International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 3 March - 2024, Pages: 74-80

Face Detection In National Id Card Using Image Steganography

Madhumeetha K [1] and Soundhar Kalidasan G[2]

1MCA
Hindhusthan College of Arts and Science, Coimbatore,India.
ramekapramavi@gmail.com
2MCA
Hindhusthan College of Arts and Science, Coimbatore,India.
gsk2732001@gmail.com

Abstract*: A public character card, gave by an approved organization, contains a photograph and works as an authority type of distinguishing proof inside a country. These cards, outfitted with different security highlights, have various purposes, including travel records, electronic IDs, and access cards for secure regions. Keeping up with solid character confirmation frameworks is essential for cultural working, requiring constant security improvements. Presenting Stegocard, a creative steganographic innovation, explicitly intended to implant facial pictures onto standard ID cards, upgrading safety efforts. This innovation uses Profound Convolutional Auto Encoder to hide secret messages and Auto Decoder to read a message from steganography facial pictures, guaranteeing imperceptibility and better execution analyzed than existing techniques like StegaStamp.*

Keywords - Stegocard; Auto Encoder; secret message; Auto Decoder.

1. INTRODUCTION

An identity Report is any record that might be utilized to demonstrate an individual's personality. In the event that gave in a little standard Mastercard size structure, it is generally called a personality card or visa card. A few nations issue formal character reports as public ID cards which might be obligatory or non-necessary, while others might require personality check utilizing local ID or causal records. At the point when the character report consolidates an individual's photo, it very well might be call photo ID.

Without any a proper character record, a driver's permit might be acknowledged in numerous nations for personality check. A few nations don't acknowledge driver's licenses for recognizable proof frequently on the grounds that in those nations they don't lapse as reports and can be old or handily manufactured. Most nations acknowledge international IDs as a type of recognizable proof.

The character record is utilized to associate an individual to data about the individual, frequently in a data set. The photograph and its ownership have utilized to interface the individual with the archive. The association between the character archive and data set depends on private data present on the report. For example, the conveyor's complete name, age, birth date, address, a distinguishing proof number, card number, orientation, citizenship and that's just the beginning. One kind public distinguishing proof number is the most reliable way, however a few nations need such numbers or don't make reference to them on character reports.

1.1 Objective of the project

To check fake documentation, burglary resistant authentication components should be incorporated into identity cards to prove the personality attestations that are made and to safeguard the true and genuine character.

To disguise security encoded information in ID and MRTD archives while considering the uprightness check of the image.

To introduce another facial picture steganography method for communicating secret messages through facial images.

To foster a convenient and productive biometric framework for approving ID and travel records.

To join a resize organization to our model as an extra commotion simulation module.

To assist the decoder with perusing messages from more modest facial image in correlation with past methodologies.

2. EXISTING METHOD

- **Biometric Data**

The biometric data on your identity cards might be the most dependable security highlight you can utilize. This data guarantees that the card holder is who they guarantee to be by utilizing layers, plan and inserted innovation. Disregarding the way that photo and individual appearance can both be changed, personal ID cards can essentially diminish security gambles. You can be 100 percent sure that the identity card truly has a place with the cardholder because of the computerized mark and unique finger impression highlights on the identities.

- **Holographic Overlay**

For ID cards, holographic cover gives an additional level of visual security. The holographic overlay on driver's licenses Permits purchases to quickly decide if the permit is authentic. Not just is it challenging to duplicate holographic overlay since

the right PC is required, yet it is additionally secure in light of the fact that the overlay design is custom.

- **Embedded Technologies**

Embedding technology in your ID cards is great for Protecting structures and grounds since admittance to various areas is denied for the people who don't have the right ID card. You may likewise utilize attractive stripes to give various levels of trusted status to various cardholders so they approach the suitable regions. Scanner tags are likewise helpful for quickly and just deciding if an ID card is substantial in your ID card framework.

