ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

Face Counterfeit Detection in National Identity Cards using Image Steganography

Manoj kumar
CSE
Paavai College of Engineering
Namakkal,TamilNadu
manojkumarbmi@gmail.com

Hariharan P
CSE
Paavai College of Engineering
Namakkal,TamilNadu
hariharanp1912@gmail.com

Harish M
CSE
Paavai College of Engineering
Namakkal,TamilNadu
harishmurugan9952@gmail.com

Ranjith A
CSE
Paavai College of Engineering
Namakkal,TamilNadu
ranjithayyakannu@gmail.com

Abstract: A national identity document is an identity card with a photo, usable as an identity card at least inside the country, and which is issued by an official authority. The most common applications for these smart cards are smart to travel documents, electronic IDs, electronic signatures, municipal cards, key cards used to access secure areas or business infrastructures, social security cards, etc. 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. Trusted identity is a vital component of a well-functioning society. To reduce risks related to this fraud problem, it is necessary those governments and manufacturer of IDs continuously develop and improve security measures. With this in mind, we introduce the first efficient steganography method - StegoCard - which is optimized for facial images printed in common IDs. StegoCard 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 StegoCard approach outperform the Stega Stamp 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

I. Overview

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.

Figure 1.1 Identity Card

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.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

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.

1) History of ID

A version of the passport considered to be the earliest identity document inscribed into law was introduced by King Henry V of England with the Safe Conducts Act 1414.For the next 500 years up to the onset of the First World War, most people did not have or need an identity document. Photographic identification appeared in 1876 but it did not become widely used until the early 20th century when photographs became part of passports and other ID documents such as driver's licenses, all of which came to be referred to as "photo IDs". Both Australia and Great Britain, for example, introduced the requirement for a photographic passport in 1915 after the so-called Lody spy scandal. The shape and size of identity cards were standardized in 1985 by ISO/IEC 7810. Some modern identity documents are smart cards including a difficult-to-forge embedded integrated circuit that were standardized in 1988 by ISO/IEC 7816. New technologies allow identity cards to contain biometric information, such as a photograph; face, hand, or iris measurements; or fingerprints. Many countries now issue electronic identity cards.

2) List of Identity documents of India

- Aadhaar Card, issued by UIDAI.
- Indian passport
- Voter ID Card, issued by the Election Commission of India
- Overseas Citizenship of India document
- Person of Indian Origin Card
- PAN Card, issued by the Income Tax Department
- Driving license in India issued by the respective state governments
- Ration card issued by the Government of India
- Identity Certificate for non-citizens or stateless people
- A Birth certificate issued by the Registry of Births and Deaths (RBD) or from a Municipality within the provisions of the RBD Act
- Transfer/School leaving/Matriculation Certificate
- Service Identity Card issued by State/Central Government, Public Sector Undertakings, local bodies or public Limited Companies
- Copy of an extract of the service record of the applicant (only in respect of Government servants) or the Pay Pension Order (in respect of retired Government Servants), duly attested/certified by the officer/in-charge of the Administration of the concerned Ministry/Department of the holder
- Policy Bond issued by Public Life Insurance Corporations/Companies
- Scheduled Caste/Scheduled Tribe/Other Backward Classes Certificates
- Freedom Fighter Identity Cards
- Arms Licenses
- Property Documents such as Pattas, Registered Deeds etc.
- Railway Identity Cards
- Student Photo Identity Cards issued by Government Recognized Educational Institutions in respect of full-time courses
- Gas Connection Bill
- Bank/ Kisan/ Post Office Passbooks
- Photo Bank ATM Card
- Photo Credit Card
- Pensioner Photo Card
- Certificate of Identify having photo issued by Gazetted Officer or Tehsildar on letterhead
- Unique Disability ID (UDID) Card / Disability medical certificate issued by the respective State / UT
- Marriage Certificate
- Proof of Marriage document issued by the Registrar
- Gazette Notification
- Legal Name Change Certificate
- Land revenue certificate
- Land Certificate Identity documents are used for multiple purposes:
- For domestic and international travel
- To obtain a mobile phone SIM card
- To apply for a passport
- To obtain government benefits
- In certain cases when asked to do so by law-enforcement officers

II. Problems Identified

Different types of identifications have been introduced ranging from national Identity (ID) Card, drivers' licenses, to workers ID Cards, however these have not helped to address the issue of insecurity, fraud and other vises for which purpose they were introduced due to the ease by which they can be manipulated and faked. Counterfeit identity cards have become increasingly commonplace; thus, authentication and verification of identity documentation has become a salient issue with the surge in incidents of identity theft. When individuals identify themselves, they are making a claim of identity based on a

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

variety of different credentials including name, birth date, birth place, address, education and professional information, amongst others. However, these claims alone do not authenticate identity; supportive evidence is required to verify that the identification document and the information contained therein are valid and the identity of the individual is verified. Due to the simple nature of the existing ID card, it became very easy to manipulate and print the ID card carelessly without any extra means of confirmation and authentication. The voter's card and the driving license also took a similar step and have no automatic referencing central system to confirm the authenticity of their holders. However, because of these lapses in authentication, an ID card may bear another person's picture with a different name or place of residence. Photograph substitution Attack in official documents (a genuine photo replaced by a non-genuine photo) or originally fraudulent documents with an arbitrary photograph. To achieve this end, industry invokes various types of security and verification features within identity cards ranging from tamper-proof laminates to holograms and more advanced features such as ultraviolet ink and micro print. Although these features verify the authenticity of the card itself, they do not verify the identity presented on the card. To do so would require the card to link to a real-time central repository that verifies the individual is authorized to possess the identity card itself, thus verifying the link between the card and the card-holder.

