IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 13, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

Face Counterfeit Detection in National Identity Cards using Image Steganography

Gowrishankar R [1], Ansar M [2], Masood [3]

Assistant Professor, Department of Computer Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamil Nadu India[1]

U.G. Student, Department of Computer Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore Tamil Nadu India[2,3]

ABSTRACT: A national ID card is an identity card with a photo that can be used as identification at least within the country and is issued by an official authority.The most common applications for these smart cards are smart travel documents, electronic IDs, electronic signatures, municipal cards, key cards for access to secure areas or corporate infrastructures, social security cards, etc. To reduce the risks associated with this fraud problem, governments and ID card manufacturers need to continuously develop and improve security measures.With this in mind, we introduce the first efficient steganography method - the StegoCard AutoEncoder, which can hide a secret message in a facial portrait to create 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 was previously printed and then captured by a digital camera.Face images encoded using our StegoCard approach outperform those generated by StegaStamp in terms of their perceptual quality.Peak signal-to-noise ratio, hiding capacity, and imperceptibility results on the test set are used to measure performance.

KEYWORDS: Smart city, digital ID, Internet of Things (IoT), deepfake, presentation attack, facialauthentication system, convolutional neural network, triplet loss, lookup table.

` I. INTRODUCTION

An identity document (also called a piece of identification or ID, or colloquiallyas 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 identitycard (IC, ID card, citizen card),[a] or passport card.[b] Some countries issue formal identity documents, as national identification cards which may be compulsoryor non compulsory ,while others may require identity verification using regional identificationor informal documents.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

II. RELATED WORK

In the past few years, research on computer vision and patternrecognition has been boosted by significant advancements indeep learning techniques, new ways of thinking about paral-lel computing, and monumental developments in hardware.Because facial authentication is at the heart of our digitalID system, this section discusses some of the most recentwork on the three main features of the proposed system: theFR system, face features-based authentication, and morphingattack detection (MAD).

III. METHODOLOGY

1.StegoFace Document Distributor Dashboard

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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

2. Preprocessing Module

Image preprocessing reduces the processing time and enhances the chances of the perfect matching.High resolution images often contain redundant data and by extracting the most meaningful features,the burden on the embedding network is reduced

3. Deep Convolutional ID Face Steganography

The first part of the generator is the encoder network. The aim of the encoder training process is tooptimize the trade-off between its ability to restore the perceptual properties of the input images and the decoder performance to extract the hidden message.

