# Steganography Photograph Substitution Attack using Deep Fractal Network

**S.Kannadhasan[1],G.Nandhini[2],N.Deepika[3],M.Sharmila[4]**

[1]Assistant Professor,Department of Electronics And Communication Engineering, Cheran College Of Engineering, Anna University, Karur , Tamilnadu, India.

[2,3,4]U.G.Student,Department of Electronics And Communication Engineering,Cheran College Of Engineering, Anna University, Karur, Tamilnadu, India.

[1]kannadhasan.ece@gmail.com,[2]nandhinigunasekaran29@gmail.com, [3]deepikan2750@gmail.com[4]ktcpuliyur@gmail.com

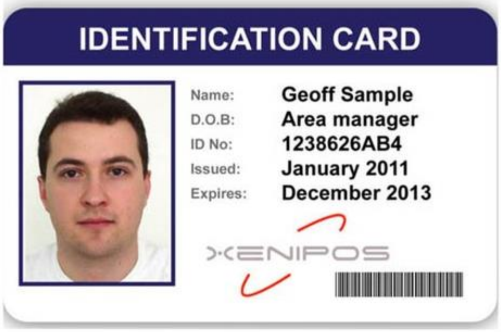
## ABSTRACT

In a variety of settings, IDs and MRTDs (Identification and Machine-Readable Travel Documents) are used to identify and validate individuals. To mitigate the dangers associated with this fraud issue, governments and ID and MRTD manufacturers must continue to develop and strengthen security measures. In light of this, we provide StegoFace, the first efficient steganography solution designed for face pictures printed in conventional IDs and MRTDs. StegoFace is an end-to-end facial image steganography model comprised of a Deep Convolutional Auto Encoder capable of concealing a secret message in a face portrait and, as a result, producing the stego facial image, and a Deep Convolutional Auto Decoder capable of reading a message from the stego facial image, even if it has been previously printed and then captured by a digital camera. In terms of perceptual quality, facial pictures encoded with our StegoeFace technique surpass StegaStamp produced images. On the test set, the peak signal-to-noise ratio, hiding capacity, and imperceptibility values are utilised to assess performance.

**Keywords** - Id proof, RNN face detection, BECC Translator, DC auto encoder/ decoder, Validation.

## 1. INTRODUCTION

Any document that may be used to confirm a person's identity is known as an identity document (also known as a piece of identification or ID, or informally as papers). It's commonly referred to as an identification card (IC, ID card, citizen card),[a] or passport card if it's issued in a compact, normal credit card size format. [b] Some nations offer formal identity papers, such as national identification cards, which may be required or optional, while others may rely on regional identification or informal documents to verify identity.



IDENTIFICATION CARD

| | |
|---|---|
| Name: | Geoff Sample |
| D.O.B: | Area manager |
| ID No: | 1238626AB4 |
| Issued: | January 2011 |
| Expires: | December 2013 |

Figure 1.1. Identity Card

In many countries, a driver's licence may be used to verify identification in the lack of a formal identity certificate. Some nations refuse to recognise driver's licences as identification, owing to the fact that they do not expire as papers in such countries and may be outdated or readily falsified. A person's identification document is used to link them to information about them, which is generally stored in a database. The most secure method is to use a unique national identification number, however some nations lack such numbers or do not include them on identity papers [1]-[5].

## 2. OVERVIEW

Different types of identifications have been introduced, ranging from national identity (ID) cards to drivers' licences to worker ID cards, but due to the ease with which they can be manipulated and faked, they have not helped to address the issue of insecurity, fraud, and other vices for which they were introduced. To do so, the card would need to be linked to a real-time central repository that confirms the individual's authorization to possess the identification card itself, therefore confirming the card-holder relationship.

ID Card Security Issues

However, identification national cards need more attention and purpose since they aid in the battle against insecurity and other vices among the country's residents and immigrants. The following are some of the problems with the National Identity Card:

Error due to human error: It is a significant task to ensuring that all personal information is input accurately. Human mistake may accidentally limit an individual's freedom, create grief, and compromise data security. It may also create delays in the issuance of ID cards, resulting in a waste of government funds.