1) Security Issues of ID Cards

ID cards have a number of vulnerabilities as with many new technologies which need to be considered. However, identity national cards need more concerned and intention because it helps to fight against insecurity and other vices among the citizens and immigrants in the country. The following are some of the National identity card's issues :

2) Human error

A number of experts say human error is the biggest threat to ID card schemes vulnerability. The potential threat can appear at any moment where the scheme of identification card is interacted. It is a big challenge to ensure that all personal information is entered correctly, furthermore; there has to be a tool in the system that allows the modification of database entries when a user of the identity card changes their address or other information. Installing incorrect cardholder's data at any stage of the enrolment process is likely to create many problems of the bearer of the ID card. According to press story in the Guardian newspaper, a foreign woman could not travel for more than a month because she received incorrect information on her identity card which enforced her to send her ID card and passport to the responsible institution (UK Borders Agency) to solve the problem. Human error may inadvertently restrict the freedom of an individual, cause distress and might breach information security. It can also cause delay in issuing ID cards and waste government money.

3) Forged identity and counterfeit cards:

The traditional ID card, which is still being used in a number of counties, is easier clone than the "smart" National identity card. A threat may come from the lack of security features or conventional materials on the ID cards which do not match
the requirement of accredited security printers. The fake identity card can be misused by teenagers to purchase alcohol, cigarettes or any unauthorized products, or even by terrorist to enter a country illegally.

4) Falsification of content:

An attacker exploits the vulnerability of the electronic ID card's system to change the citizens' data. The consequences are various and depend upon an attacker's motives, for example it could be used to take revenge on a particular person.

5) Man in the middle attacks:

As a result of lack of National ID card system security, an attacker might intercept communication between the identity card and server. The attacker stands between the two victims and then he will be able to access the sensitive data of a card holder.

6) Skimming attacks: The threat comes from creating a clandestine connection to the ID card in order to obtain data. An attacker can use a hidden, small machine like a reading device which is able to skim the information from "smart" identity cards and misuse the information.

7) Centralization of Database storing: In spite of giving hackers an obvious target to concentrate on by storing citizens' data in one place, hackers are intelligent enough to discover the weak aspects of their victim(s) before they attack. Hackers can observe the data for illicit purposes or to corrupt the identity card system.

8) Abuse by Authorized individual: people are already concerned about misuse of their information by criminals. However, a greater, threat is if such misused comes from authorized people such as the police or employers who deal with the citizens' database. They might use this information to stalk, threaten people, take revenge or settle scores.

9) Decrypting Data: There is small possibility of decrypting the biometric card's data when a secret key is known. For instance, hackers can interfere with the data stored on chip sand also monitor data flows using probing pins. This enables them to steal private keys and to access private data.

10) Theft or loss of the ID Cards: If the identity card has been stolen or lost it put a lot of pressure on both the government and bearer especially in the case of traditional ID cards which have more information on them than "smart" ID Cards. For example, the traditional Saudis identity cards used to contain sensitive information such as the card holders' full name, an identification number, address and the telephone number, but such information is now hidden in

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

the new biometric ID cards. [3] proposed a system, this system has concentrated on finding a fast and interactive segmentation method for liver and tumor segmentation. In the pre-processing stage, Mean shift filter is applied to CT image process and statistical thresholding method is applied for reducing processing area with improving detections rate. In the Second stage, the liver region has been segmented using the algorithm of the proposed method. Next, the tumor region has been segmented using Geodesic Graph cut method. Results show that the proposed method is less prone to shortcutting than typical graph cut methods while being less sensitive to seed placement and better at edge localization than geodesic methods. This leads to increased segmentation accuracy and reduced effort on the part of the user. Finally Segmented Liver and Tumor Regions were shown from the abdominal Computed Tomographic image.

III. Steganography

Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. Steganography has been used for centuries, but these days, hackers and IT pros have digitized the word “steganography” seems fancy, but it actually comes from a fairly normal place. The root “steganos” is Greek for “hidden” or “covered,” and the root “graph” is Greek for “to write.” Put these words together, and you’ve got something close to “hidden writing,” or “screw writing.”

Figure 1.1 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. It’s not a form of cryptography, because it doesn’t involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways. Where cryptography is a science that largely enables privacy, steganography is a pract ice that enables secrecy – and deceit.

1) Types of Steganography

Steganography breaks down into five types:

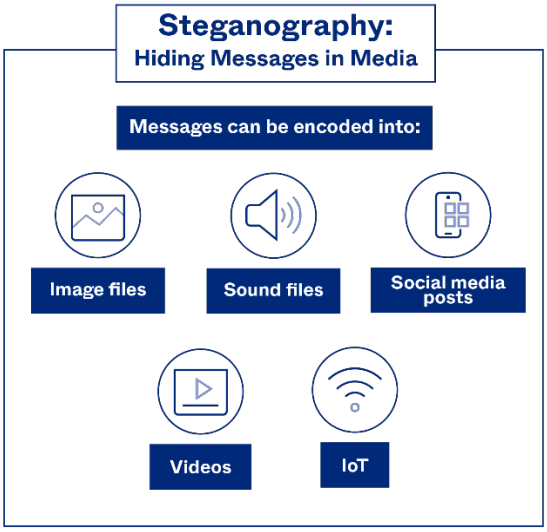


Figure 1.2 Types of steganography

- Text Steganography

This type of steganography involves using white spaces, capital letters, tabs, and other characters.

