IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

FACE COUNTERFEIT DETECTION IN NATIONAL ID CARDS USING IMAGE STEGANOGRAPHY

[1]C.Surya, [2]P.Nivashini, [3]K.Aboorva, [4]S.Logeshwari,[5]A.Pugazhvani

[1]Assistant Professor, [2,3,4,5]Student
[1]Computer Science and Engineering,
[1]Sri Ramakrishna College Of Engineering, Perambalur, Tamil Nadu, India

Abstract : Counterfeit national ID cards can pose a serious threat to national security and public safety, as they can be used for identity theft, fraud, and other criminal activities. Therefore, it is crucial to have reliable mechanisms to detect counterfeit ID cards. One approach to improving the security of national ID cards is to use steganography, a technique that involves hiding additional data within an image without significantly altering its appearance. Steganography is the practice of concealing a message or information within another object, such as an image, without changing its appearance significantly. In the context of national ID cards, steganography can be used to embed additional data orfeatures in the card's images that can help in detecting counterfeit cards. Select the features that will be embedded in the ID card image. In this system, user's idnumber taken for embedding into the ID card. User's Id number can be converted into a binary data and then that can be embedded in the ID card. The features can be embedded using a steganography algorithm called LSB. LSB algorithm modifies the Least Significant Bits of the ID card image pixels to embed the additional features. To verify the embedded features, data extraction approach can be used that reads the embedded data from the ID card image and verifies its authenticity. By using steganography to embed additional features in national ID card images, it becomes much more difficult to create counterfeit cards. The embedded features can be verified by proposed system, making it easier to detect fake cards.

***IndexTerms* - Counterfeit National ID Cards, Reliable Mechanisms, Steganography.**

I. INTRODUCTION

INTRODUCTION

Managing security means understanding the risks and deciding how much risk is acceptable. Different levels of security are appropriate for different organizations. No network is 100 percent secure, so don't aim for that level of protection. If you try to stay up-to-date on every new threat and every virus, you'll soon be a quivering ball of anxiety and stress. Look for the major vulnerabilities that you can address with your existing resources. Here present numerous advantages of computer networks and the Internet.

Connecting your network to the Internet provides access to an enormous amount of information and allows you to share information on an incredible scale. However, the communal nature of the Internet, which creates so many benefits, also offers malicious users easy access to numerous targets. The Internet is only as secure as the networks it connects, so we all have a responsibility to ensure the safety of our networks. Information security is the process of securing information data from unauthorized access, use, modification, tempering, or disclosure. Including any attempt to probe, scan or test the vulnerability of a system, server or network or to breach security or authentication measures without express authorization of the owner of the system, server or network. Members of the University should not run computer programs that are associated with hacking without prior authorisation. Obtaining and using such programs is not typical of normal usage and may therefore otherwise beregarded as misuse.

TYPES OF SECURITY MEASUREMENTS

3.1 AUTHENTICATION

Authentication is used by a client when the client needs to know that the server is system it claims to be. In authentication, the user or computer has to prove its identity to the server or client. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints. Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

3.2 Authorization

Authorization is a process by which a server determines if the client has permission to use a resource or access a file. Authorization is usually coupled with authentication so that the server hassome concept of which the client is that is requesting access.The type of authentication required for authorization may vary; passwords may be required in some cases but not in others. In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

3.3 Encryption

Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key. The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. The SSL drives the secure part of "https://" sites used in e-commerce sites (like E-Bay and Amazon.com.) All data in SSL transactions is encrypted between the client (browser) and the server (web server) before the data is transferred between the two. All data in SSH sessions is encrypted between the client and the server when communicating at the shell. By encrypting the data exchanged between the client and server information like social security numbers, credit card numbers, and home addresses can be sent over the Internet with less risk of being intercepted during transit.

EXISTING SYSTEM

Face counterfeit detection in ID cards is a crucial issue in today's world, where the use of fake IDs has become increasingly prevalent. National ID cardsare used for various purposes, including voting, obtaining government services, opening bank accounts, and many more.

As a result, national ID cards need to be secure and reliable to prevent any potential harm that might be caused by counterfeit cards. In the case of counterfeit ID cards, hackers can reconstruct the facial image of original user into fake one. Existing counterfeit detection techniques are not well suitable for real time detection process.

Techniques such as analyzing facial movements, detecting blinking, assessing depth perception, or requiring specific actions from the user can be employed for this purpose. Biometric authentication methods such as fingerprintscans or iris recognition can complement facial recognition, adding an extra layer of security. Through collaboration between government agencies, law enforcement, technology companies, and academia, comprehensive and effective counterfeit detection systems for ID cards can be developed, mitigating risks across various sectors.

PROPOSED SYSTEM

Face counterfeit detection in national ID cards is a crucial issue in today's world, where the use of fake IDs has become increasingly prevalent. NationalID cards are used for various purposes, including voting, obtaining government services, opening bank accounts, and many more. As a result, national ID cards need to be secure and reliable to prevent any potential harm that might be caused by counterfeit cards.