Forged identification and counterfeit cards are simpler to clone than the "smart" National identity card, which is still in use in a handful of counties.

Falsification of content: an attacker takes advantage of a flaw in the electronic ID card system to alter the data of people. The repercussions vary depending on the motivations of the attacker; for example, it might be employed to exact vengeance on a specific individual.

Theft or loss of identification cards puts a lot of strain on both the government and the holder, particularly in the case of standard ID cards, which include more information than "smart" ID cards [6]-[10].

## 3. STEGO ANALYSIS

Steganography is a method of hiding secret information inside (or even on top of) a non-secret document or other medium in order to prevent discovery. The word "steganos" means "hidden" or "covered" in Greek, while the term "graph" means "to write" in Greek. When you put these words together, you get something that sounds like "secretwriting" or "hidden writing."

Figure .1. Steganography

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 is shown in figure.1.

## 4. SYSTEM INFRASTRUCTURE

The face picture and the secret message are received as inputs into the encoder initially. Using a face identification model, the relevant portion of the picture is identified and cropped. A binary error correcting coding scheme is also used to encode the secret message. The secret message information contained inside the face picture is resistant to imagecarrier physical distortions and other forms of noise and mistake is shown in figure.2.

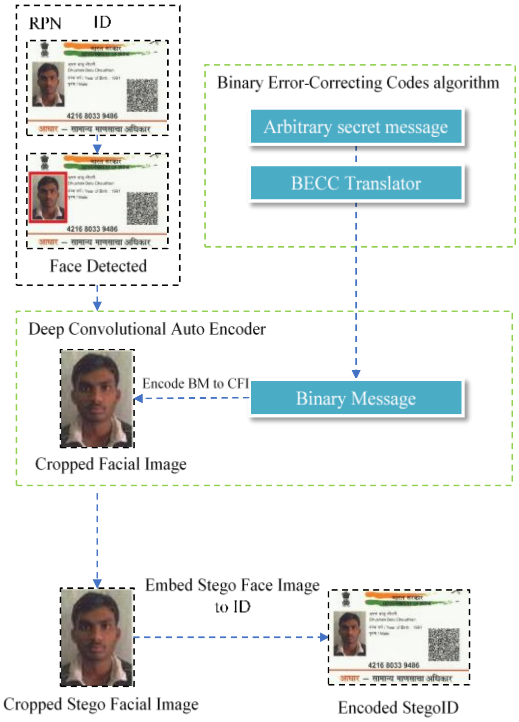

RPN
ID
Face Detected
Binary Error-Correcting Codes algorithm
Arbitrary secret message
BECC Translator
Deep Convolutional Auto Encoder
Encode BM to CFI
Binary Message
Cropped Facial Image
Embed Stego Face Image to ID
Cropped Stego Facial Image
Encoded StegoID

Figure.2.: System Design – Deep Convolutional Auto Encoder

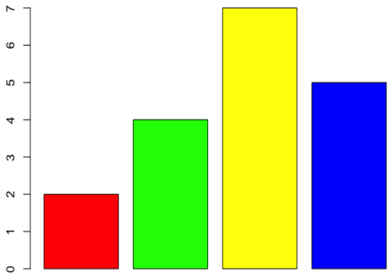


Figure.3.Cropped Facial image

Authorized Verifiers connect into the StegoFace online dashboard and then upload the ID card to Auto Decoder in this module. A document picture is shot using a mobile camera, then the encoded section of the image (the portrait) is recognised and clipped in the decoding process. Finally, the recovered message is examined, and the portrait's integrity is confirmed is shown in Figure.3.