- Audio Steganography

Audio steganography is used with digital audio formats like WAVE, MIDI, and AVI MPEG, using echo hiding, parity coding, and LSB coding, to name a few.

- Video Steganography

Video steganography deals with video formats like H.264, Mp4, MPEG, and AVI. In addition, it employs pictures to carry concealed data.

- Image Steganography

Pixel intensities are employed to hide information.

- Network Steganography

Network protocols use TCP, UDP, and IP as carriers.

2) Deep Learning

Deep Learning is a subset of Machine Learning, which on the other hand is a subset of Artificial Intelligence. Artificial Intelligence is a general term that refers to techniques that enable computers to mimic human behavior. Machine Learning represents a set of algorithms trained on data that make all of this possible. Deep Learning, on the other hand, is just a type of Machine Learning, inspired by the structure of a human brain. Deep learning algorithms attempt to draw similar conclusions as humans would by continually analyzing data with a given logical structure. To achieve this, deep learning uses a multi-layered structure of algorithms called neural networks

Artificial intelligence is the ability of a machine to imitate intelligent human behavior. Machine learning allows a system to learn and improve from experience automatically. Deep learning is an application of machine learning that uses complex algorithms and deep neural nets to train a model.

3) Importance of Deep Learning

- Machine learning works only with sets of structured and semi-structured data, while deep

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

learning works with both structured and unstructured data

- Deep learning algorithms can perform complex operations efficiently, while machine learning algorithms cannot
- Machine learning algorithms use labeled sample data to extract patterns, while deep learning accepts large volumes of data as input and analyzes the input data to extract features out of an object
- The performance of machine learning algorithms decreases as the number of data increases; so, to maintain the performance of the model, we need a deep learning.

4) Types of Learning in Deep Learning Within deep learning, there are various learning techniques and algorithms used by data scientists and ML practitioners.

- Supervised Learning

With the supervised learning technique, deep learning models are trained with output data corresponding to the input data. For example, if you were training a model to recognize email spam, you would supply the model with email data and specify which emails were spam and which were not. The model would then use backpropagation to tune itself to make its predictions match the output data it was supplied with.

Deep learning models that use supervised learning are often used in Natural Language Processing (NLP) which is designed to understand human language, as well as Computer Vision (CV) to process images and videos.

- Unsupervised Learning

Unsupervised learning is used when the output data is not supplied to the model during training. In this case, the model is only given input data with the goal of uncovering potentially interesting patterns in the provided dataset.

Examples of neural networks using this technique are Deep Belief Networks (DBN), which are comprised of stacks of either Restricted Boltzmann Machines (RBMs) or Variational Auto encoders (VAEs), and can be used in either an unsupervised or a supervised setting. These are often applied to video recognition, motion capture, image classification or even image generation tasks.

- Reinforcement Learning

Reinforcement learning involves training ML models to make a sequence of decisions. The model learns to achieve a goal in an unstructured, complex environment. When used with deep learning algorithms, this is known as Deep Reinforcement Learning (DRL). DRL is used in inventory management, demand forecasting, supply chain management, as well as financial portfolio management and stock market trading.

- Transfer Learning

Transfer learning is a technique where a model used for one task is reused as the starting point for another model working on a second task. Transfer learning can be used for Natural Language Processing or Computer Vision. It's particularly useful when the first model is already trained, speeding up development time. However, its benefits aren't able to be determined until after the second model has been trained and tested.

5) Deep Learning in Action

For such a relatively new technology, deep learning has inundated every sector of business. For consumers, deep learning and neural networks are probably most familiar in today's automotive technology, like the autopilot systems in cars produced by Tesla. Other examples of deep learning used today include:

- E Commerce: used to customize product recommendations to customers based on their unique behavior.
- Security: used to protect computer systems from viruses, as well as credit cardholders from fraud.
- Logistics: used to plan, monitor and modify shipping routes while predicting delivery times.
- Image Recognition: Deep learning has also showed a lot of success in the field of image recognition. Image recognition is the process to detect a specific person, animal, object and several variables in a certain digital image.
- Machine Translation: Machine Translation is the task of automatically translating a specific word, phrase, sentence or even a document from one language to another.

6) Objective of the Project

To counteract counterfeit documentation, theft resistant authentication mechanisms must be built into identity cards to prove the identity assertions that are made, and to protect the true and legitimate identity.

To conceal security encoded data in ID and MRTD documents while allowing for the integrity verification of the portrait.

To present a new facial image steganography method for transmitting secret messages through facial images.

To develop a portable and efficient biometric system for validating ID and travel documents.

To attach are size network to our model as an additional noise simulation module.

To help the decoder read messages from smaller photos in comparison with previous approaches.

7) Scope of the Project

In this project, the scope of a system to detect and code faces in IDs photographs is proposed with the purpose of safekeeping identities and preventing them from being easily identified. The system detects faces, applies steganography, and implements a new robust and effective encoded system. The novel system employs a key space that can be doubled depending on the security that will be implemented. It also possesses excellent properties against different types of attacks like photo substitution attack.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

II. System Analysis

I. Existing System

1) Water marks, microtext

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.

2) Laminate and holographic laminate

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.

3) Embedded technologies (magnetic stripes, barcodes, etc.)

