IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Face Counterfeit Detection In National Identity Cards Using Deep Learning

Kaviyarasu S , Karan S , Mathish P , Nandhakumar N (Students)

Ms.Umapriya., Assistant Professor , Department Of Computer Science Engineering,

Hindusthan College Of Engineering And Technology, Coimbatore.

ABSTRACT :

A National Identity document is an Identity card with a photo, usable as an identity card at least inside the country, and which is issued by an official authority. The most common applications for these smart cards are smart to travel documents, electronic IDs, electronic signatures, municipal cards, key cards used to access secure areas or business infrastructures, social security cards, etc. These documents have several security features which mitigate and combat document forgery. As these security systems are difficult to circumvent, criminal attacks on ID verification systems are now focusing on fraudulently obtaining genuine documents and the manipulation of the facial portraits. Trusted identity is a vital component of a well-functioning society. To reduce risks related to this fraud problem, it is necessary those governments and manufacturer of IDs continuously develop and improve security measures. With this in mind, we introduce the first efficient steganography method - StegoCard - which is optimized for facial images printed in common IDs. StegoCard is an end-to-end facial image steganography model that is formed by n Deep Convolutional Auto Encoder, that can conceal a secret message in a face portrait and, hence, producing the stego facial image, and a Deep Convolutional Auto Decoder, which is able to read a message from the stego facial image, even if it is previously printed and then captured by a digital camera. Facial images encoded with our StegoCard approach outperform the StegaStamp generated images in terms of their perception quality. Peak Signal-to-Noise Ratio, hiding capacity and imperceptibility results on the test set are used to measure the performance.

INDEX TERMS : Smart Cities , Digital ID , Deepfake , Facial authentication system , Convolutional Neural Network , RPN , BECC Translator etc..,

INTRODUCTION

An identity document (also called a piece of identification or ID, or colloquially as papers) is any document that may be used to prove a person's identity. If issued in a small, standard credit card size form, it is usually called an identity card (IC, ID card, citizen card),[a] or passport card.[b] Some countries issue formal identity documents, as national identification cards which may be compulsory or non-compulsory, while others may require identity verification using regional identification or informal documents. When the identity document incorporates a person's photograph, it may be called photo ID.

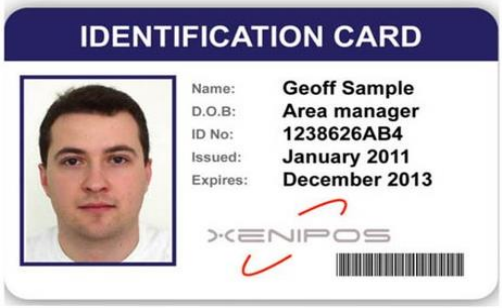


Figure 1.1. Identity Card

In the absence of a formal identity document, a driver's license may be accepted in many countries for identity verification. Some countries do not accept driver's licenses for identification, often because in those countries they do not expire as documents and can be old or easily forged. Most countries accept passports as a form of identification. Some countries require all people to have an identity document available at any time. Many countries require all foreigners to have a passport or occasionally a national identity card from their home country available at any time if they do not have a residence permit in the country.

PROPOSED SYSTEM

The proposed system is called StegoFace. The StegoFace is a model to encode and decode a secret message in facial images in the context of IDs and MRTDs. Our model is the first one to be designed as a security method for the verification of document portraits and it is inspired by steganography models.

Region Proposal Network (RPN)

Region Proposal Network, or RPN, is a fully convolutional network that simultaneously predicts object bounds and objectless scores at each position. The RPN is trained end-to-end to generate high-quality region proposals. RPNs are designed to efficiently predict region proposals with a wide range of scales and aspect ratios. RPNs use anchor boxes that serve as references at multiple scales and aspect ratios.

Binary Error-Correcting Codes algorithm

During encoding, an arbitrary secret message is translated to a binary message using a Binary Error-Correcting Codes algorithm. Subsequently during decoding, the same Binary Error-Correcting Code algorithm translates the binary message to a string with the secret message.

Deep Convolutional Auto Encoder

The first part of the generator is the encoder network. The aim of the encoder training process is to optimize the trade-off between its ability to restore the perceptual properties of the input images and the decoder performance to extract the hidden message. In the encoder, the facial image and the secret message are first received as inputs. At the end of the encoder application, a pretrained encoder model embeds the message in the cropped face and produces an encoded facial image. The encoded cropped image then replaces the original facial image which is subsequently printed on an ID card.