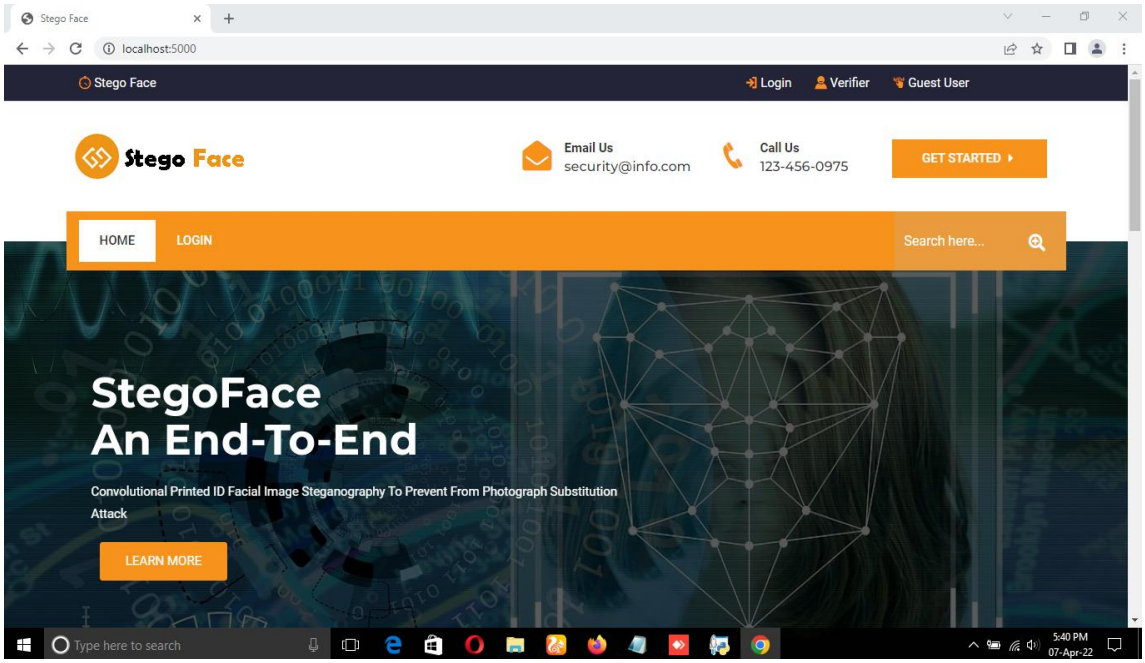
4. Loss Function

The most important loss functions in our model are LPIPS (Learned Perceptual Image PatchSimilarity) and face embedding.Unlike conventional image reconstruction, image steganography process requires two input images and two output images.

5.Performance Evaluation

Steganographic techniques are commonly assessed using three criteria: imperceptibility, capacity, and security. A further important numerical metric is the peak signal-to-noise ratio.