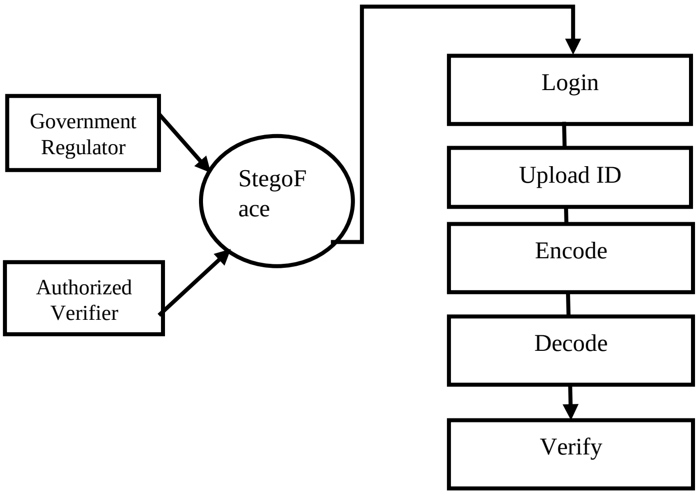


Figure .4.Verifier Control panel

Image preparation speeds up the matching process and increases the odds of a perfect match. Face photos are preprocessed to fulfil the encoding criteria. Because the cover picture and the secret image should be the same size, the preprocessing module resizes the hidden image to 256 x 256 is shown in fig.4 & 5. One input layer and three convolutional layers with increasing numbers of filters make up the preprocessing module is shown in

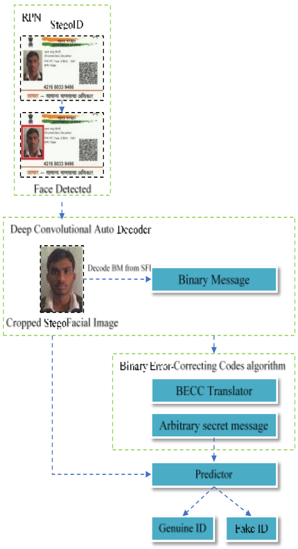

RPN
StegoID
4216 8033 9486
आधार – सामान्य माणसाचा अधिकार
4216 8033 9486
आधार – सामान्य माणसाचा अधिकार
Face Detected
Deep Convolutional Auto Decoder
Decode BM from SFI
Binary Message
Cropped StegoFacial Image
Binary Error-Correcting Codes algorithm
BECC Translator
Arbitrary secret message
Predictor
Genuine ID
Fake ID

fig.5.

Figure.5.:System Design – Deep Convolutional Auto Encoder

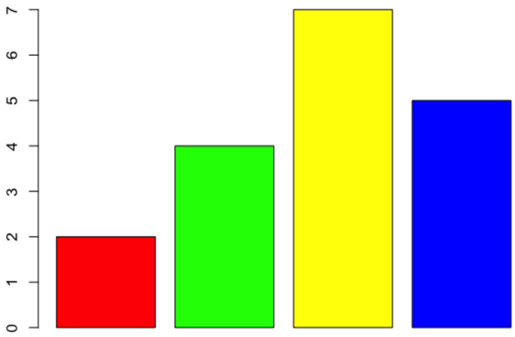


Figure.6.Embed Stego face image to id PSNR value is 100DB

**Face Detection**

For a robust ID verification process that conceals a messagein the facial image is shown in fig.6..

**Detect faces**

Region proposal network (RPN) The region proposal network (RPN) starts with the input image being fed into the backbone convolutional neural network is shown in fig.7.

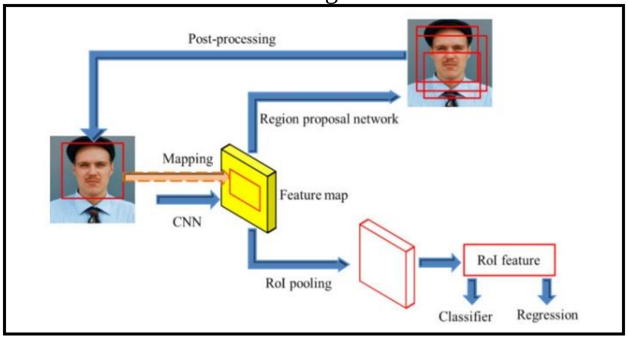


Figure.7.: RPN

Face segmentation is required for face detection from faces with a backdrop. Before performing the recognition method, it is necessary to choose sub-regions (patches) of the picture.