Deep Convolutional Auto Decoder

The decoder is designed to recover a message that is encoded in a facial image. As for the decoder, the ID card's encoded facial image is captured by a digital camera. The face detection module then detects the encoded part of the facial image, which the StegoFace decoder network then receives, retrieving the hidden message. Then the final resulting message, the retrieved message, is checked using a hash function or checksum verification algorithm to validate the message, thus providing a way to check the integrity of the face portrait in IDs and MRTDs.

LITERATURE SURVEY

1. Steganographic Secret Sharing With GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT.

Author: *Sisheng Chen; Ching-Chun Chang; Isao Echizen.*

Year: *2021*

Doi: *https://ieeexplore.ieee.org/document/9514916*

Objective

This paper proposes a secure message authentication scheme based on steganographic secret sharing for building trust in IoT systems. In this scheme, the message is split and distributed to two participants by a dealer, and it can be revealed only when the two authorized participants grant their consents.

Findings

The simulation experiments and analysis show the feasibility and security of the proposed secret sharing scheme. The cover of meaningful images and the new properties of the extractor assure the security of the secret shares.

2. Forensic Digital Data Tamper Detection Using Image Steganography and S-Des
Author: *Isaac Baffour Senkyire; Emmanuel Addai Marful; Eric Adjei Mensah*

Year: *2021*

Doi: *https://ieeexplore.ieee.org/document/9706596*

Objective

This paper focuses on protecting and securing data by hiding the data using steganography techniques, after encrypting the data to avoid unauthorized changes or modification made by adversaries to the data through using the Simplified Data Encryption Technique.

Findings

By leveraging on these two approaches, secret data security intensifies to two levels and a steganography image of high quality is attained.

3. Fake Safe: Human Level Steganography Techniques by Disinformation Mapping Using Cycle-Consistent Adversarial Network
Author: *He Zhu; Dianbo Liu*

Year:*2021*

Doi: *https://ieeexplore.ieee.org/document/9623552*

Objective

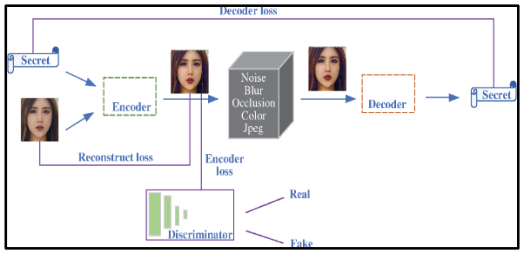
In this paper, the author proposes Fake Safe, a novel cycle-consistent adversarial network proffering human-level steganography. Mapping the confidential information into fake messages, Fake Safe efficaciously precludes the detection of steganalysis algorithms and human eyes.

Findings

Fake Safe method furnishes users the flexibility to map private data onto various data domains depending on use cases. Fake Safe can be efficiently utilised in combination with conventional data protection technologies but focuses on human-level steganography which considers human factors in data security and privacy protection.

PROJECT DESCRIPTION

The StegoFace is a model to encode and decode a secret message in facial images in the context of IDs and MRTDs. Our model is the first one to be designed as a security method for the verification of document portraits and it is inspired by steganography models such as StegoFace is composed of two processes: the encoder and the decoder.



StegoFace Network

In the encoder, the facial image and the secret message are first received as inputs. The relevant part of the image is detected and cropped using a face detection model. Simultaneously, the secret message is coded by a binary error correcting codes algorithm. At the end of the encoder application, a pretrained encoder model embeds the message in the cropped face and produces an encoded facial image. The encoded cropped image then replaces the original facial image which is subsequently printed on an ID card.

As for the decoder, the ID card's encoded facial image is captured by a digital camera. The face detection module then detects the encoded part of the facial image, which the StegoFace