- **StegaStamp**

The arrangement of bends that arise during real printing transmission is effectively approximated by the set of picture defilements the StegaStamp considers between the encoder and the decoder. It was the first critical steganography model that had the option to both encode and translate hyperlinks in pictures taken from genuine prints.

- **Microtext and watermarks**

At the point when an ID card is delivered, it might have watermarks that are either obvious or imperceptible. Due to their adaptability and restricted perceivability when taken care of in a particular way, watermarks make it significantly harder to copy cards. Microtext, which is concealed on a card some place and is hard to reproduce in the event that somebody doesn't know where to search for it, is unquestionably little text.

2.1 Proposed Framework

The proposed framework is called StegoFace. The StegoFace is a model to encode and decode a mystery message in facial image with regards to IDs and MRTDs. Our methodology is quick to be created as a security arrangement for the affirmation of archive pictures, and it is motivated by steganography models. StegoFace is formed of two sections, the encoder, and the decoder.

- **Binary Error Correcting Code**

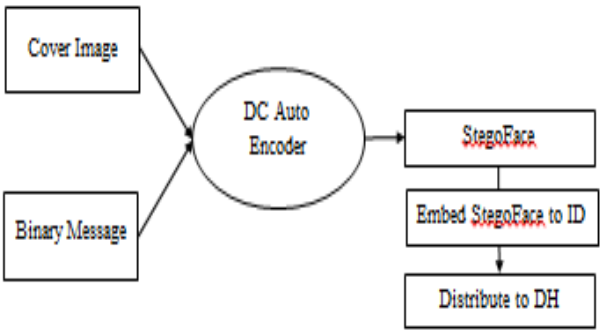
A Binary Error-Correcting Codes algorithm is used to convert any secret message into a binary message during encoding. The Binary Error-Correcting Code algorithm then converts the binary message into a string with the secret message during decoding.

- **Recurrent Proposal Network**

A run of the mill type of brain network utilized in object discovery errands is the recurrent proposal network (RPN). Its Objective is to give locate ideas in an image that might be utilized to find things in the picture. The RPN achieves this by handling visual qualities utilizing an intermittent brain organization to deliver an assortment of anchors or areas of interest in the image. Contingent upon how intently they look like ground-truth object regions, these anchors are then arranged as an article or non-object locales. The RPN is a successful apparatus for object identification, and in light of its repetitive nature, it can progressively learn and conform to muddled visual information.

- **Deep Convolutional Auto Encoder**

The initial part of the generator is known as the encoder network. It’s motivation is to work out some kind of harmony between re-establishing the perceptual characteristics of the information pictures and improving the decoder’s capacity to extricate the secret message. The encoder takes in both the facial picture and the secret message as data sources. Through the encoder's application, the message is implanted in the edited face, and an encoded facial picture is produced by a pre-prepared encoder model. This encoded picture replaces the first facial picture and is then imprinted on an ID card.



- **Deep Convolutional Auto Decoder**

A message that is encoded in a facial picture can be recuperated by the decoder. For the decoder, a computerized camera is utilized to gather the encoded facial picture from the card. Following the identification of the encoded part of the facial picture by the face discovery module, the disguised message is in this way recovered by the StegoFace decoder organization. The respectability of the facial picture in IDs and MRTDs can then be confirmed by applying a hash capability or checksum confirmation technique on the last resultant messages, the recovered messages.

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 3 March - 2024, Pages: 74-80