Make boxes around people's faces.

Anchors with 4, 8, 16, 32 scales and 0.5, 1, 2 aspect ratios are employed. Each grid in the picture now has a total of 12 anchors. W = w/16, H = h/16, and 16 is the sub sampling ratio, resulting in a total of W x H x 12 anchors.

• Proposal Layer for Regions

The RPN loss is designed to encourage the network to identify anchors as either background or foreground, and to alter the foreground anchor to better match the face area.

Classification Loss + Bounding Box Regression Loss = RPN Loss

Cross entropy loss is used to topenalize the erroneously classified boxes in the classification loss. The difference between the real regression coefficients and the regression coefficients predicted by the RPN is used to calculate regression loss.

Cropper

Cropping refers to the area of a picture where the face may be found and can be utilised for encoding.

Cropping the face body is done by beginning the crop at (0, 90) and finishing it at (290, 450) in the original picture.

BECC Translator 1.2

A binary error correcting code (BECC) is an encoding system that sends messages as binary integers and allows them to be retrieved even if some bits are flipped incorrectly. They're employed in almost every kind of communication delivery.

Codes in blocks

The message is contained in block codes, which are fixed-size blocks of bits. The superfluous bits are added for mistake correction and detection.

Codes with convolutions

The message is made up of data streams of varying lengths, with parity symbols formed by sliding the Boolean function across the data stream.

Error correction is accomplished via the hamming code approach.

Code Hamming

A block code is an example of hamming code. This algorithm detects the two simultaneous bit mistakes and corrects single-bit faults.

Face Steganography Using Deep Convolutional ID

Auto Encoder (version 2.1)

The encoder network is the generator's initial component. The goal of the encoder training process is to find the best balance between the encoder's capacity to restore perceptual qualities of input pictures and the decoder's ability to recover the concealed information. The preprocessing module's concatenated features are sent into the embedding network. A convolutional layer with 3 filters isplaced at the end of the embedding network to convert the256 X 256 X 8 feature vector into 256 X 256 X 3 stegoimage output.

Auto Decoder (version 2.2)

After adding noise to the pictures, the decoder network is included into the whole design. The decoder's purpose is to retrieve a message encoded in a face picture.

Before the DCAD, the RPN block is put. Five convolutional layers with a rising number of filters make up the expanding encoder section of the extraction network (8, 16, 32, 64, 128). There are five convolutional layers in the decoder, each with a decreasing number of filters (128,64, 32, 16, 8). AnReLU activation is included into each layer is shown in figure 8. There are five convolutional layers in the decoder, each with a decreasing number of filters (128,64, 32, 16, 8).

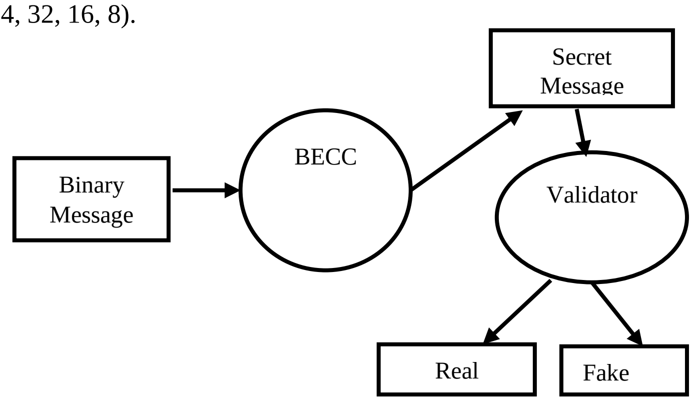


Figure.8.: BECC

In the context of IDs and MRTDs, the StegoFace is a paradigm for encoding and decoding a secretmessage in face photographs. The encoder receives the face picture and the secret message as inputs initially. A binary errorcorrecting codes algorithm is used to code the secret message at the same time. The encoded cropped picture is then printed on an ID card in lieu of the original face image.

