ENHANCED SECURITY MEASURES FOR NATIONAL IDENTITY CARD USING IMAGE STEGANOGRAPHY

M.VASUKI[1], Dr.T.AMALRAJ VICTOIRE[2] , M.SWETHA SRI[3]

Associate professor[1] , Professor[2] , PG student[3]
dheshna@gmail.com, amalrajvictoire@gmail.com, swethasri16062002@gmail.com
Department of Master Computer Application, Sri Manakula Vinayagar, Engineering College, Pondicherry-605 107 ,India.

ABSTRACT:

National identity documents are essential cards issued by official authorities, typically containing a photo and used for various purposes within a country, such as travel, electronic identification, and access to secure locations. These documents incorporate multiple security features to combat forgery, yet criminals increasingly target the manipulation of genuine documents and facial images. Trusted identity is crucial for societal function, necessitating continuous improvements in security measures by governments and ID manufacturers. To address this, we present StegoCard, a novel steganography method specifically designed for concealing messages within facial images commonly found on IDs. StegoCard employs a series of Deep Convolutional Auto Encoders to embed secret messages into facial portraits, creating stego facial images. These stego images can then be decoded by Deep Convolutional Auto Decoders, even after being printed and captured digitally. Our StegoCard approach outperforms existing methods like StegaStamp in terms of perceptual quality, as demonstrated by metrics such as Peak Signal-to-Noise Ratio, hiding capacity, and imperceptibility. By leveraging deep learning and steganography, StegoCard enhances the security of national identity documents, contributing to the preservation of trusted identities within society.

KEYWORD:Deep Learning, Steganography,Recurrrent proposal Network(RPN)

1. INTRODUCTION

Identity documents are foundational tools for verifying one's identity. Whether in the form of identity cards, passport cards, or other standardized formats, these documents play a critical role in personal identification. Some jurisdictions mandate national identification cards, while others accept regional or informal documents for this purpose. When these documents include a photograph, they are commonly referred to as photo IDs. Steganography, an ancient practice with modern applications, involves concealing secret information within seemingly innocuous documents or media. The term "steganography" originates from Greek roots, meaning "hidden writing," underscoring its core function of concealment. Unlike cryptography, which involves encrypting data with keys, steganography focuses on hiding messages without altering the original data. In the digital age, steganography has evolved significantly. It enables covert communication through various mediums and techniques, providing a means for secret communication and manipulation. While cryptography primarily ensures privacy, steganography specializes in secrecy and deception. Steganography offers several advantages over cryptography. It can embed messages in images, audio files, or even text, making detection challenging. Additionally, steganographic messages may be hidden in plain sight, further complicating detection efforts. Furthermore, steganography does not rely on encryption keys, reducing the risk of interception and decryption. One common application of steganography is in digital images. By subtly altering pixel values or hiding data within image files, steganographic techniques can conceal messages within photographs or other visual media..

LITERATURE SURVEY

Utilizing GAN-Based Face Synthesis and Morphing for Secure Authentication in IoT through Steganographic Secret Sharing. This paper introduces a novel secret sharing scheme employing deep learning-driven steganography and image morphing techniques, specifically focusing on face images as cover images. The authors commence by training a generator through a generative adversarial network (GAN) along with independent extractors based on Convolutional Neural Networks (CNNs), utilizing shared participant keys. The secret shares are then embedded within shadow images using the generator and participant keys. Subsequently, the dealer utilizes the shared participant images as source images and the shadow images as target images to generate morphed images for shadow image authentication.

Detecting Digital Data Tampering Forensically through Image Steganography and S-Des. Cryptography transforms plaintext into ciphertext (unreadable text), while steganography involves concealing secret messages within other messages. Initially, data is encrypted using the Simplified Data Encryption Standard (S-DES) algorithm. Subsequently, the encrypted message is embedded in the cover image using the Least Significant Bit (LSB) approach.

FakeSafe: Achieving Human-Level Steganography Through Disinformation Mapping Utilizing Cycle-Consistent Adversarial Networks. The FakeSafe approach aims to effectively conceal private information by mapping it onto a realistically looking but fake message. The author develops a multi-step FakeSafe mapping strategy employing a series of stenographic functions, thereby significantly enhancing the security of sensitive data. Even if attackers identify the message as fake, they may struggle to discern the number of mapping steps involved, further complicating their efforts. Additionally, a steganography method is devised to accommodate various data domains, including images and text. The fake message can originate from the same domain as the original private information or an entirely different domain, thereby enhancing the framework's resilience. Furthermore, a coverless solution is introduced for conducting steganography.