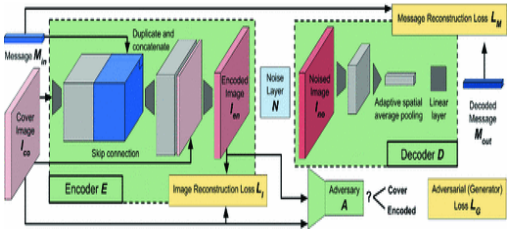
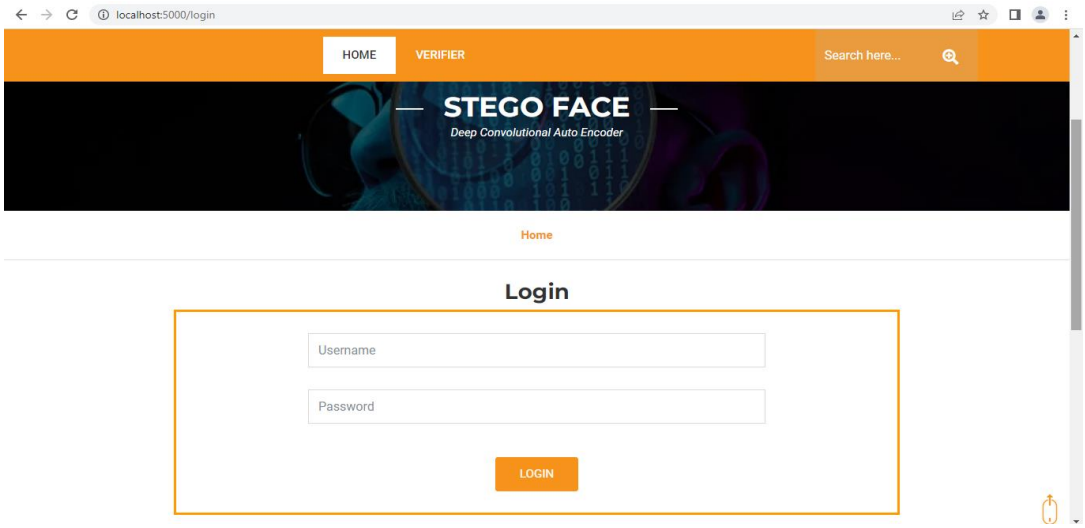
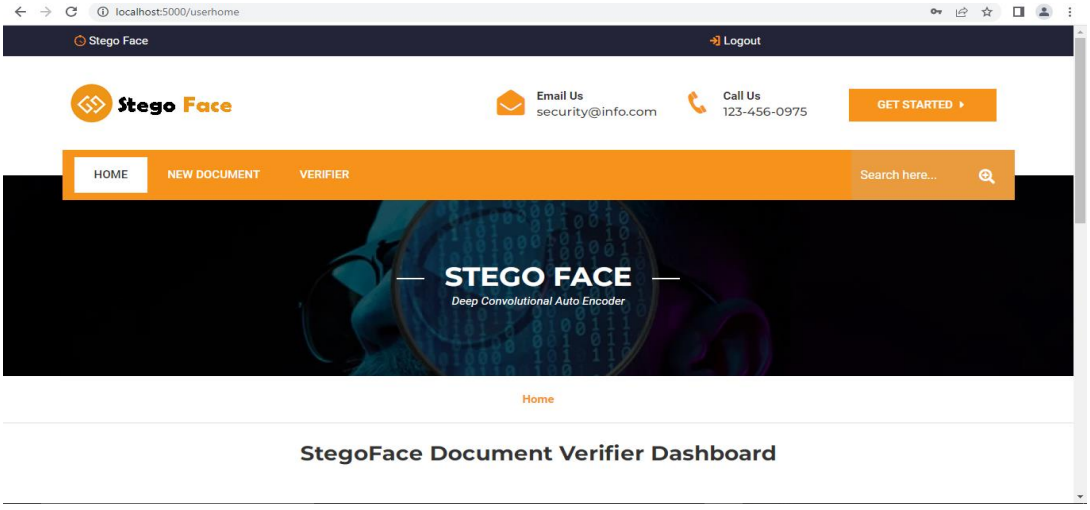


Figure 4.2. Encoder-Decoder Network

network then receives, retrieving the hidden message. A binary-error codes algorithm converts the retrieved binary message into a number or a string. Then the final resulting message, the retrieved message, is check edusing a hash function or checksum verification algorithm to validate the message, thus providing a way to check the integrity of the face portrait in IDs and MRTDs.

SAMPLE OUTPUT SCREENSHOTS





CONCLUSION

The focus of this paper is on concealing security encoded data in ID and MRTD documents while allowing for the integrity verification of the portrait. With this in mind, we introduce the first efficient steganography method - StegoFace - which is optimized for facial images printed in common IDs and MRTDs. StegoFace is an end-to-end Deep Learning Network that is formed by a Deep Convolutional Auto Encoder, that can conceal a secret message in a face portrait and, hence, producing the encoded image and a Deep Convolutional Auto Decoder, which is able to read a message from the encoded image, even if it is previously printed and then captured by a digital camera. StegoFace surpasses state-of-the-art methods in allowing the use of images in their context, irrespectively of the background. This feature also allows us to use the method without any restrictions relating to photo parameters. The novel idea proposed in this research is to attach are size 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. From the results shown, it can be clearly seen that the proposed architecture has higher security, robustness, imperceptibility and information hiding capacity.

REFERENCES

1. A. Ferreira, E. Nowroozi, and M. Barni, ‘‘VIPPrint: Validating syntheticimage detection and source linking methods on a large-scale dataset ofprinted 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 angularmargin 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 forembedding 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.