Face Counterfeit Detection in National Identity Cards Using Image Steganography Deep Learning Techniques

[1]N.DEEPASRI, [2]Ms. K.MEENATCHI,

[1]MCA, [2]MCA, M.Phil, ASSISTANT PROFESSOR,
A.R.J COLLEGE OF ENGINEERING AND TECHNOLOGY, MANNARGUDI.

Abstract-
IDs and MRTDs (Identification and Machine-Readable Travel Documents) are used to identify and authenticate identities in several scenarios such as crossing national borders, in civil applications, sales and purchasing portals, or admission to transaction processing systems. 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. To reduce risks related to this fraud problem, it is necessary those governments and manufacturer of IDs and MRTDs continuously develop and improve security measures. 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 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 Stego Face 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

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. 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.The identity document is used to connect a person to information about the person, often in a database. The photo and the possession of it is used to connect the person with the document. The connection between the identity document and information database is based on personal information present on the document, such as the bearer's full name, age, birth date, address, an identification number, card number, gender, citizenship and more. A unique national identification number is the most secure way, but some countries lack such numbers or don't mention them on identity documents.

II.SOFTWARE DESCRIPTION

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language. Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer especially when they are working in Web Development Domain. Python is often described as a "glue language," meaning it can let disparate code (typically libraries with C language interfaces) interoperate. Its use in data science and machine learning is in this vein, but that's just one incarnation of the general idea. If you have applications or program domains that you would like to hitch up, but cannot talk to each other directly, you can use Python to connect them.

III. LITERATURE SURVEY

In this paper, the author proposes a new self-seeking steganalysis method based on visual attention and deep reinforcement learning to detect the JPEG-based adaptive steganography. 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 which can be roughly divided into soft attention and hard attention. 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. 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.

IV.EXISTING SYSTEM

Water marks are designs that can be either visible or invisible and are put onto the ID card during production. Water marks make it more difficult for cards to be duplicated as they can be customized and only visible when held a certain way. Micro text is extremely tiny text that is printed onto the card somewhere, and it is hard to replicate if people don't know to look for it. Holographic laminate on ID cards adds an extra layer of visual security. Drivers' licenses have holographic laminate so that people can easily decipher whether or not it is valid. Not only is it hard to replicate holographic laminate because you have to have the right computer, it's also secure in that the design of the laminate is customized as well. Used mostly for access control ID card systems, embedding technologies in your ID cards is perfect for keeping buildings and campuses secure as access to different areas is restricted for those without the proper ID card. Using magnetic stripes, you can also designate different levels of security clearance for different card holders so that they have access to the proper places. Barcodes are also great for quickly and easily identifying ID cards as legitimate to your ID card system or not. Perhaps the most secure security features you can include in your ID cards is biometric data. This data goes being layers, design, and embedded technologies and makes sure that the card holder is who they say they are. Photo ID cards can greatly reduce security threats; however, photos can be altered and so can people's appearances. With fingerprints, and digital signatures included on the ID cards you can make absolutely sure that the ID card actually belongs to

the cardholder. Laser engraving is a highly secure method of monochrome card personalization that etches features into the card body itself. This provides tamper-proof and highly durable personalization, making forgery and manipulation virtually impossible. Attempts to alter engraved information will result in visually evident card damage.

V.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. 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.