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.

4) Biometric data (fingerprints, digital signatures, etc.)

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. [5] proposed a system, in which a predicate is defined for measuring the evidence for a boundary between two regions using Geodesic Graph-based representation of the image. The algorithm is applied to image segmentation using two different kinds of local neighborhoods in constructing the graph. Liver and hepatic tumor segmentation can be automatically processed by the Geodesic graph-cut based method. This system has concentrated on finding a fast and interactive segmentation method for liver and tumor segmentation. In the preprocessing stage, the CT image process is carried over with mean shift filter and statistical thresholding method for reducing processing area with improving detections rate. Second stage is liver segmentation; the liver region has been segmented using the algorithm of the proposed method. The next stage tumor segmentation also followed the same steps. Finally the liver and tumor regions are separately segmented from the computer tomography image.

5) Laser Engraving

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.

6) StegaStamp

StegaStamp considers a set of different image corruptions between the encoder and the decoder that successfully approximates the set of distortions resulting from real printing transmission. It was the first notable steganography model that could encode and decode hyperlinks in photos captured from real prints.

II. Disadvantages

- Fail to decode secret message from small, encoded images.
- Do not preserve sufficiently the visual structure of the encoded face, thus introducing noticeable distortion in the appearance of the face.
- Message to be encoded in a full image.
- Currently available steganography models are not suitable security systems for application to IDs and MRTDs.
- Expensive to administer
- Encroachment of privacy
- Increased threat for fraudsters to acquire people's identities
- Restricting the freedom and increasing monitoring
- Potential abuses of identification cards

III. 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.

1) Recurrent Proposal Network (RPN)

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.

2) Binary Error-Correcting Codes algorithm

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

During encoding, an arbitrary secret message is translated to a binary message using a Binary Error-Correcting Codes algorithm. subsequently during decoding, the same Binary Error-Correcting Code algorithm translates the binary message to a string with the secret message.

3) Deep Convolutional Auto Encoder

The first part of the generator is the encoder network. The aim of the encoder training process is to optimize the trade-off between its ability to restore the perceptual properties of the input images and the decoder performance to extract the hidden message. In the encoder, the facial image and the secret message are first received as inputs. At the end of the encoder application, a pre trained encoder model embeds the message in the cropped face and produces an encoded facial image. The encoded cropped image then replaces the original facial image which is subsequently printed on an ID card.

4) Deep Convolutional Auto Decoder

The decoder is designed to recover a message that is encoded in a facial image. As for the decoder, the ID card's encoded facial image is captured by a digital camera. The face detection module then detects the encoded part of the facial image, which the StegoFace decoder network then receives, retrieving the hidden message. Then the final resulting message, the retrieved message, is checked using a hash function or checksum verification algorithm to validate the message, thus providing a way to check the integrity of the face portrait in IDs and MRTDs.

IV. 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 the 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.

III. PROJECT DESCRIPTION

I. Problem Description

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 such as StegoFace is composed of two processes: the encoder and the decoder, as shown in Figure 4.1.

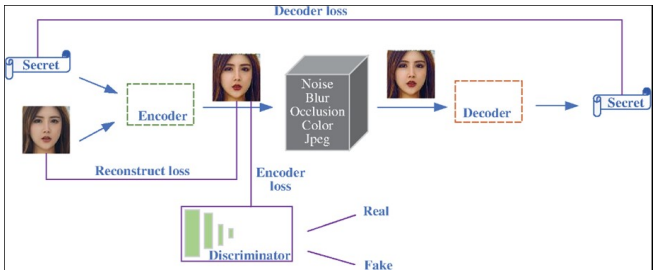


Figure 4.1 StegoFace Network

In the encoder, the facial image and the secret message 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. At the end of the encoder application, a pretrained encoder model embeds the message in the cropped face and produces an encoded facial image. The encoded cropped image then replaces the original facial image which is subsequently printed on an ID card.

As for the decoder, the ID card's encoded facial image is captured by a digital camera. The face detection module then detects the encoded part of the facial image, which the StegoFace decoder network then receives, retrieving the hidden message. A binary-error codes algorithm converts the retrieved binary message into a number or a string. Then the final resulting message, the retrieved message, is checked using a hash function or checksum verification algorithm to validate the message, thus providing a way to check the integrity of the face portrait in IDs and MRTDs.

The StegoFace encoder and decoder networks are trained using Deep Convolutional Auto Encoder-Decoder Network, whose structure is shown in Figure 4.2.

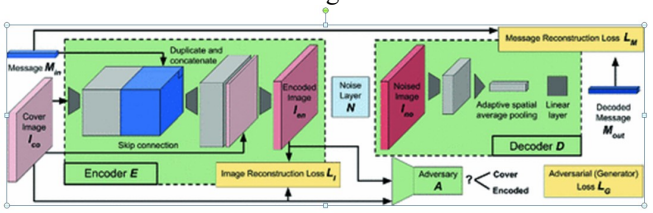


Figure 4.2 Encoder-Decoder Network

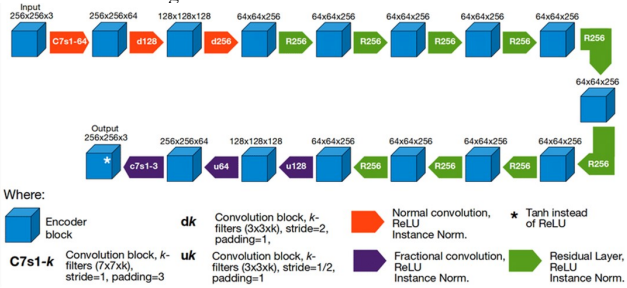


Figure 4.3 Deep Convolutional Layers

It is composed of four parts: the encoder, decoder, noise simulation module and loss functions. The encoder and decoder networks are trained to hide and read messages in facial images while the noise simulation layers, included before the decoder, create a realistic environment for the complete network during the training. Loss functions consist

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

of various pre-defined network components and additional loss functions that preserve the appearance of the encoded face and message during the training.