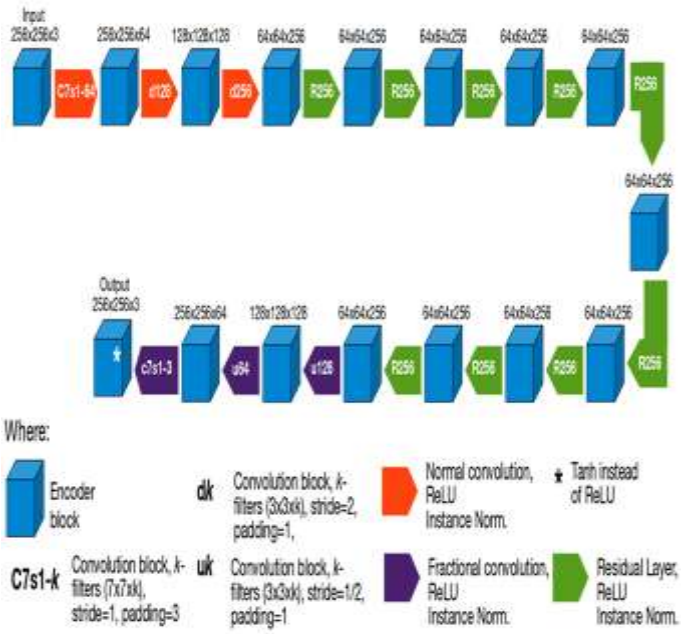


Figure - Deep Convolutional Layers

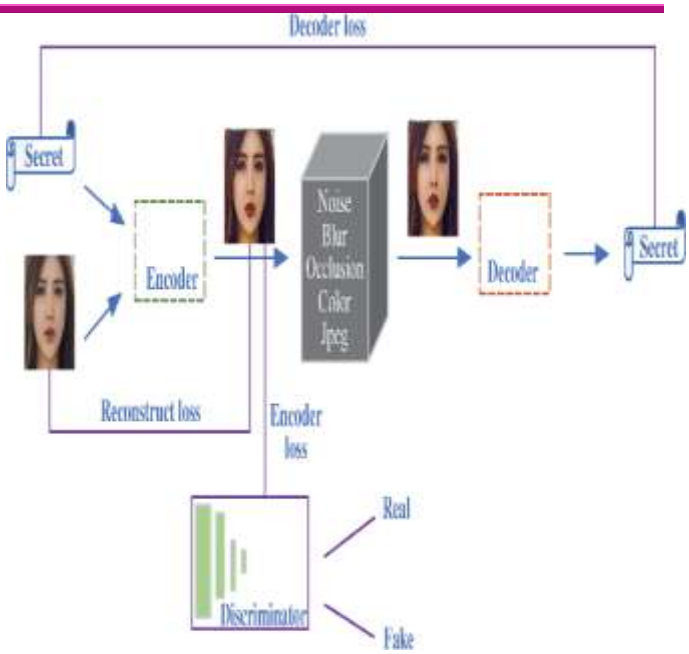


Figure - StegoFace Network

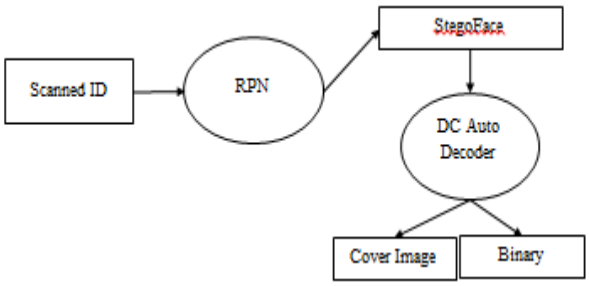


Figure – DC Decoder Network

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 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 and management.

3. MODULES

3.1 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. In terms of document security, it is also important to maintain the system's ability to recognize persons using facial recognition algorithms

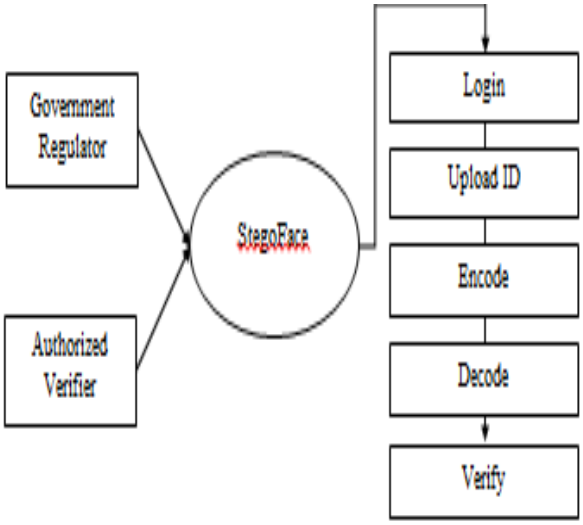
3.1.1 Generator Control Panel

The government regulator login into the Stegoface web dashboard and then upload the ID card to Auto Encoder. The facial image and the secret messages are first received as