In the case of national ID cards, steganography can be used to embed additional features or data in the card's images that can help in detecting counterfeit cards. This can include holographic images, watermarks, barcodes, or other features that are difficult to replicate.

By using steganography to embed additional features in national ID card images, it becomes much more difficult to create counterfeit cards, making it easier to ensure the security and authenticity of national ID cards. One of the primary challenges in detecting counterfeit national ID cards is that the counterfeiters are continually improving their techniques, making it increasinglydifficult to distinguish between genuine and fake cards.

The LSB algorithm ensures that the changes made to the ID card imageare subtle and not easily detectable by the naked eye. The use of a data extraction approach allows for the verification ofembedded features, making it easier to detect counterfeit cards. Embedding features in the ID card, making it more challenging forcounterfeiters to replicate.

IV. MODULE DESCRIPTION

4.1 Framework Creation

National ID cards are used for various purposes, including voting, obtaining government services, opening bank accounts, and many more. As a result, national ID cards need to be secure and reliable to prevent any potential harm that might be caused by counterfeit cards. A secure counterfeit ID card detection system could be implemented using steganography approach. Here users are obtaining their information and then the server provides the unique ID number to the User. Then implement stegnography approach to create secure IDcard. This will helps to detect whether the provided ID card is valid or fake one.

4.2 User Process

This module explains about process carried out by user to generate ID card. Here user should enter their information such as name, address, date of birth, email id, aadhar number, mobile number and user image, etc. These details are sending to the server for further verification process. Usingthese details server can generate ID card for particular user.

4.3 Provide ID Number

This This process explains about ID number generation for each user. After receiving details from user, server will generate unique ID card number for regarding user. This ID number helps to predict whether the user is valid or not. The server uses the details submitted by the user to generate a unique ID card number that can be used to verify the user's identity. This unique ID number is typically composed of two parts: the user's personal details and a randomly generated string of characters Here random number generation technique implemented to generate unique ID card number.

4.4 Steganography process

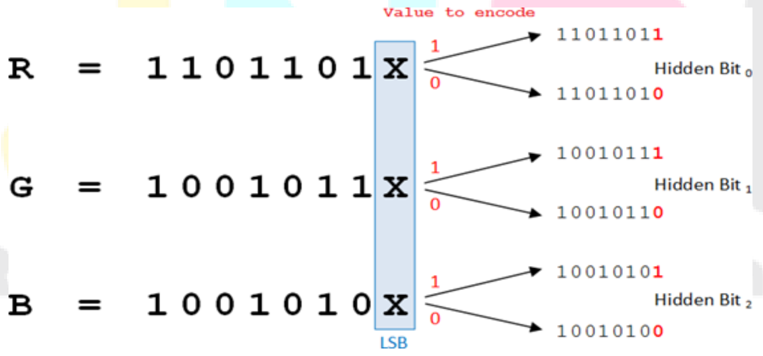
Data hiding is the process of hiding secret message into cover file. In this application ID number is considered as secret message is present in the form of text and cover file is user face image. The unique ID card number of the user was hidden within the user’s face image to create stegno image. In the process of embedding, the cover image is divided into non-overlapping pixel blocks of 3x3 pixel blocks. Block levels are based cardinality of the cover image. If secretbit is 1 and LSB of stego pixel is 0 or vice-versa, then 1 is added or subtractedto the stego pixel.

LSB(Least Significant Bit)

In the embedding process of a secret message, a cover image is partitionedinto non-overlapping blocks of nine consecutive pixels. A difference value is calculated from these values of the nine pixels in eachblock. All possible difference values are classified into a number of ranges. The calculated difference value then replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value. The way of embedding the secret information within the cover file is called LSB insertion. In proposed technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit colour images are used to perform LSB, then the amount of modification will be small.

LSB Encoding

First the unique image and the compressed encrypted secret message are taken. Then the encrypted secret facts need to be transformed into binary format.



Binary conversion is accomplished via taking the American Standard Code of Information Interchange (ASCII) values of the person and converting them into binary layout and producing move of bits. Similarly, in cover photo, bytes representing the pixels are taken in unmarried array and byte stream is generated. Message bits are taken sequentially after which are positioned in LSB little bit of image byte. Same process is followed till all the message bits are located in photograph bytes. Image generated is called ‘Stegno-Image’. It is prepared for transmission through the Internet.

LSB Decoding

First, ‘Stegno-Image’ is taken and single array of bytes are generated as itbecome carried out at the time of encoding. The general number of bits of encrypted secret information and the bytes representing the pixels of stegno- image are taken. Counter is to begin with set to 1, which in turn offers the index range of the pixel byte where secret message bit is available in LSB. The procedure is continued till very last secret message bit is reached. After this, the bit circulation of the message shall be generated.

Available bits are grouped to shape bytes such that each byte represents single ASCII character. Charactersare stored in textual content record which represents the encrypted embedded message. After that the decryption and decompression are to be done.