Methodologies:

Recurrent Proposal Network (RPN)

The Region Proposal Network (RPN) is a fully convolutional network capable of predicting object bounds and objectless scores simultaneously at every position. Trained end-to-end, the RPN excels in generating top-quality region proposals. Its design ensures efficient prediction of region proposals across various scales and aspect ratios. RPNs leverage anchor boxes as reference points across multiple scales and aspect ratios. This approach can be likened to a pyramid of regression references, eliminating the need to enumerate images or filters with diverse scales or aspect ratios.

The Binary Error-Correcting Codes (BECC) algorithm.

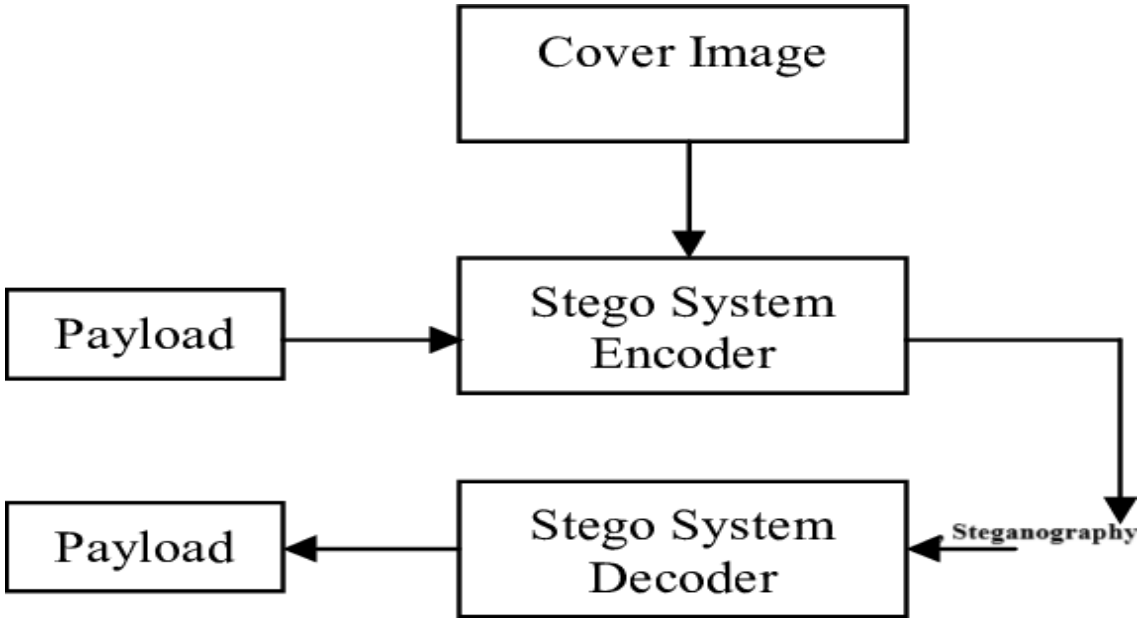
During encoding, an arbitrary secret message is translated to a binary message using a Binary Error-Correcting Codes algorithm. Subsequently during decoding, the same Binary Error-Correcting Code algorithm translates the binary message to a string with the secret message.

Deep Convolutional Auto Encoder

The initial segment of the generator comprises the encoder network, tasked with a dual objective: balancing its capability to restore the perceptual qualities of input images and optimizing the decoder's efficacy in extracting hidden messages. Within the encoder, both the facial image and the secret message are initially inputted. Subsequently, a pretrained encoder model integrates the message into the cropped face, generating an encoded facial image. This encoded cropped image supplants the original facial image, thereafter printed onto an ID card..

Deep Convolutional Auto Decoder

The decoder is tailored to extract a message encoded within a facial image. In the decoding process, the encoded facial image from the ID card is captured by a digital camera. Subsequently, the face detection module identifies the encoded region within the facial image, which is then passed to the StegoFace decoder network. This network extracts the hidden message from the encoded region. Following this extraction, the resulting message undergoes verification using a hash function or checksum algorithm to ensure its integrity. This validation process offers a means to verify the authenticity of the facial portrait in IDs and Machine-Readable Travel Documents (MRTDs).



Advantages

A novel approach is introduced to enhance security, robustness, imperceptibility, and information hiding capacity in facial image steganography. This streamlined architecture ensures lightweight yet effective implementation, aimed at minimizing suspicion and scrutiny. With the integration of a resize layer, StegoFace excels in extracting messages from smaller images, offering a seamless solution for real-world document validation systems such as ID cards and MRTDs. This innovation promises not only heightened security protocols but also cost-effective implementation, making it a practical choice for various applications.