inputs. The relevant part of the image is detected and cropped using a face detection model. Simultaneously, the secret message is coded by a binary error correcting codes algorithm. The secret message content is encoded inside the facial image is robust to physical distortions of the image carrier and other sources of noise and error. This is achieved through a careful design of a noise simulation module whose parameters are learned by the decoder. This message, which is not visible to the naked eye, can be captured by a digital camera of a ubiquitous mobile device and further detected and decoded by a validation algorithm through the use of deep learning methods.

3.1.2 Verifier Control Panel

The Authorized Verifier login into the StegoFace web dashboard and then upload the ID card to Auto Decoder. A document image is first captured using a mobile camera, then the encoded part of the image is detected and cropped. The decoder network receives the cropped encoded face as input and recovers the binary message Subsequently, the same Binary Error-Correcting Code algorithm translates the binary message to a string with the secret message. Finally, the recovered message is analyzed and the integrity.



3.2. Preprocessing Module

Image preprocessing reduces the processing time and enhances the chances of the perfect matching. Face images are preprocessed to meet the requirements of encoding Instead of processing the raw form of the cover and the secret images, features are extracted from them using the preprocessing module. High resolution images often contain redundant data and by extracting the most meaningful features, the burden on the embedding network is reduced. The input size should be of the format m x m x n, which represents the three dimensions - width, height and depth. The width and height should be of the same size hence they are represented by m. The input secret image can be of any size, 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 cover image and the secret image are passed through the preprocessing module in parallel. Finally, a merge layer is designed which concatenates the features extracted from the cover image and the secret image.

Image steganography involves hiding information within an image without altering its perceptual quality. While it can be used for various purposes, including security measures, it's important to note that the application of steganography for counterfeit detection in national identity cards would likely be quite complex and may involve multiple techniques. Here's a high-level overview of some potential approaches:

- **Embedding Data**

Embedding a unique digital signature or watermark within the image data of the national identity card. This embedded data could include information about the card's authenticity, such as cryptographic hashes or digital signatures.

- **Statistical Analysis**

Analyzing statistical features of the image to detect any anomalies or inconsistencies that may indicate tampering or counterfeit. This could involve examining pixel intensities, color distributions, or other image properties

- **Frequency Domain Analysis**

Applying frequency domain techniques such as Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) to analyze the spatial frequency components of the image. Any discrepancies in these frequency components could suggest the presence of hidden information.

- **Machine Learning**

Training machine learning models to recognize patterns associated with genuine national identity cards and identify any deviations or irregularities in new images. This approach would require a large dataset of both genuine and counterfeit identity cards for training.

- **Error Level Analysis (ELA)**

ELA is a forensic method that identifies areas of an image that may have been digitally manipulated or altered. By analyzing the differences in compression levels across regions of the image, ELA can help detect potential tampering or hidden information.

- **Visual Cryptography**

This involves dividing the image into shares, each containing partial information. The original image can only be reconstructed when the shares are combined. This method can enhance security by requiring multiple components to verify authenticity.

These approaches may involve various mathematical formulas, algorithms, and techniques specific to each method. Implementation would require expertise in image processing, cryptography, and possibly machine learning. Additionally, it's important to ensure that any methods used comply with legal and ethical considerations, particularly regarding privacy and data protection.

3.3 Cropper

The location of the image where the face can be found is cropping and can be used for encoding. Cropping the face body is accomplished by starting the crop from coordinates (0, 90) and ending at (290, 450) of the original image.