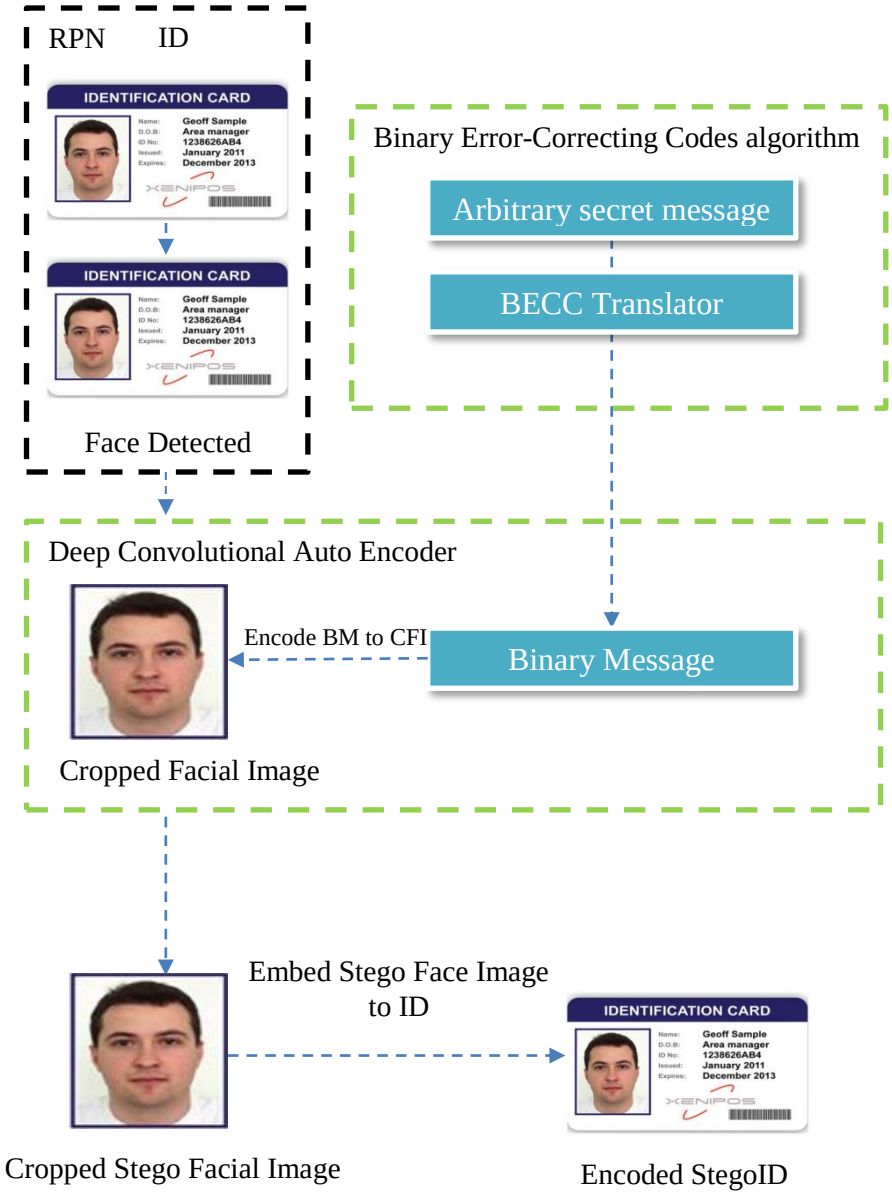

Fig.6a. **Deep Convolutional Auto Encoder Diagram**

StegoFace is a new web-based security concept. It is designed to protect the ID holder's portrait against any subsequent change through an additional laser personalized portrait. The focus of this dashboard is on

concealing security encoded data in ID and MRTD documents while allowing for the integrity verification of the portrait. In terms of document security, it is also important to maintain the system's ability to recognize persons using facial recognition algorithms.The preprocessing module resizes the secret image to 256 x 256 since the cover image and the secret image should be of same size. The resize function from the skimage library is used to resize the cover image and the secret image to a fixed size of 256 x 256. Instead of representing the input images as color gradients, the preprocessing module converts them into useful features that can be used by the embedding network. The preprocessing module consists of one input layer and three convolutional layers with increasing number of filters. The choice of the number of filters, filter size and the stride are purely dependent on the application.

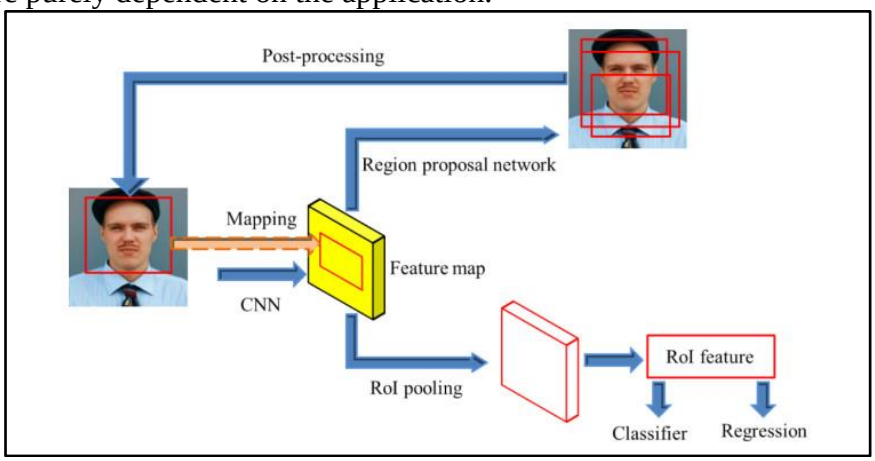

Fig.6.b Region Proposal Network

Face Detection from faces with background needs face segmentation. To localize the face, selection of sub-regions (patches) of the image is required before applying the recognition algorithm. Generation of these smaller sub-regions is done by use of Region Proposal Network.

VI.CONCLUSION

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. 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 StegoStamp 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.
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.