4.5 Counterfeit ID Card Detection

This module explains about the process of detecting original ID cards and Fake ID cards. Verifier can check whether the user's ID card is valid or not. Data extraction is the process of extracting the embedded information from cover file. In proposed application system will automatically check the embedded ID number with user's original ID number. If numbers are same, it will show the ID card is valid. Otherwise shows the message of "Invalid ID carddetected". A small system error can conceivably explode into a much larger Problem. Effective testing early in the purpose translates directly into long term cost savings from a reduced number of errors. Another reason forsystem testing is its utility, as a user-oriented vehicle before implementation.

A program represents the logical elements of a system. For a program to runsatisfactorily, it must compile and test data correctly and tie in properly with other programs. Achieving an error free program is the responsibility of the programmer. Program testing checks for two types of errors: syntax and logical.

CONCLUSION

In conclusion, the integration of steganography, specifically the LSB algorithm, into the design of national ID cards presents a robust solution to bolster security measures against counterfeiting and fraudulent activities. By embedding additional features such as the user's ID number directly into the image data, without significantly altering its appearance, this approach ensures that crucial identification information remains securely encoded within the card.Through the proposed system, verification of the embedded features becomes streamlined, allowing for swift and reliable authentication processes. By extracting and comparing the embedded data, authorities can efficiently detect any discrepancies, thus enabling prompt action against potential instances of forgery or misuse.

REFERENCES

[1] Wu, Rongliang, Gongjie Zhang, Shijian Lu, and Tao Chen. "Cascade ef-gan:Progressive facial expression editing with local focuses." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 5021- 5030. 2020.

[2] Li, Yuezun, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. "Celeb-df: A large-scale challenging dataset for deepfake forensics." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 3207- 3216. 2020.

[3] Shen, Yujun, Jinjin Gu, Xiaoou Tang, and Bolei Zhou. "Interpreting the latent space of gans for semantic face editing." In Proceedings of the IEEE/CVFconference on computer vision and pattern recognition, pp. 9243-9252. 2020.

[4] Nirkin, Yuval, Yosi Keller, and Tal Hassner. "FSGANv2: Improved subject agnostic face swapping and reenactment." IEEE Transactions on Pattern Analysis and Machine Intelligence 45, no. 1 (2022): 560-575.

[5] Nguyen, Thanh Thi, Quoc Viet Hung Nguyen, Dung Tien Nguyen, Duc Thanh Nguyen, Thien Huynh-The, Saeid Nahavandi, Thanh Tam Nguyen, Quoc-Viet Pham, and Cuong M. Nguyen. "Deep learning for deepfakes creationand detection: A survey." Computer Vision and Image Understanding 223 (2022): 103525.

[6] Huang, Yihao, Felix Juefei-Xu, Qing Guo, Yang Liu, and Geguang Pu. "Fakelocator: Robust localization of GAN-based face manipulations." IEEE Transactions on Information Forensics and Security 17 (2022): 2657-2672.

[7] Wang, Zhi, Yiwen Guo, and Wangmeng Zuo. "Deepfake forensics via an adversarial game." IEEE Transactions on Image Processing 31 (2022): 3541- 355

[8] Rana, Md Shohel, Mohammad Nur Nobi, Beddhu Murali, and Andrew H. Sung. "Deepfake detection: A systematic literature review." IEEE Access (2022).

[9] Wubet, Worku Muluye. "The deepfake challenges and deepfake video detection." Int. J. Innov. Technol. Explor. Eng 9 (2020).

[10] Tripathy, Soumya, Juho Kannala, and Esa Rahtu. "Facegan: Facial attribute controllable reenactment gan." In Proceedings of the IEEE/CVF winter conference on applications of computer vision, pp. 1329-1338. 2021.

[11] C. Chu, A. Zhmoginov, and M. Sandler, "CycleGAN, a master ofsteganography," 2017, arXiv:1712.02950.

[12] V. Albiero et al., "Identity document to selfie face matching across adolescence," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Sep. 2020, pp.

[13] M. Stokkenes, R. Ramachandra, and C. Busch, "Biometric transaction authentication using smartphones," in Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG), Sep. 2018, pp. 1–5.

[14] P. Perera and V. M. Patel, "Face-based multiple user active authentication on mobile devices," IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1240– 1250, May 2019.

[15] M. E. Fathy, V. M. Patel, and R. Chellappa, “Face-based active authentication on mobile devices,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Apr. 2015, pp. 1687–1691.

[16] V. V. Arlazarov, K. B. Bulatov, and T. S. Chernov, “MIDV-500: A dataset for identity documents analysis and recognition on mobile devices in video stream,” 2018, arXiv:1807.05786.

[17] X. Zhu et al., “Large-scale bisample learning on ID versus spot face recognition,” Int. J. Comput. Vis., vol. 127, nos. 6–7, pp. 684–700, Jun. 2019.

[18] R. Lara, A. Valenzuela, D. Schulz, J. Tapia, and C. Busch, “Towards an efficient semantic segmentation method of ID cards for verification systems,” 2021, arXiv:2111.12764.

[19] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “ImageNet: A large-scale hierarchical image database,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2009, pp. 248–255.

[20] T. Salimans, I. J. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, “Improve techniques for training GANs,” 2016, arXiv:1606.03498.