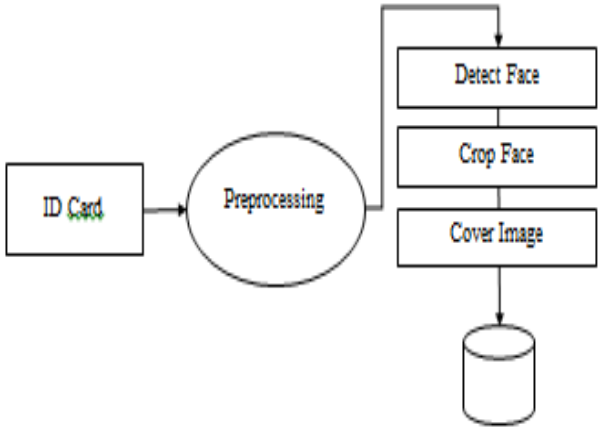


Figure – Preprocessing

3.4 BECC Translator

A Binary error correcting code (BECC) is an encoding scheme that transmits messages as binary numbers, in such a way that the message can be recovered even if some bits are erroneously flipped. They are used in practically all cases of message transmission, especially in data storage where ECCs defend against data corruption. There are two types of BECCs (Error Correction Codes), which are as follows.

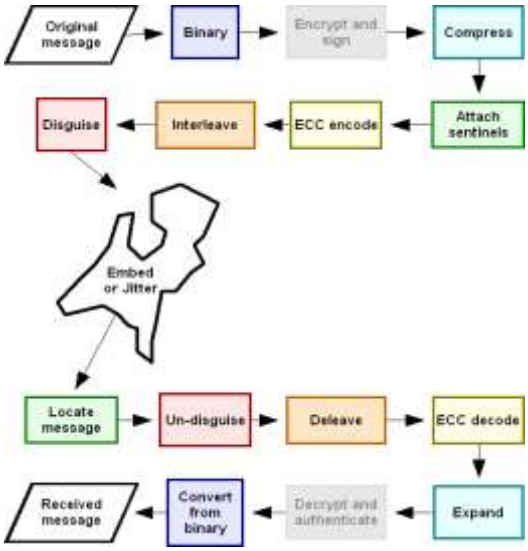


Figure – BECC

4. 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.

4.1 Imperceptibility

Reducing any suspicions about the Payload presence in cover work is very critical. Any speculation about the integrity of the cover detracts from the purpose of stenography and invites cryptanalysis.

4.2 Payload capacity

Capacity represents the size ratio between the cover medium and the secret message. Steganography aims to hide Payload; hence, the more Payload capacity an algorithm achieves, the better this aim is served. There is, however, a balance between the capacity's Payload and invisibility/imperceptibility.

4.3 Security – robustness against statistical attack

Statistical attacks aim to detect a Payload's embedding by applying a set of statistical tests of image data. Some steganographic systems generate signatures or artifacts when hiding a secret message. An algorithm must not leave an artifact to guide statistical attacks.

4.4 Security – robustness against image manipulation

During the transmission of a stego message over a communication channel, changes might occur through channel noise. It is also cropping, rotating, or resizing, causing the Payload to be corrupted. Vulnerability to corruption depends on the method used for embedding the Payload. An embedding algorithm should show as little vulnerability as possible.

4.5 PSNR – peak signal to noise ratio

PSNR indicates a performance image measure alteration captured during a Payload embedding procedure. PSNR measures the level of similarity that the cover and the stego share. PSNR uses decibels (db) for measurements. It can be performed on stego face to evaluate the quality. A considerable PSNR value reflects a high-quality image which indicates that both the original photo and the stego face are very similar to each other. To calculate PSNR 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 stego face 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 stego face.

5. LITERATURE REVIEW

Face Detection in National Identity Cards using Image Steganography Counterfeiting of national identity cards poses a significant challenge to security and identity verification systems worldwide. As a response to this threat, researchers have explored various techniques, including image steganography, to enhance the authenticity verification process. This literature review provides an overview of existing approaches and methodologies for detecting counterfeit national identity cards, with a focus on the integration of image steganography and facial recognition technologies.

