IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12553

COUNTERFIET DETECTION IN NATIONAL IDENTITY CARDS USING IMAGE STEGANOGRAPHY

Mounica.R[1], Nikitta Joshie.J[2], Sahaya Rani.A[3], Geetha.G[4]

Assistant Professor, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[1]

B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[2-4]

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.

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indAn identity document (also called a piece of identification or ID, or colloquially as papers) is any documents 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) or passport card. 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 documents or informal documents.When the identity document incorporates a person's photograph, it may be called photo ID. Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. Steganography has been used for centuries, but these days, hackers and IT pros have digitized the word "steganography" seems fancy, but it actually comes from a fairly normal place. The root "steganos" is Greek for "hidden" or "covered," and the root "graph" is Greek for "to write." Put these words together, and you've got something close to "hidden writing," or "secret writing." The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways. Where cryptography is a science that largely enables privacy, steganography is a practice that enables secrecy – and deceit.

1.2. OBJECTIVE OF THE PROJECT:

To counteract counterfeit documentation, theft resistant authentication mechanisms must be built into identity cards to prove the identity assertions that are made, and to protect the true and legitimate identity.To conceal security encoded data in ID and MRTD documents while allowing for the integrity verification of the.To develop a portable and efficient biometric system for validating ID and travel documents.To attach a resize network to our model as an additional noise simulation module.To help the decoder read messages from smaller photos in comparison with previous approachesicated on the conference website. Information about final paper submission is available from the conference website.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12553

II. LITERATURE SURVEY

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

In this paper, the author proposes a secret sharing scheme via deep learning-based steganography and image morphing technique, which takes face images as cover images. The authors first train a generator via a generative adversarial network (GAN) and independent extractors based on CNN with shared participant keys. The secret shares are hidden in the shadow images using the generator with participant keys. Then, the dealer takes the shared participant images as source images and the shadow images as target images to generated morphed images for shadow image authentication.

2.2. Forensic Digital Data Tamper Detection Using Image Steganography and S-Des. Cryptography converts plaintext into cipher text (unreadable text); whereas steganography is the technique of hiding secret messages in other messages. First encryption of data is done using the Simplified Data Encryption Standard (S-DES) algorithm after which the message encrypted is embedded in the cover image by means of the Least Significant Bit (LSB) approach.

2.3. FakeSafe: Human Level Steganography Techniques by Disinformation Mapping Using Cycle-Consistent Adversarial Network. The FakeSafe method aims to map the original private information onto a fake but realistically looking message. The author constructs a multi-step FakeSafe mapping with a cascade of stenographic functions, which significantly ensures the safety of sensitive data. Even if the attackers know the message is fake, they may not recognize how many steps the messages were mapped. Then design a steganography method applicable to various data domains, including image and text information. The fake message can be either from the same domain of the original private information or from a completely different domain, which drastically enhances the framework's robustness. Then introduce a coverless solution to conduct steganography. Unlike the conventional steganography methods, which require a dedicated cover for secret information embedding, our model enshrouds the hidden messages in the medium of a particular category. This approach greatly satiates the demands of those who wish to simplify the steganographic procedure without a premeditated container.

2.4. A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans.

Medical data confidentiality is important because disclosure diminishes patient candor thereby compromising health care. The author proposed a method where patient information is inserted inside the patient scans in an encrypted format. The proposed procedure is having three stages. The first stage is the dual encryption of data, the second stage is search for an image window where the data is to be inserted. And the third stage is data insertion in the LSB of the image.

2.5. StegaStamp: Invisible Hyperlinks in Physical Photographs.

The inputs are an image and a desired hyperlink. First, assign the hyperlink a unique bit string (analogous to the process used by URL-shortening services such as tinyurl.com). Second, use our StegaStamp encoder to embed the bit string into the target image. This produces an encoded image that is ideally perceptually identical to the input image. Third, the encoded image is physically printed (or shown on an electronic display) and presented in the real world. Fourth, a user takes a photo that contains the physical print. Fifth, the system uses an image detector to identify and crop out all images. Sixth, each image is processed with the StegaStamp decoder to retrieve the unique bitstring, which is used to follow the hyperlink and retrieve the information associated with the image.

2.6. A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers.

A multi-layer data encryption and decryption scheme that uses the science of steganography and cryptography is proposed and developed. The operators of GA such as selection, crossover and mutation are leveraged on at different levels of encoding and decoding in order to build a secure and robust data encryption and decryption scheme. The desirable features of RNS such as residues and parallelism together with a fusing criterion to embed text within images are also employed to further enhance the security, robustness and the throughput of the scheme.

2.7. Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment.

To conquer these problems, the author designs a novel robust image coverless information hiding system using Faster Region-based Convolutional Neural Networks (Faster-RCNN). Then employ Faster-RCNN to detect and locate objects in images and utilize the labels of these objects to express secret information. Since the original images without any modification are used as stego-images, the proposed method can effectively resist steganalysis and will not cause attackers' suspicion.