II. Modules Description

1) StegoFace Document Distributor Dashboard

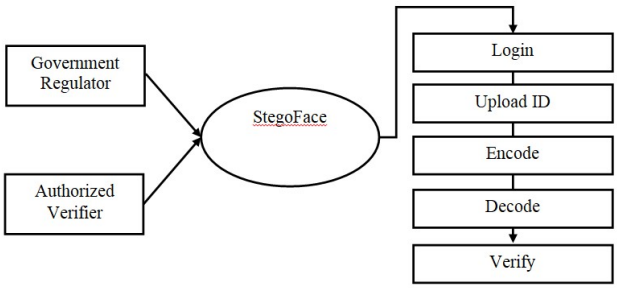
StegoFace is a new web-based security concept. It is designed to protect the ID holder's portrait against any subsequent change through an additional laser personalized portrait. The focus of this dashboard is on concealing security encoded data in ID and MRTD documents while allowing for the integrity 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.

2) Generator Control Panel

In this module the government regulator login into the StegoFace web dashboard and then upload the ID card to Auto Encoder. In the encoder, the facial image and the secret message 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) Verifier Control Panel

In this module the Authorized Verifier login into the StegoFace web dashboard and then upload the ID card to Auto Decoder. In the decoding process, a document image is first captured using a mobile camera, then the encoded part of the image (the portrait) is detected and cropped. The decoder network receives the cropped encoded face as input and recovers the binary message Sub sequently, 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 of the portrait is verified.



III. 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 resize function from the sk image 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. The main purpose of the preprocessing module is to extract usable and meaningful features through convolutional layers with different filter sizes. Initially, lower-level local features such as edges are extracted by using smaller filter sizes. The filter size is increased to help the model learn more sophisticated features. The number of filters used are 8, 16 and 32. 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.

1) Face Detection

For a robust ID verification process that conceals a message in the facial image, we need a face detection model to identify the part of the face where the secret message is hidden. It is important to note that the facial detection model should reveal the exact part of the face used to encode information. A region proposal network (RPN) is a

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

conventional technique used for various detection purposes that can be easily applied by the Open CV Toolkit. Furthermore, PR net provides a complete solution for facial detection and facial pose analysis, that increases the detection accuracy under pose variation and occlusion. Then chose PR net method as it had the best performance for these purposes. And then significantly optimized the network and reduced its size by converting the model to the Tensor Flow Lite format in order to embed it into a web application.

2) Read images

Using the read image function the ID card is upload to the web page for further process

IV. Detect faces

Region proposal network (RPN) The region proposal network (RPN) starts with the input image being fed into the backbone convolutional neural network. The input image is first resized such that its shortest side is 600px with the longer side not exceeding 1000px. The output features of the backbone network are usually much smaller than the input image depending on the stride of the backbone network. For every point in the output feature map, the network has to learn whether an object is present in the input image at its corresponding location and estimate its size. This is done by placing a set of "Anchors" on the input image for each location on the output feature map from the backbone network. These anchors indicate possible objects in various sizes and aspect ratios at this location. As the network moves through each pixel in the output feature map, it has to check whether these k corresponding anchors spanning the input image actually contain objects, and refine these anchors' coordinates to give bounding boxes as "Object proposals" or regions of interest.

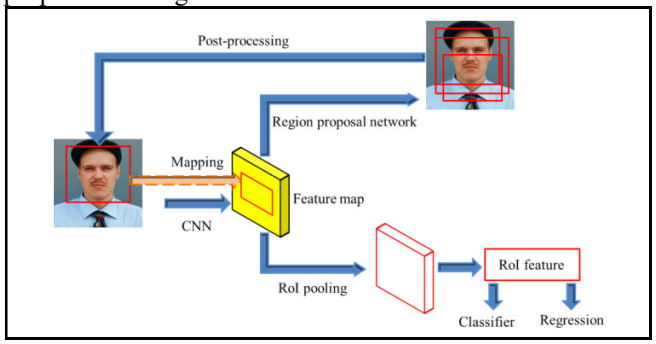


Figure 4.4 RPN

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. The region proposal network takes the feature maps provided by head network through a convolutional layer followed by Re LU activation. This convolutional layer has 512 channels as input and 512 channels as output. This output is run through two (1,1) kernel convolutional layers to produce background/foreground class scores and probabilities and their corresponding bounding box regression coefficients. The main task of RPN network is to produce promising Ro Is and that of classification network is to assign object class scores to each Ro I. Therefore, training this network requires corresponding ground truth annotations i.e., the coordinates of the bounding boxes around the faces present in an image. The ground truth comes from the image dataset. The annotation file in the data set contains the coordinates of the bounding box and the respective class label for each object present in an image. The region proposal network consists of Anchor Generation Layer and Region Proposal Layer.