IV. EXPERIMENTAL RESULTS

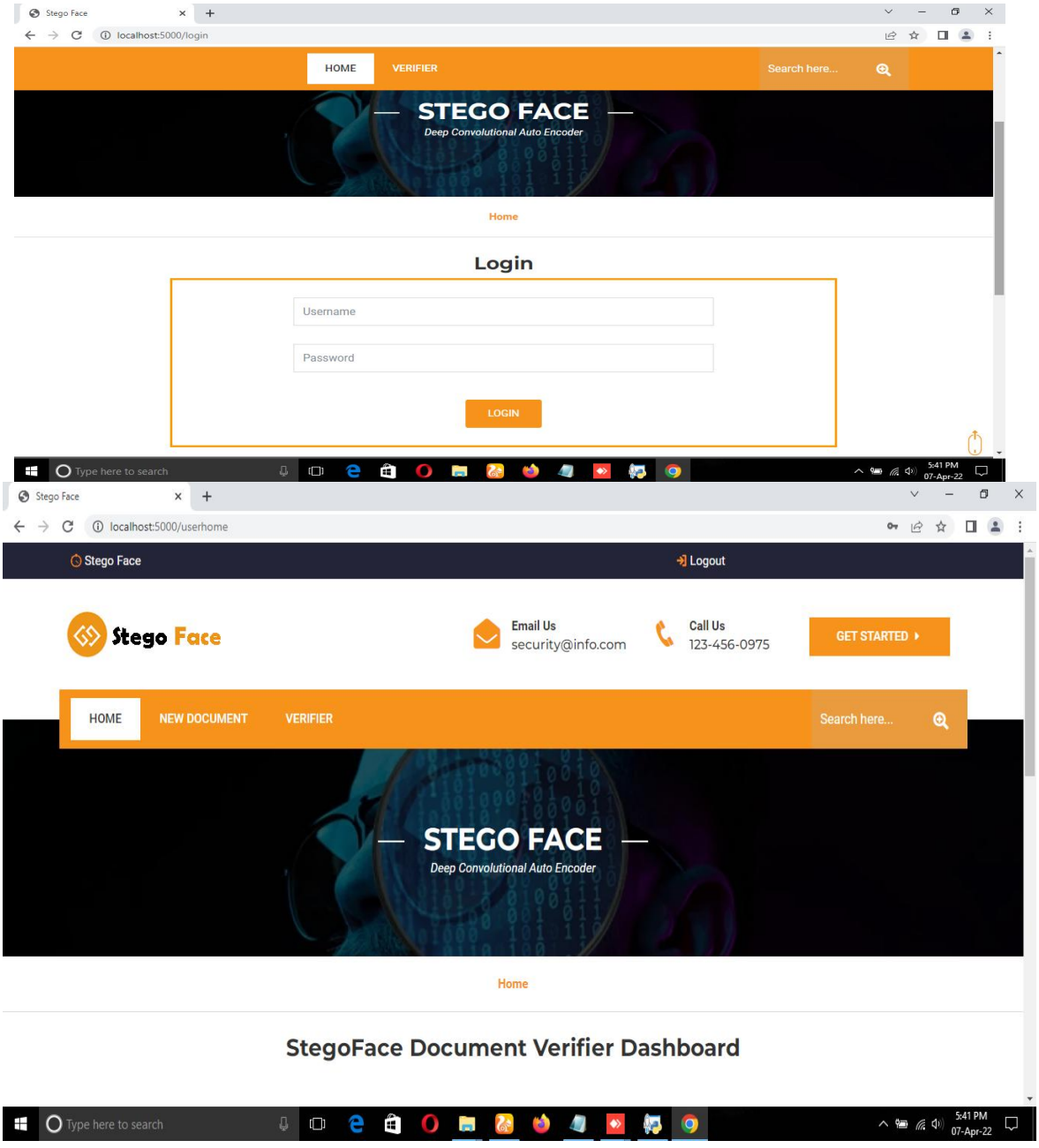


|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

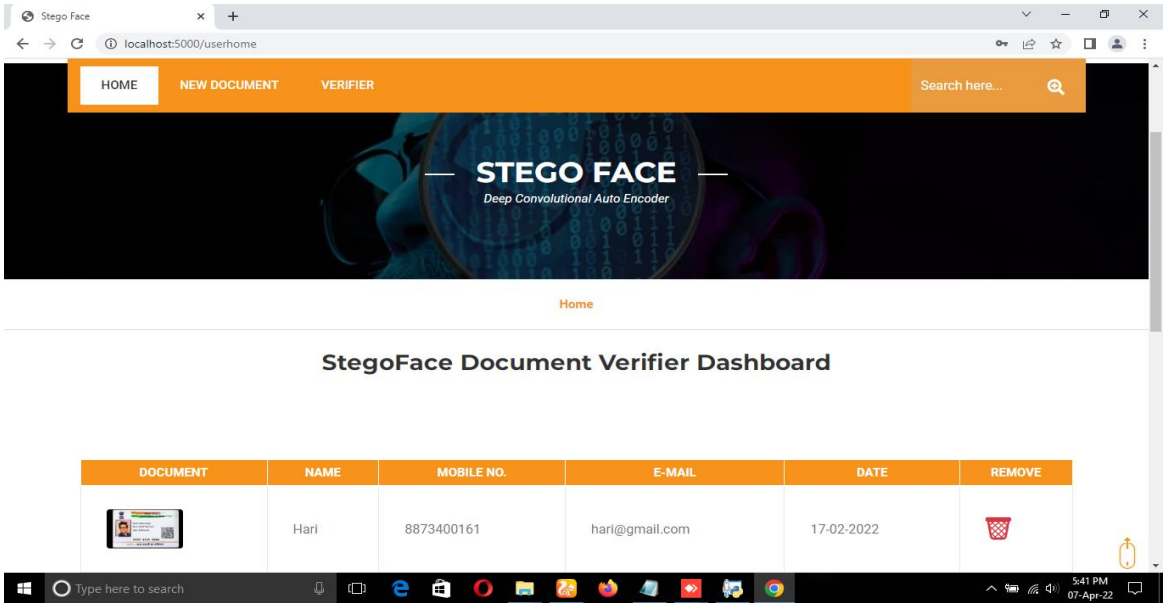


|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India



V. CONCLUSION

The focus of this paper is on concealing security encodeddata in ID and MRTD documents while allowing for theintegrity verification of the portrait. Withthis in mind, we introduce the first efficient steganographymethod - StegoFace - which is optimized for facial imagesprinted in common IDs and MRTDs. StegoFace is an end-to-end Deep Learning Network that is formedby a Deep Convolutional Auto Encoder, that can conceal a secret messagein a face portrait and, hence, producing the encoded image,and a Deep Convolutional Auto Decoder, which is able to read a messagefrom the encoded image, even if it is previously printed andthen captured by a digital camera.StegoFacesurpasses state-of-the-art methods in allowing the use ofimages in their context, irrespectively of the background.This feature also allows us to use the method without anyrestrictions relating to photo parameters.The novel idea proposed in this research is to attach aresize network to our model as an additional noise simulationmodule. This is designed to help the decoder read messagesfrom smaller photos in comparison with previous approaches.The resize network decreases the size of the encoded imagesthat the decoder receives.Facial images encoded with our StegoFace approach outperform the StegaStamp generated images in terms of theirperception quality.From the results shown, it can be clearly seen that theproposed architecture has higher security, robustness, imperceptibilityand 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.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

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.

INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details