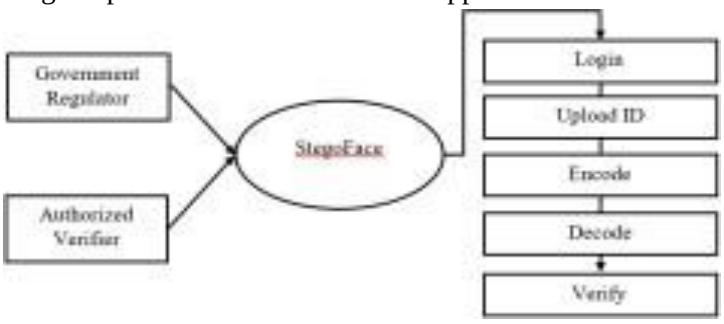


Fig.1 Verifier control panel

RESULTS AND DISCUSSION

In assessing our method's performance, we benchmark it against the current state-of-the-art techniques using the FDDB dataset. Key evaluation metrics encompass the recall rate, gauging the ratio of detected faces to the total marked faces within the sample, and false positives, representing errors in detected face identification. These metrics are visualized through ROC (Receiver Operating Characteristic) curves, providing a comprehensive comparison of method effectiveness and accuracy.

The AUC (Area Under the Curve) metric is employed alongside the ROC curve to offer a clearer assessment of method superiority. AUC quantifies the proportion of area under the ROC curve, ranging between 0 and 1, where higher values denote superior method performance. Subsequently, our model's efficacy is evaluated on the WIDER FACE dataset, renowned for its challenging face detection benchmarks compared to FDDB. Remarkably, our model consistently demonstrates competitive performance across all three subsets of the dataset. Notably, it exhibits heightened robustness in detecting faces with substantial occlusion and angle variations, aligning closely with the evaluation findings from the FDDB dataset.

CONCLUSION

This paper introduces StegoFace, a pioneering steganography method tailored specifically for concealing security-encoded data within ID and MRTD documents, while ensuring the integrity verification of the portrait. StegoFace represents a significant advancement as the first efficient solution optimized for facial images commonly found in such documents. It comprises an end-to-end Deep Learning Network, consisting of a Deep Convolutional Auto Encoder for encoding a secret message into a face portrait, and a Deep Convolutional Auto Decoder for extracting the message from the encoded image, even after printing and subsequent capture by a digital camera. StegoFace outperforms existing methods by enabling the use of images within their contextual settings, irrespective of background variations. This flexibility eliminates restrictions related to photo parameters. Moreover, facial images encoded with StegoFace demonstrate superior perception quality compared to those generated by other methods like StegaStampStegoFace is a breakthrough in steganography, designed specifically for hiding security-encoded data within ID and MRTD documents while maintaining portrait integrity verification. Unlike previous methods, StegoFace focuses on concealing data within facial images commonly found in these documents. It utilizes an end-to-end Deep Learning Network, including a Deep Convolutional Auto Encoder for embedding secret messages into facial portraits, and a Deep Convolutional Auto Decoder for extracting the message even after printing and subsequent digital capture.What sets StegoFace apart is its ability to seamlessly integrate images within their contextual settings, regardless of background variations. This eliminates restrictions typically imposed by photo

parameters. Additionally, facial images encoded with StegoFace exhibit higher perception quality compared to other methods like StegaStamp. Overall, StegoFace represents a significant advancement in steganography, offering enhanced security measures for identity documents.

REFERENCES

[1] A. Ferreira, E. Nowroozi, and M. Barni, ‘‘VIPPrint: Validating synthetic image detection and source linking methodson 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 neuralface detection on mobile GPUs,’’ 2019, arXiv:1907.05047.

[3] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ‘‘ArcFace: Additive angular margin loss for deep face recognition,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4685–4694

[4] R. L. Jones, Y. Wu, D. Bi, and R. A. Eckel, ‘‘Line segment code for embedding information,’’ U.S. Patent App. 16236 969, Jul. 4, 2019.

[5] S. Ciftci, A. O. Akyuz, and T. Ebrahimi, “A Reliable and Reversible Image Privacy Protection Based on False Colors,” IEEE Transactions on Multimedia, vol. 20, no. 1, pp. 68–81, 2018.

[6] M. Jiménez Rodríguez, C. E. Padilla Leyferman, J. C. Estrada Gutiérrez, 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.