DOI: 10.17148/IJARCCE.2023.12553

2.8. Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning. Reinforcement learning is widely applied in many areas, including controlling robots, managing merchandise inventory, and playing game. It can adapt to the changing environment and response with a series of corresponding actions to approach ultimate goals. This approach is based on visual attention mechanism and reinforcement learning. The attention mechanism is to focus on a selected region with ‘‘high resolution’’, and to use ‘‘low resolution’’ to perceive the surrounding pixels roughly. In the field of computer vision, attention mechanism can be realized in various forms, which can be roughly divided into soft attention and hard attention.

2.9. A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks.
In this work, the author proposes a new SWE method based on DCGANs. We establish a relationship between the secret information and a noise vector, which is the input of DCGANs. Stego images are generated by the generator in DCGANs according to preprocessed secret information, and no information is embedded in stego images during the generation period. Another convolutional neural network (CNNs) called the extractor is designed to recover the secret information from these stego images.

2.10. New Secret Sharing Scheme Based on Faster R-CNNs Image Retrieval.
The author proposes a novel secret sharing scheme that utilizes the representation capability of deep learning. Then need to send a query image rather than all shadow images to all participants, thus reducing the risk and the load on network communications. A novel approach is put forward to ensure security and specificity for shadow images.

The sender is the owner of a database with more than ten thousand images. If any cheating events occurred, the sender could replace the shadow images in the database immediately. The security of the secret image is further improved. Since the search results may change according to the change of the database content, the sender can also use this feature to update the query image to enhance the security in real time.

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. StegoFace is composed of two processes: the encoder and the decoder.

Recurrent 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. The scheme can be thought of as a pyramid of regression references, which avoids enumerating images or filters of multiple scales or 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.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12553

Advantages

- Higher security, robustness, imperceptibility and information hiding capacity.
- Light-weight but simple architecture is proposed to achieve end-to-end ID facial image steganography.
- Reducing any suspicion and scrutiny.
- StegoFace with the resize layer can better read a message from a smaller image
- StegoFace presents an innovation that can be easily implemented in real world document validation systems and applied directly to ID cards and MRTDs as a security protocol.
- lower cost of implementation