In terms of the decoder, a digital camera captures the encoded face picture on the ID card.

## 5. EXPERIMENTAL RESULT

Three criteria are widely used to evaluate steganographic techniques: imperceptibility, capacity, and security. The peak signal-to-noise ratio is another essential numerical statistic. It's vital to dispel any concerns regarding the Payload's existence in cover operations. Any conjecture about the cover's veracity detracts from stenography's goal and facilitates cryptanalysis. The size ratio between the cover medium and the hidden message is referred to as payload capacity. Steganography strives to conceal Payload; hence, the more the Payload capacity achieved by an algorithm, the better this goal is serviced. However, there is a balance between the Payload of the ability and its invisibility/imperceptibility. Statistical assaults use a series of statistical tests on visual data to identify a Payload's embedding. When a secret message is hidden, certain steganographic methods create signs or artefacts. A statistical assault must not be guided by an artefact left by an algorithm.

Channel noise may cause modifications during the transmission of a stego message through a communication channel. The Payload is also corrupted as a result of cropping, rotating, or resizing. The mechanism for embedding the Payload determines the vulnerability to corruption. The vulnerability of an embedding algorithm should be as low as feasible.

PSNR (peak signal to noise ratio) = 1.5

PSNR denotes a change in the performance image metric collected during the Payload embedding method. A high PSNR value suggests a high-quality picture, indicating that the original photo and the stegoface are quite similar to one another. PSNR may be calculated using log:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

where (255) is the maximum 8 bits value representation of a pixel; while MSE indicates the mean squared error or difference between the cover and the stegoface in pixel’s values, given as

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

where *M* and *N* represent the photo’s dimensions, *x* and *y* denote the photo coordinates, Cx,yCx,y denotes the cover photo, and Sx,ySx,y represents the stegoface.

## 6. CONCLUSION

The goal of this article is to hide security encoded data in ID and MRTD papers while still allowing for picture integrity checking. With this in mind, we provide StegoFace, the first efficient steganography solution for face photos printed in standard IDs and MRTDs. StegoFace is an end-to-end Deep Learning Network comprised of a Deep Convolutional Auto Encoder capable of concealing a secret message in a face portrait and, as a result, producing the encoded image, and a Deep Convolutional Auto Decoder capable of reading a message from the encoded image, even if it has been previously printed and then captured by a digital camera. StegoFace outperforms current approaches by enabling pictures to be used in their context, regardless of the backdrop. This feature also enables us to utilise the approach without any picture parameter limits. In compared to prior techniques, this is aimed to aid the decoder in reading messages from smaller pictures. The resize network reduces the size of encoded pictures sent to the decoder. In terms of perceptual quality, facial pictures encoded with our StegoFace technique surpass StegaStamp produced images.

## 7. 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.Bharathi, T.Abirami,” Energy efficient compressive sensing with predictive model for IoT based medical data transmission”, Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z

5. R.Bharathi, T.Abirami," Energy Efficient Clustering with Disease Diagnosis Model for IoT based Sustainable Healthcare Systems", Sustainable Computing: Informatics and Systems, 23 September 2020, https://doi.org/10.1016/j.suscom.2020.100453
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. Parameswari Subbian, Chitra Chinnasamy and Kannadhasan Suriyan, Textile UWB Antenna Performance for Healthcare Monitoring System, Frequenz, De Gruyter, 15 March 2022, https://doi.org/10.1515/freq-2021-0227
8. S.Kannadhasan, R.Nagarajan and R.Banupriya, Performance Improvement of an ultra wide band antenna using textile material with a PIN diode, Textile Research Journal, DOI: 10.1177/00405175221089690 journals.sagepub.com/home/trj
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, 20.