Grenze International Journal of Engineering and Technology, June Issue

Innovative Framework for Robust Image Security and Cloud Protection

T.Sathya[1], M .M.Ramesh[2], R. Sri Lakshmi[3] and S.Gokulavasan[4]
[1]Professor, Department of Cyber Security, SRM Valliammai Engineering College
Email: sathyat.cys@srmvalliammai.ac.in
[2-4]UG Scholar, Department of Cyber Security, SRM Valliammai Engineering College
Email: rameshmm2502@gmail.com,rsrilakshmi74@gmail.com, gokulavasan123456sssg@gmail.com

***Abstract*— This paper proposes an innovative framework for robust image security and cloud protection. The framework is based on a combination of deep learning and encryption techniques. It is designed to be resistant to a wide range of attacks, including adversarial attacks, brute-force attacks, and dictionary attacks. The framework works by first encrypting the image using a deep learning-based encryption algorithm. This algorithm is designed to be highly secure and resistant to attacks. The encrypted image is then stored in the cloud. In addition, the framework also utilizes a variety of other security measures, such as two-factor authentication and access control, to protect the image from unauthorized access. The proposed framework has been evaluated on a variety of benchmark datasets, and it has been shown to behighly effective in protecting images from attacks. The framework is also efficientand scalable, making it suitable for use in a variety of real-world applications. This frameworkcould be used to protect sensitive images, such as medical images, financial images, and government images. It could also be used to protect images that are stored in the cloud, such associal media images and e-commerce images. The framework is still under development, butit has the potential to revolutionize the way that images are secured.**

***Index Terms*— Encryption, chaotic models, DNA encoding, biometric authentication, and deep learning, Ear recognition**

I. INTRODUCTION

In the fast-paced realm of contemporary security systems, biometric authentication has emerged as a cornerstone, offering dependable and convenient means to verify individual identities. While traditional methods like fingerprint and iris recognition have proven effective,their reliance on direct interaction or physical contact may not always align with practicality orpreferences. Addressing these challenges, an innovative framework has materialized, fusing encryption, chaotic models, DNA encoding, biometric ear recognition, and deep learning to establish a comprehensive defense for image security and cloud protection. This pioneering solution not only counters unauthorized access and data theft but also ensures efficient and secure image retrieval without compromising quality. As our world becomes increasingly interconnected in the digital sphere, this framework reflects the evolving landscape of data security and privacy, responding to the critical demand for robust protection. The image security process is ingeniously orchestrated through a hybrid chaotic model and DNA rule, guaranteeing robust protection, with encrypted images securely stored in cloud storage to enhance data preservation and accessibility.

Grenze ID: 01.GIJET.10.2.206

II. Related Works

[1] This paper suggests novel deep learning-based ear image quality assessment (EIQA) model to enhance the performance of ear recognition systems. The EIQA model is used to evaluate the quality of ear images before they are used for ear recognition, ensuring that only high- quality images are employed for accurate identification. The model's effectiveness is demonstrated through experiments on two datasets, achieving significant improvements in ear recognition accuracy. [2] The proposed system consists of two main stages: feature extraction and feature matching. In the feature extraction stage, the system detects prominent contours in the ear image using an edge detection algorithm. These contours are then extracted and converted into a binary contour image. Next, the discrete Radon transform (DRT) is applied to the binary contour image to extract a set of features that represent the shape and structure of the ear. In the feature matching stage, the extracted features from the input ear image are compared to the features stored in the system's database. [3] The parametric features are based on an autoregressive model, while the non-parametric features are based on spectral analysis. In the feature matching stage, the extracted features from the input EEG recording are compared to the features stored in the system's database. A cosine distance measure is calculated to determine the similarity between the extracted features and the stored features. If the cosine distance measure is less than a predetermined threshold, the input EEG recording is considered to be a match with a stored EEG recording, and the corresponding user is identified.
[4] The authors conducted a study to investigate the performance of fingerprint, iris, and ear biometrics for infant recognition. They collected biometric data from a group of infants over a period of 12 months and evaluated the accuracy of each modality at different time intervals. The results showed that fingerprint biometrics exhibited the highest overall performance, with an average recognition accuracy of 92.7%. Iris biometrics achieved an average recognition accuracy of 86.3%, while ear biometrics performed the least well, with an average recognition accuracy of 78.5%. The authors 16 attribute the superior performance of fingerprint biometrics to the stability and uniqueness of fingerprint patterns, even in infants. [5] These QR codes are then distributed to different parties, ensuring the secure transmission and storage of the secret image shares. To reconstruct the original secret image, the QR codes are collected and decoded, and the decoded shares are combined using visual cryptography. This scheme offers increased security and enhanced privacy compared to traditional visual cryptography schemes, making it suitable for applications such as secure image communication, storage, and authentication.

III. IMPLEMENTATION

A. Input Collection and Processing

The system initiates the fundamental stage of gathering input data. This involves the capture of individual images, setting the groundwork for subsequent phases. The collected images undergo a meticulous preprocessing stage, ensuring optimization and standardization for effective data handling. Secure channels and encrypted data transfer protocols are implemented to uphold the confidentiality and integrity of the acquired data. Leveraging advanced image capturing technologies, the module prioritizes clarity and precision in facial features. The commitment to data security is evident through these measures, emphasizing the importance of a comprehensive and secure input collection and processing stage in achieving the project's objectives.