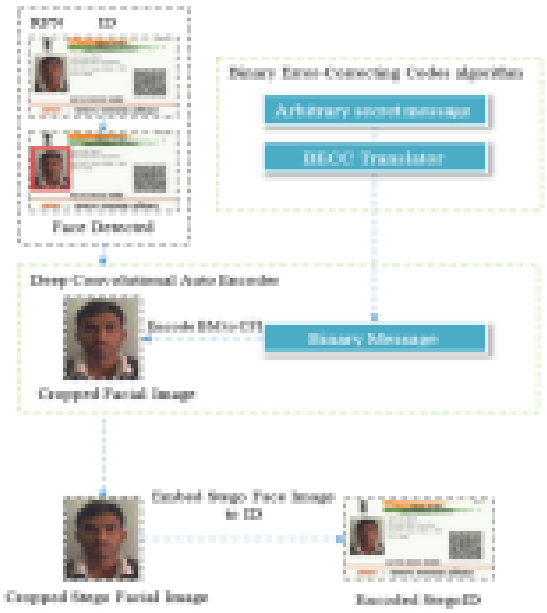


Fig.1 Deep Convolutional Auto Encoder

Fig.2 Deep Convolutional Auto Decoder

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12553

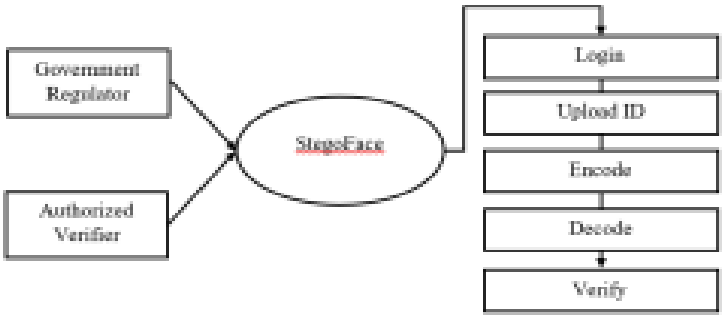
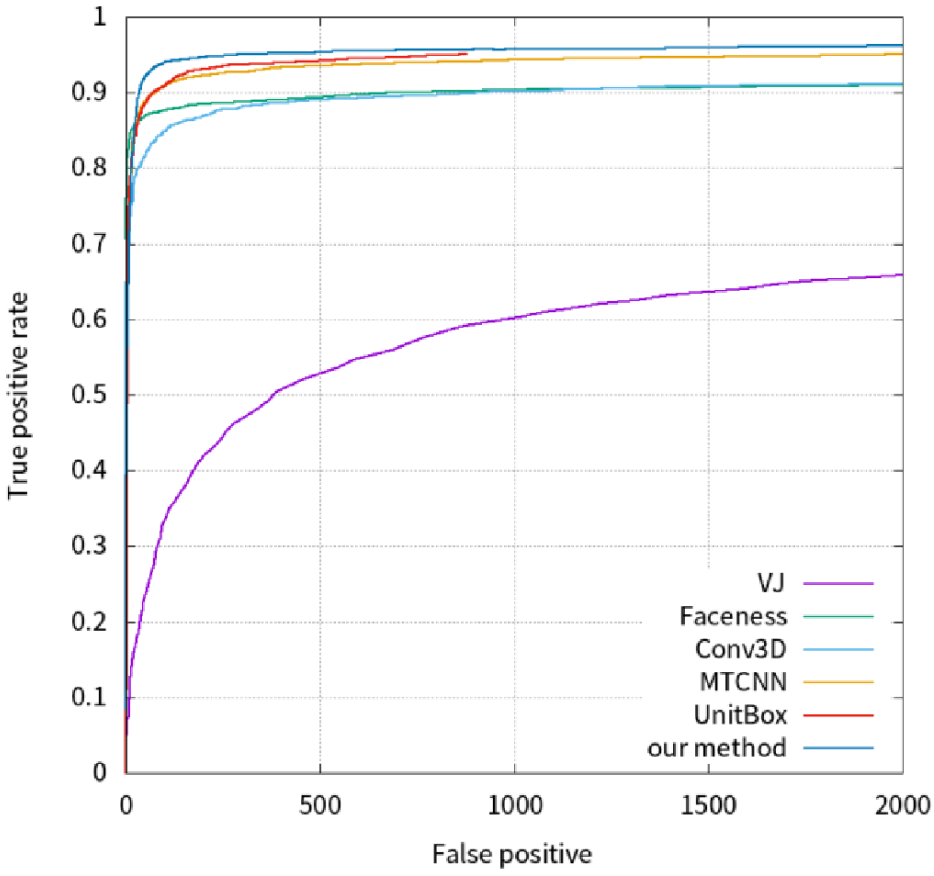


Fig.3 Verifier control panel

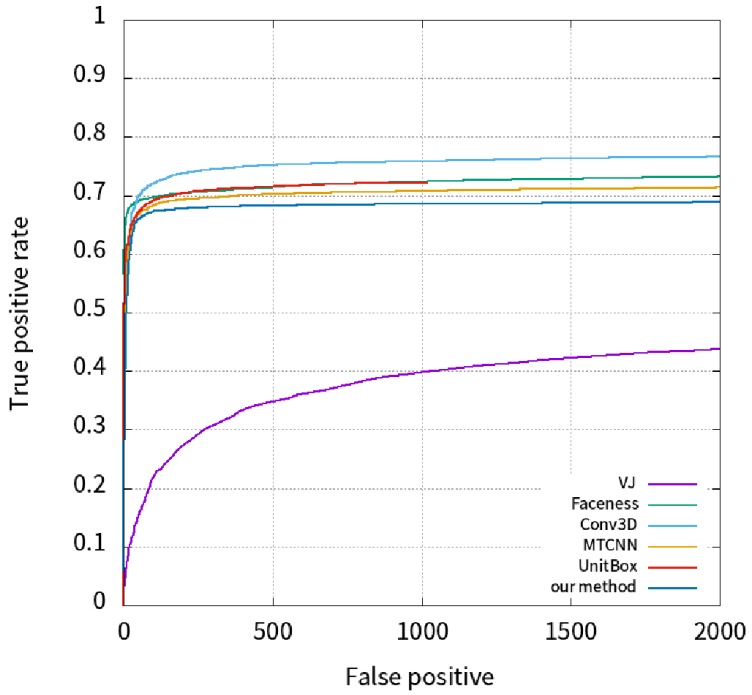
RESULTS AND DISCUSSION

To evaluate the performance of our method, we compare our method against the state-of-the-art methods in FDDB. The evaluation indicators include: recall rate is used to evaluate the proportion of the detected face to the total face of the sample mark; false positive is the number of errors in the detected face. These two indicators are expressed by the ROC (Receiver Operating Characteristic) curve.



a. Discontinuous ROC Curves

DOI: 10.17148/IJARCCE.2023.12553



The results are shown in FIGURE. 1(a) and FIGURE.1(b). The ROC curve detection results show that the traditional face detection method VJ recall rate is only 66.6%, the detection method based on deep learning has been greatly improved. Our method achieves state-of-the-art performance in terms of both the discrete ROC curve and continuous ROC curve. Our discrete ROC curve is superior to the MTCNN.We also obtain the best true positive rate of the discrete ROC curve at 2000 false positives (96.1%). In addition, the possible influencing factor is that our method is not very effective in detecting the side face.

The ROC curve does not clearly indicate which method is better, so another indicator AUC is used to illustrate the pros and cons of the method. AUC represents the area proportion under the ROC curve and the value is between 0 and 1. The higher the AUC value is, the better the method performance will be. Then test on the WIDER FACE dataset, WIDER FACE is a more challenging benchmark than FDDB in face detection. It is very encouraging to see that our model consistently achieves the competitive performance across the three subsets. It has higher robustness for faces with large occlusion and Angle change, which is basically consistent with the evaluation results in the FDDB dataset.

V. 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. 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 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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12553

[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.

