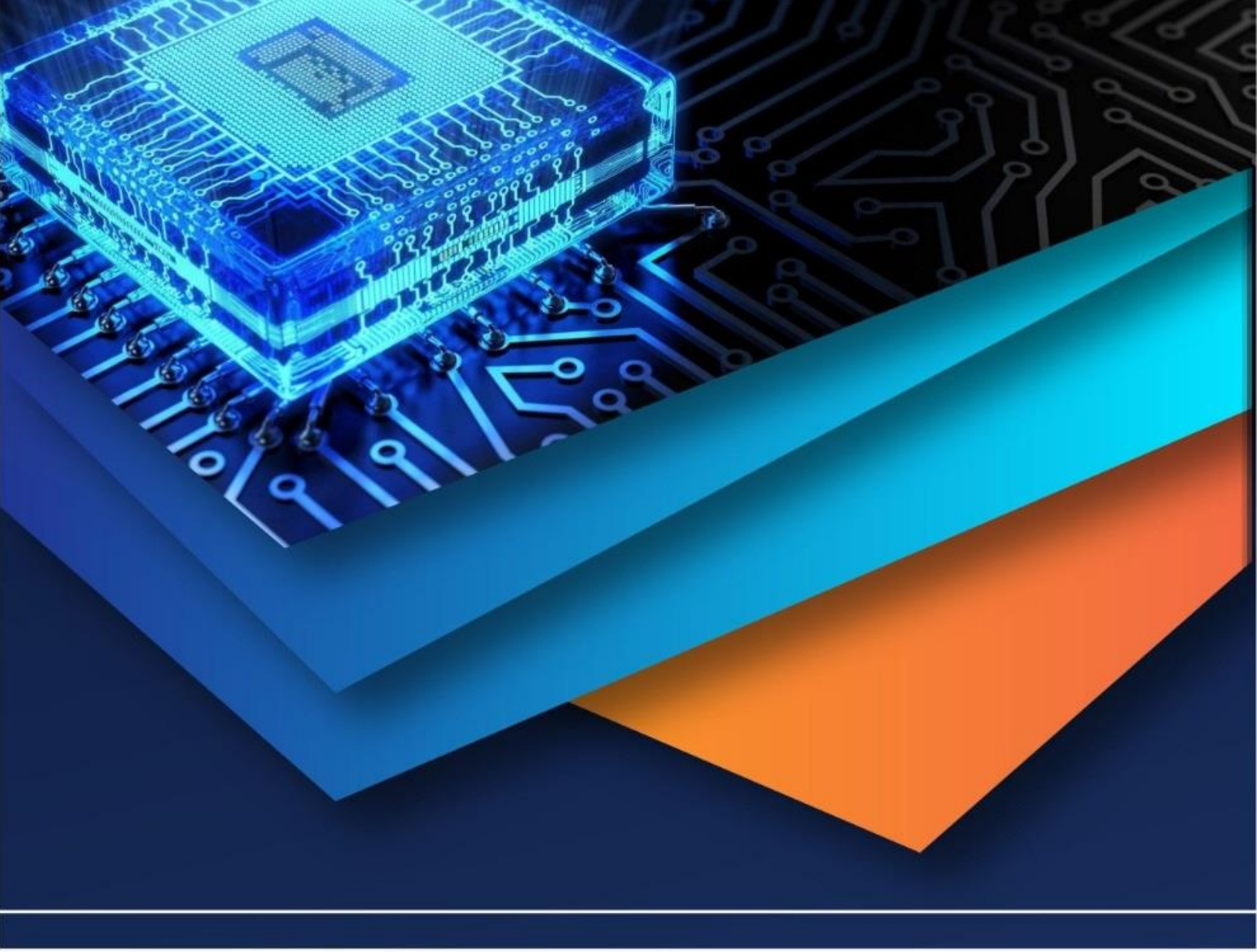
VII. FUTURE ENHANCEMENT

The novel idea proposed in this research is to attach a resize network to our model as an additional noise simulation module. This is designed to help the decoder read messages from smaller photos in comparison with previous approaches. The resize network decreases the size of the encoded images that the decoder receives. Facial images encoded with our StegoFace approach outperform the StegaStamp generated images in terms of their perception quality.

REFERENCES

[1] A. Ferreira, E. Nowroozi, and M. Barni, ‘‘VIPPrint: Validating synthetic image detection and source linking methods on a large-scale dataset of printed documents,’’ J. Imag., vol. 7, no. 3, p. 50, Mar. 2021.
[2] V. Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, ‘‘BlazeFace: Sub-millisecond neural face detection on mobile GPUs,’’ 2019, arXiv:1907.05047.
[3] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ‘‘ArcFace: Additive angular margin loss for deep face recognition,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4685–4694
[4] R. L. Jones, Y. Wu, D. Bi, and R. A. Eckel, ‘‘Line segment code for embedding information,’’ U.S. Patent App. 16 236 969, Jul. 4, 2019.
[5] S. Ciftci, A. O. Akyuz, and T. Ebrahimi, “A Reliable and Reversible Image Privacy Protection Based on False Colors,” IEEE Transactions on Multimedia, vol. 20, no. 1, pp. 68–81, 2018.
[6] M. Jiménez Rodríguez, C. E. Padilla Leyferman, J. C. Estrada Gutiérrez, M. G. González Novoa, H. Gómez Rodríguez, and O. Flores Siordia, “Steganography applied in the origin claim of pictures captured by drones based on chaos,” Ingeniería e Investigación, vol. 38, no. 2, pp. 61–69, 2018.
[7] L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, ‘‘DeepLab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 4, pp. 834–848, Apr. 2018.

[8] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos-based S-Box," Chaos, Solitons & Fractals, vol. 95, pp. 92–101, 2017.
[9] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," Multimedia Tools and Applications, vol. 75, no. 17, pp. 10631–10648, 2016.
[10] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," Neural Computing and Applications, vol. 26, no. 5, pp. 1137–1148, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY