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 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11659

PROTECTION OF PHOTO IDENTIFICATION BY USING STEGANOGRAPHY (STEGOFACE)

Vimala P[1], Ajith B[2], Barath M[3], Nirmal Raj T[4]

Assistant Professor, Department of Computer Science and Engineering,Dhirajlal Gandhi College of Technology, Salem, Tamil Nadu, India[1]

Student, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology,Salem, Tamil Nadu, India[2,3,4]

Abstract: Identification and machine-readable travel documents, or IDs and MRTDs, are used to identify and authenticate identities in a variety of contexts, including the crossing of borders, civil applications, sales and purchase portals, and access to transaction processing systems. Criminal attacks on ID verification systems now concentrate on falsified copies of real papers and the alteration of facial images because these security mechanisms are tough to go around. Governments and producers of IDs and MRTDs must constantly develop and enhance security measures if they want to lessen hazards associated with this fraud problem. In light of this, we provide the first effective steganography technique, StegoFace, which is tailored for the printing of facial photos in standard IDs and MRTDs. A Deep Convolutional Auto encoder can hide a secret message in a face portrait, creating the stego facial image. A Deep Convolutional Auto encoder can also read a message from the stego facial image, even if it has been printed and then taken with a digital camera. Together, these two components make up the end-to-end facial image steganography model known as StegoFace. In terms of perceptual quality, facial images encoded using our StegoFace method perform better than images created using the stega stamp. Results from the test set's peak signal-to-noise ratio, concealing capacity, and imperceptibility are used to gauge performance.

Keywords: StegoFace, Fake user, Deep convolutional Auto encoder, StegaStamp

I.INTRODUCTION

Any document that can be used to prove a person's identity is referred to as an identity document (sometimes termed a piece of identification, ID, or simply "papers"). It is typically referred to as an identity card (IC, ID card, citizen card), or passport card, if it is issued in a small, typical credit card-sized form. While some nations issue formal identity documents such as national identification cards that may be required or optional, others may demand the use of informal or regional documents for identity verification. A document may be referred to as photo ID if it contains a person's photograph. A driver's licence may be recognised in many countries as identification proof in the lack of an official identity certificate. Driver's licences are not always accepted as valid forms of identity in other nations, frequently because they have long expiration dates and are susceptible to forgery. Passports are recognised as a means of identification in most nations. Some nations mandate that everyone always carry an identity card on them. If they do not have a resident permission in the country, several nations require all foreigners to always have a passport or sporadically a national identity card from their home country on hand. The identity document serves as a link between a person and information about them, which is frequently stored in a database. The use of the photo and the document's possession to link the individual with it. Based on the personal information on the identity document, such as the bearer's full name, age, birthdate, residence, an identity card, card number, gender, citizenship, and more, a connection can be made between the database and the identity document. The most secure method is to use a unique national identification number, however some nations do not have such numbers or do not include them on identity documents.

II.EXISTING SYSTEM

Water marks are patterns that are printed onto the ID card during production and can be seen or not. Due to their customizability and limited visibility when handled in a specific manner, water marks make it more difficult to duplicate cards. If people don't know to look for it, micro text—which is put on the card somewhere—can be difficult to recreate.

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 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11659

ID cards with holographic laminate give an additional level of visual security. To make it simple for anyone to determine whether a driver's licence is valid, it has a holographic laminate. Holographic laminate is not only challenging to duplicate because the proper computer is required, but it is also secure because the laminate's design is unique. Monochrome cards can be personalised through laser engraving, which permanently engraves details into the card's body. This offers tamper-proof personalisation that is extremely robust, making forgery and manipulation nearly difficult. Any attempts to change the information that has been engraved will cause obvious card damage. Between the encoder and decoder, Stega Stamp takes into account a variety of image corruptions.

DISADVANTAGE:

- Do not sufficiently preserve the visual structure of the encoded face, creating visible distortion in the look of the face
- Unable to decode small, encoded images' internal elements

III.PROPOSED SYSTEM

StegoFace is the name of the suggested system. In the context of IDs and MRTDs, the StegoFace is a model to encode and decode a hidden message in facial photographs. Our approach, which draws inspiration from steganography models, is the first to be created as a security method for the verification of document portraiture. The encoder and the decoder are the two components that make up StegoFace. A Binary Error-Correcting Codes algorithm is used to convert any secret message into a binary message during encoding. The Binary Error-Correcting Code algorithm then converts the binary message into a string with the secret message during decoding. The encoder network is the generator's first component. The encoder training technique aims to strike a compromise between the decoder's ability to correctly decode and understand the concealed information and the encoder's capacity to restore the perceptual properties of the input images. The facial image and the encrypted messages are fed into the encoder first. At the end of the encoder application, a pre-trained encoder model embeds the message in the cropped face to produce an encoded facial image. The encoded cropped image is then used in place of the original facial image before being printed on an ID card. The decoder can extract a message that is concealed in a facial image. A digital camera was used to gather the facial images from the ID card that were encoded for the decoder. After receiving the encoded component of the facial image from the face detection module, the StegoFace decoder network decodes it and determines the hidden message. We can confirm the veracity of the facial portrait in IDs and MRTDs by validating the final message sent, the one that was retrieved, using a hash function or checksum verification technique.