V. Create boxes around faces

Show white boxes around all the faces recognized in the image. Anchor Generation Layer. This layer produces a set of bounding boxes (anchors)of varying sizes and aspect ratios. These anchors must be spread through the image and enclose the foreground objects (faces) but most of the anchors won't. The goal of the RPN network is learning to identify the anchors enclosing the faces and calculate target regression coefficients. The identified anchor is transformed to a better bounding box fitting the face more closely. Anchors with scales of 4, 8, 16, 32 and aspect ratios of 0.5, 1, 2 are used. This gives a total of12 anchors for each grid in the image. A total of W xH x 12 anchors are generated where W = w/16, H =h/16 and 16 is the sub sampling ratio. The anchors that lie outside of the image boundary have been excluded.

VI. Region Proposal Layer

The inputs to proposed system are the "region proposals" that produce a sparse or a dense set of features. In this approach a sliding window technique is used to generate a set of dense candidate regions and the Region Proposal Network is used to rank these region proposals according to the probability of a region containing faces. The region proposal layer has to identify the background and fore ground anchors and transform the foreground anchors by applying a set of regression coefficients to make them fit the face boundary. The region proposal layer consists of Proposal Layer, Anchor Target Layer and Proposal Target Layer. The proposal layer takes the anchor boxes produced by the anchor generation layer and reduces the number of anchors by applying non-maximum suppression based on the foreground scores and outputs the transformed bounding boxes by applying the regression coefficients. Anchor target layer selects promising anchors that can be used to train the RPN network to distinguish between foreground and background regions and generate good bounding box regression coefficients for the foreground boxes. RPN loss is formulated to encourage the network to classify anchors as background or foreground and transform the foreground anchor to fit the face region more closely.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

RPN Loss = Classification Loss + Bounding Box Regression Loss

The classification loss uses cross entropy loss to penalize the incorrectly classified boxes and regression loss uses a function of the distance between the true regression coefficients and the regression coefficients predicted by the RPN. The proposal target layer selects promising ROIs from the list of ROIs output by the proposal layer. These promising ROIs are used to perform RoI pooling from the feature maps produced by the head layer and passed to the rest of the network that calculates predicted class scores and box regression coefficients. The main purpose of RoI pooling is to speed up the encode/decode time and to train the whole system from end-to-end. The regions corresponding to the promising ROIs produced by proposal target layer are extracted from the convolutional feature map produced by the head network. The extracted feature maps are then run through the rest of the network to produce object class probability distribution and regression coefficients for each ROI.

VII. 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.

VIII. 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.

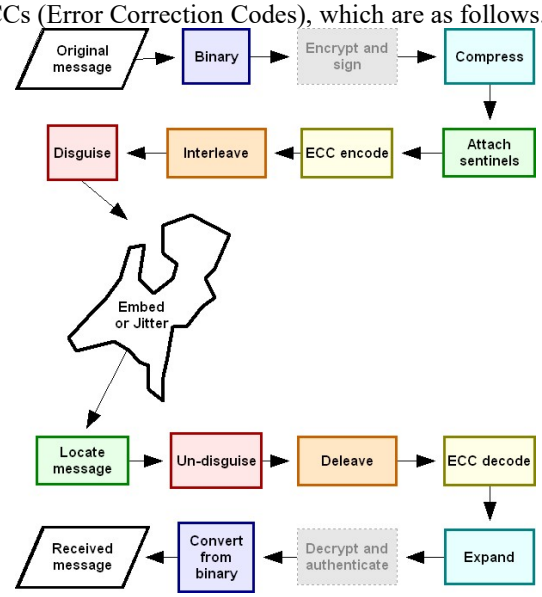


Figure 4.5 BECC

IV. BLOCK CODES

In block codes, in fixed-size blocks of bits, the message is contained. In this, the redundant bits are added for correcting and detecting errors.

1) Convolutional codes

The message consists of data streams of random length, and parity symbols are generated by the sliding application of the Boolean function to the data stream.

The hamming code technique is used for error correction.

2) Hamming Code

Hamming code is an example of a block code. The two simultaneous bit errors are detected, and single-bit errors are corrected by this code. In the hamming coding mechanism, the sender encodes the message by adding the unessential bits in the data. These bits are added to the specific position in the message because they are the extra bits for correction.

II. Deep Convolutional ID Face Steganography

1) Auto Encoder

The first part of the generator is the encoder network. The aim of the encoder training process is to optimize the trade-off between its ability to restore the perceptual properties of the input images and the decoder performance to extract the hidden message. The encoder network architecture that we selected is based on U Nets. However, the pooling layers were removed to

Preserve the information of the secret messages that may otherwise be lost during the network training. It thus receives an aligned face and a random binary message as inputs and produces an encoded image of the same size. The secret binary message is transformed (by reshaping and up sampling) to coincide with the size of the encoder input as expected. The input face image is then processed by the encoder. Since the encoder does not have pooling layers, we need to design its architecture in a special manner by manually matching the parameters of convolutions to avoid layer connection errors.