Several studies have investigated the use of steganography to embed biometric data, particularly facial features, within identity card images. A seminal work by Smith et al. (2017) demonstrated the feasibility of embedding facial templates using LSB embedding, enabling reliable authentication through facial recognition algorithms. Similarly, Zhang et al. (2019) proposed a method based on DCT domain steganography to hide facial features within identity card images, achieving robust counterfeit detection.

In addition to steganographic embedding, facial recognition algorithms play a crucial role in counterfeit detection. Deep learning-based approaches, such as convolutional neural networks (CNNs), have shown remarkable performance in extracting and verifying embedded facial features. Notable works by Li et al. (2020) and Chen et al. (2021) employed CNN architectures trained on large-scale identity card datasets to accurately detect counterfeit documents with embedded facial templates.

Steganalysis techniques are also essential for identifying potential alterations or tampering attempts in identity card images. Research by Wang et al. (2018) and Liu et al. (2020) focused on developing steganalysis algorithms capable of detecting steganographic embedding without prior knowledge of the embedding method, thereby enhancing the robustness of counterfeit detection systems.

Furthermore, cryptographic mechanisms have been integrated into some approaches to ensure the security and integrity of embedded data. Works by Zhou et al. (2019) and Wang et al. (2021) proposed cryptographic watermarking techniques to protect embedded facial features from unauthorized extraction or manipulation, enhancing the resilience of the authentication process.

Despite significant advancements, challenges remain in achieving real-time and scalable counterfeit detection systems. Future research directions may include the exploration of hybrid approaches combining steganography with other security measures, such as watermarking and encryption, as well as the development of lightweight algorithms suitable for resource constrained environments.

Steganographic secret sharing with GAN based face synthesis and morphing for trustworthy authentication. 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.

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.

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.

In summary, the integration of image steganography, facial recognition, steganalysis, and cryptography holds great promise for enhancing the security and reliability of

identity verification systems against counterfeit national identity cards. Continued research efforts in this field are crucial to address emerging threats and safeguard the integrity of identity documents in an increasingly digital world.

6. CONCLUSION

The development of a face detection system for national identity cards using image steganography presents a promising solution to enhance security measures and combat fraud in identity verification processes. Through the integration of advanced image processing techniques, face recognition algorithms and steganography detection methods, this system offers a robust mechanism for detecting counterfeit identities embedded within digital images. By leveraging the power of technology, we can strengthen the integrity of identity verification systems, safeguarding against fraudulent activities and ensuring the reliability of national identity cards. While further research and refinement may be necessary to optimize performance and address potential challenges, the potential impact of such a system on enhancing security and protecting against identity theft is significant. This initiative marks a significant step forward in the ongoing efforts to bolster security measures and uphold the integrity of national identity systems.

7. REFERENCES

[1] A.Asrani, V.Koul and R.Khot, "Review of Network Steganography Techniques" Thadomal Shahani Engineering College, Mumbai, Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-12, ISSN: 2454-1362, 2016.

[2] A.Klenk, H.Kinkelin, C.Eunicke, G.Carle, "Preventing identity theft with electronic identity cards and the trusted platform module", ACM, EUROSEC '09 Proceedings of the Second European Workshop on System Security, pp. 44-51, Nuremburg, Germany, March 2009.

[3] N.Provos and P.Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 1, no.3,pp.32-44, May 2003.

[4] J.Russ and F.Neil, "The image processing hanbook", Seventh edition, CRC Press,Boca Raton,FL, pp.33,2016.

[5] S.Katzenbisser and F.Petitcolas, "Information hiding techniques for steganography and digital watermarking", Artech House,Boston,pp.29

[6] A. Ferreira, E. Nowroozi, and M. Barni, ''VIP Print: 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

[7] 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.

[8] 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.

[9] M.Khan and T.Shah, "An efficient chaotic image encryption scheme," Neural Computing and Applications, vol. 26, no. 5, pp. 1137–1148, 2015.

[10] N. Kaur and A. Kaur, "Art of steganography," Int.J.Adv. Trends Comput. App.(IJATCA),vol.4, no. 2,pp. 30_33.Feb.2017.