ADVANTAGE:

• Greater strength, imperceptibility, security, and the ability to conceal information.
• A simple yet lightweight architecture is used to enable end-to-end ID facial picture steganography.
• StegoFace's capacity to discern a message from a smaller image is increased by the resize layer, reducing any scrutiny and suspicion.

IV.SYSTEM REQUIREMENT

A. Hardware Requirements

- Processors: Intel® Core TM i5 CPU 4300M @ 2.60 GHz or 2.59 GHz (1 socket, 2 cores, and 2 threads per core)
- Disk space: 320 GB
- Operating systems Linux, macOS, and Windows® 10

B. Software Requirements

- Server Side : Python 3.7.4(64-bit) or (32-bit)
- Client Side : HTML, CSS, Bootstrap
- IDE : Flask 1.1.1
- Back end : MySQL 5.
- Server : WampServer 2i
- BC DLL : PyChain, Node Package Manager, Virtualenv, Block chain hash

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 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11659

V.SYSTEM IMPLEMENTATINON

A Module Split Up

- Stego face Document Distributor Dashboard
- Preprocessing Module
- Deep convolutional ID face steganography
- Loss function

B Modules Description

Stego face is a cutting-edge concept in web-based security. To protect the ID holder's portrait from any future alterations, a second laser-customized portrait is employed. The main objective of this dashboard is to maintain the integrity check of the portrait while protecting security-encoded data in ID and MRTD papers. For document security, it is essential to keep the system's ability to recognise individuals using facial recognition algorithms. The government employee uploads their ID card to Auto Encoder after inputting their login credentials for the StegoFace web dashboard. The facial image and the encrypted messages are fed into the encoder first. The relevant area of the image is located and eliminated using a face detection model.

The likelihood of a perfect match is increased and processing time is decreased by image preparation. To meet encoding standards, face photos are pre-processed. The pre-processing programme extracts features from the cover and hidden photos rather than processing them in their raw form. The strain on the embedding network is lessened by removing the most important features from high resolution photos, which frequently contain redundant data. The format for the input size should be m x m x n, which stands for the three dimensions of width, height, and depth. Since the width and height should be the same size, they are denoted by the unit m. The preprocessing module resizes the input secret image to 256 × 256 since the cover image and the secret image should be the same size. The input secret image can be of any size. The cover image and the secret image are resized to a set size of 256 by 256 using the resize function from the SK image library. The preprocessing module transforms the input photos into helpful attributes that the embedding network may use rather than expressing them as colour gradients.

The encoder network is the first component of the generator. The encoder training technique seeks to reach a compromise between the encoder's capacity to restore the perceptual qualities of the input images and the encoder's ability to correctly decode and comprehend the concealed information. We chose an Unets-based encoder network architecture and erased the pooling layers to safeguard the secret message data that would otherwise be lost during network training. By reshaping and up sampling, the Secret binary message is altered to fit the anticipated size of the encoder input. The encoder modifies the supplied facial image. Because the encoder lacks pooling layers, we must manually match the convolutions' parameters as we design the encoder's architecture in order to prevent issues with layer connections. The preprocessing module and embedding network are built using an auto-encoder architecture.

Every single output of the StegoFace generator is sent to the decoder. The decoder is constructed with a number of loss functions to improve the model's performance. The two main loss functions in our model are face embedding and PIPS (Learned Perceptual Image Patch Similarity). Unlike typical image reconstruction, the picture steganography process needs two input images and two output images. Because of this, a regular loss function might not be suitable for this application. A novel loss function is introduced to enhance the performance of the architecture. The two losses that must be computed are the embedding loss and the extraction loss. The embedding loss is calculated between the input cover image and the StegoFace that the embedding network generates as its output. While the input secret image and the extracted secret image are compared, the extraction network determines the extraction loss. The overall loss is produced by combining the embedding loss with the extraction loss.

VI.CONCLUSION

The main objective of this study is to enable portrait integrity checks while protecting security-encoded data in ID and MRTD documents. In response, we provide StegoFace, the first successful steganography method designed specifically for the printing of facial photographs in conventional IDs and MRTDs. The end-to-end Deep Learning Network known as StegoFace is made up of a Deep Convolutional Auto Encoder, which can conceal a secret message in a face portrait and produces the encoded image, and a Deep Convolutional Auto Decoder, which can read a message from the encoded image even if it has been printed and then taken with a digital camera. StegoFace, which outperforms cutting-edge techniques in allowing the use of photographs in their context regardless of the background, is intended to help the decoder

DOI: 10.17148/IJARCCE.2022.11659

read messages from smaller photos in comparison to older methods. The results, which were clearly given, show that the proposed architecture has superior security, robustness, imperceptibility, and information-hiding capabilities.

REFERENCES

[1] 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. Bazarewsky, 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 , 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,‘‘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.