The preprocessing module and the embedding network together are designed based on an auto-encoder architecture concept. The embedding network along with the preprocessing module have a hourglass structure with an expanding phase and a contracting phase. The auto encoder network takes the input and extracts the features using the encoder part. The latent space in an auto encoder is the feature representation of the input. The decoder part of the auto encoder is used to reconstruct the output image from the latent space. Image steganography applications does not require any dimensionality changes, the latent space should be the combined feature representation of the cover image and the secret image. The embedding network takes the concatenated features from the preprocessing module as the input to produce a latent space and reconstruct the stegoface (which is close in resemblance to the cover image) from the latent space. Every bit of the secret image is hidden across every available bit of the cover image. The

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

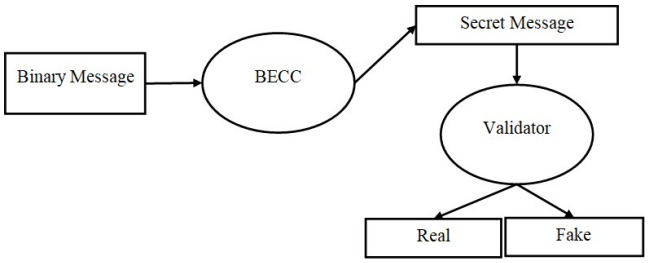
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

embedding network is designed with two convolutional layers with an increasing number of filters. The latent space at the end of the encoder represents the finer features of both cover image and the secret image concatenated. The decoder part of the embedding network has five convolutional layers with a decreasing number of filters since there is no need for any dimensionality change(s). The number of filters in the encoder part are 64, 128 and the decoder part of the embedding network has 128, 64, 32,16 and 8 filters. ReLU activation is added at the end of the convolutional layers to introduce linearity by giving the max value for positives and 0s for negatives. ReLU is used because it makes the training easier with better performance as it overcomes the vanishing gradient problem which is common in architectures with multiple layers. ReLU can be given as h(c) D max(0,c). A convolutional layer with 3 filters is placed at the end of the embedding network to convert the256 X 256 X 8 feature vector into 256 X 256 X 3 stego image output.

2) Auto Decoder

The decoder network that is incorporated into the whole architecture after applying the noise to the images. The decoder is designed to recover a message that is encoded in a facial image. For this network RPN helps to crop out the appropriate region and normalize its scale, which can simplify the subsequent steganography decoding task and lead to better performance. It removes the spatial invariance from the encoded images by applying a learnable affine transformation that is followed by interpolation.

The RPN block is placed before the DCAD. The extraction network aims to extract the secret image hidden inside the stego image. After conducting controlled experiments, an architecture identical to the embedding network seems to give the best results in extracting the secret image with minimum information loss. The extraction network has an expanding phase and a contracting phase. The number of filters, filter size, stride and other hyper parameters are fine-tuned based on the experimental results. The architecture which produced the best result is described here. The expanding encoder part of the extraction network has five convolutional layers with an increasing number of filters (8, 16, 32, 64, 128). The decoder part has five convolutional layers with a decreasing number of filters (128 ,64, 32, 16, 8). Each layer is designed with an ReLU activation. The decoder of the extraction network is followed by a convolutional layer with 3 filters to construct the extracted secret image.



3) Loss Function

All the outputs of the StegoFace generator are received by the StegoFace decoder. The decoder is designed with a set of loss functions to improve the model's performance. The most important loss functions in our model are LPIPS (Learned Perceptual Image Patch Similarity)and face embedding. Unlike conventional image reconstruction, image steganography process requires two input images and two output images. Therefore, regular loss function may not be suitable for this purpose. A customized loss function is introduced to increase the performance of the architecture. There are two losses to be calculated: the embedding loss and the extraction loss. The embedding loss is calculated between the input cover image and the output StegoFace produced by the embedding network. On the other hand, the extraction loss is calculated between the input secret image and the extracted secret image by the extraction network. The overall loss is the sum of the embedding and extraction loss. Let i be the cover image and I' the reconstructed cover image with the secret image generated by the embedding network. Also, let h be the secret image and h' the extracted secret image by the extraction network. The loss function has to be customized in such a way that it will help the model to optimize the learning function. Loss is a feedback measure given back to the model while training in each epoc has a measure of how well the model is performing through back-propagation. The loss of the embedding network, L_{emb}, is given by equation 1 and the loss of the extraction network, L_{ext}, is given by equation 2.

$$L_{emb} = |i - i'|$$

$$L_{ext} = |h - h'|$$

$$L = L_{emb} + \alpha * L_{ext} = |i - i'| + \alpha * |h - h'|$$

where α is the error adjustment and is fixed to 0.3.Initial experiments were conducted by varying the values of from 0.3, 0.6 and 0.9. Increasing the value of increased the loss and 0.3 value produced optimal loss value. The embedding network's loss function is given back to the embedding network and the overall loss is given to the extraction network to minimize the distortions of the extracted secret image.

4) Performance Evaluation

Steganographic techniques are commonly assessed using three criteria: imperceptibility, capacity, and security. A

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

further important numerical metric is the peak signal-to-noise ratio.

5) 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.

6) 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.

7) 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 systems generate signatures or artifacts when hiding a secret message. An algorithm must not leave an artifact to guide statistical attacks.

8) 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.

9) 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:

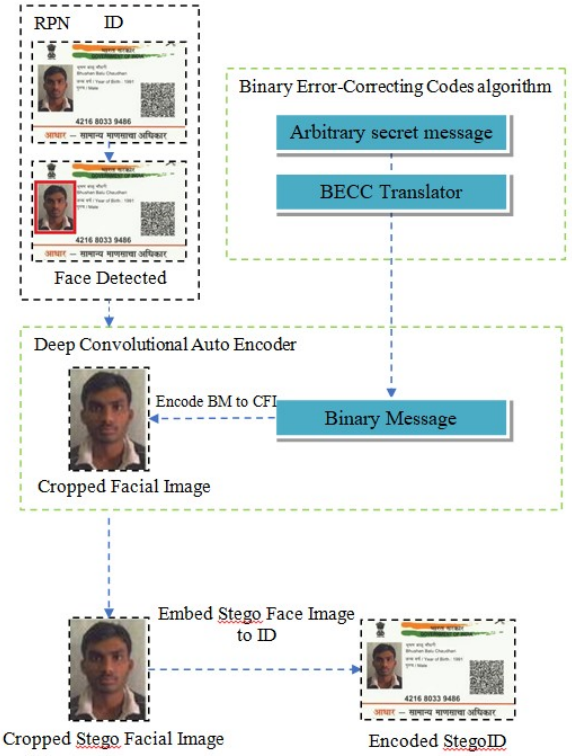
$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

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.

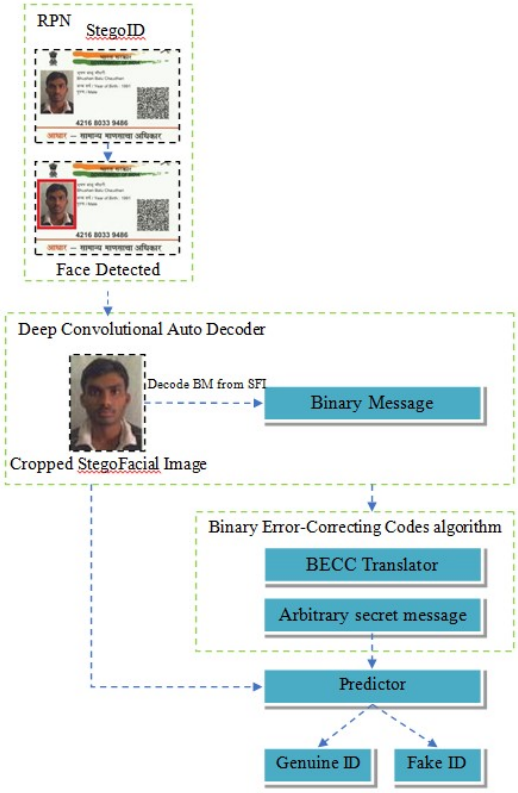
J. System Design – Deep Convolutional Auto Encoder



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

K. System Design – Deep Convolutional Auto Decoder



V. SYSTEM TESTING

In this phase of methodology, testing was carried out on the several application modules. Different kind of testing was done on the modules which are described in the following sections. Generally, tests were done against functional and non-functional requirements of the application following the test cases. Testing the application again and again helped it to become a reliable and stable system.

I. Usability Testing:

This was done to determine the usability of the application that was developed. This helped to check whether the application would be easy to use or what pitfalls would the users come through. This was used to determine whether the application is user friendly. It was used to ascertain whether a new user can easily understand the application even before interacting with it so much. The major things checked were: the system flow from one page to another, whether the entry points, icons and words used were functional, visible and easily understood by user.

II. Functional Testing:

Functional Testing is defined as a type of testing which verifies that each function of the software application operates in conformance with the requirement specification. This testing mainly involves black box testing and it is not concerned about the source code of the application. Functional tests were done based on different kind of features and modules of the application and observed that whether the features are met actual project objectives and the modules are hundred percent functional. Functional tests, as shown in the following Table-1 to Table-5, were done based on use cases to determine success or failure of the system implementation and design. For each use case, testing measures were set with results being considered successful or unsuccessful. Below are the tables which are showing some of the major test cases along with their respective test results.

III. System Testing:

In this phase of methodology, testing was carried out on the several application modules. Different kind of testing was done on the modules which are described in the following sections. Generally, tests were done against functional and non-functional requirements of the application following the test cases. Testing the application again and again helped it to become a reliable and stable system.

IV. Unit Testing:

Before you can test an entire software program, make sure the individual parts work properly on their own. Unit testing validates the function of a unit, ensuring that the inputs (one to a few) result in the lone desired output. This testing type provides the foundation for more complex integrated software. When done right, unit testing drives higher quality application code and speeds up the development process. Developers often execute unit tests through test automation.

V. Integration Testing:

Integration testing is often done in concert with unit testing. Through integration testing, QA professionals verify that individual modules of code work together properly as a group. Many modern applications run on micro services, self-contained applications that are designed to handle a specific task. These micro services must be able to communicate with each other, or the application won't work as intended. Through integration testing, testers ensure these components operate and communicate together seamlessly.

VI. CONCLUSION

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 – Stego Face - which is optimized for facial images printed in common IDs and MRTDs. Stego Face 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

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

camera. Stego Face 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. The novel idea proposed in this research is to attach are size network to our model as an additional noise simulation module. This is designed to help the decoder read messages from smaller photos in comparison with previous approaches. The resize network decreases the size of the encoded images that the decoder receives. Facial images encoded with our Stego Face approach outperform the Stega Stamp 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.

VII. References

[1] 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.

[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] Christo Ananth, D.L.Roshni Bai , K.Renuka, C.Savithra, A.Vidhya, “Interactive Automatic Hepatic Tumour CT Image Segmentation”, International Journal of Emerging Research in Management &Technology (IJERMT), Volume-3, Issue-1, January 2014,pp 16-20

[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] Christo Ananth, D.L.Roshni Bai, K.Renuka, A.Vidhya, C.Savithra, “Liver And Hepatic Tumors Segmentation in 3-D CT Images”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3,Issue-2, February 2014,pp 496-503.

[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.