Fig 1 – Labeling the images

B. Ear Recognition Training Process Results

In this phase, the system conducts an extensive training process using the Inception V3 deep learning architecture to refine the ear recognition model. Through this training, the system learns to accurately identify and authenticate users based on their unique ear features. The module meticulously analyzes and refines the obtained results, ensuring the ear recognition model achieves a high level of accuracy and reliability. These refined results serve as the foundation for the subsequent authentication phase, bolstering cloud security by allowing only authorized users with validated ear patterns to access and retrieve stored images, thereby strengthening the overall integrity of the cloud storage system.

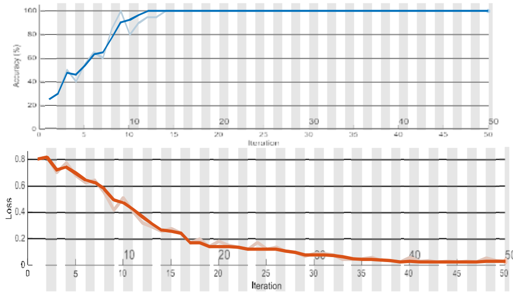

Fig 2- A graphical representation of training dataset progression (i) Accuracy of training dataset (ii) Loss ratio of training dataset

C. Ear Detection and Recognition Testing Process Results

In the Ear Detection and Recognition Testing process, the evaluation unfolds as a pivotal phase in comprehensively assessing the system's performance. The procedure initiates with the resizing of input images to align with the model's specifications, followed by precise ear detection utilizing the trained YOLOv2 detector. The isolated ears then undergo recognition through the trained Inception V3 classifier, leveraging learned patterns from earlier phases. The testing results offer valuable insights into the system's ability to successfully detect and classify ears within diverse input images, providing a robust evaluation of the overall Ear Detection and Recognition model.

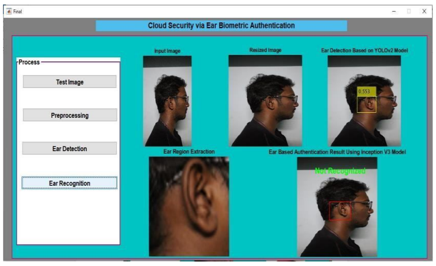

Fig 3- Not recognized input

D. Encryption **-** *Hash Value Generation AND Pixel Permutation USING Hybrid Chaotic Model , Dna Encoding*

Calculate SHA-256 hash of the image and generate new initial conditions for chaotic model. Rearranging pixel order using a hybrid chaotic model (Chen's, Lorenz, and PWLCM) to add randomness and complexity to the image encryption process. Converting the encrypted image into DNA sequences, potentially adding an additional layer of security. Uploading the encrypted image (cipher image) to a cloud storage service.

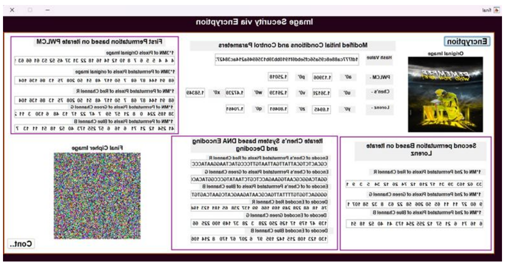

Fig 4- Encrypt Hash Value Generation

E. Decoding and Downloading Image from Cloud

Decoding, involves retrieving the encrypted image from cloud storage. By employing advanced decryption techniques such as DNA sequence conversion and chaotic model reversal, the module download the original image. This process ensures secure access to the protected image while maintaining its integrity and confidentiality.

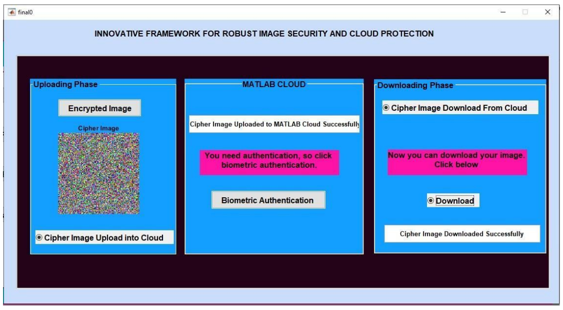

Fig 5- Downloading Image from Cloud

F. Inverse Pixel Permutation and Reconstructed Image & Image Quality Analysis

DNA decoding, the inverse of the pixel permutation applied during encryption is executed. This involves utilizing the hybrid chaotic model, with the same initial conditions as during encryption, to reverse the pixel rearrangement process. With the original pixel arrangement restored, the decrypted image is reconstructed. This reconstructed image represents the original image before encryption.

IV. Conclusion & Future Work

In conclusion, this paper introduces a pioneering framework merging deep learning and encryption to establish robust image security and cloud protection, resilient against a spectrum of attacks. The deep learning-based encryption algorithm ensures high security, and coupled with additional measures like two-factor authentication and access control, safeguards images from unauthorized access. Extensive evaluation on benchmark datasets demonstrates the framework's effectiveness, efficiency, and scalability for diverse real-world applications. While the framework presently excels in protecting sensitive images like medical, financial, and government data, its potential extends to securing cloud-stored images in realms such as social media and e-commerce. Future work entails refining the framework, enhancing its capabilities, and addressing evolving threats. The ongoing development aims to position this framework as a transformative force in reshaping the landscape of image security, ensuring a resilient and adaptive solution for safeguarding digital assets in an ever-changing technological landscape.

References

[1] S. El-Naggar and T. Bourlai, "Image Quality Assessment for Effective Ear Recognition," in IEEE Access, vol. 10, pp. 98153-98164, 2022, doi: 10.1109/ACCESS.2022.3206024.

[2] A. Kohlakala and J. Coetzer, "Ear-based biometric authentication through the detection of prominent contours," in SAIEE Africa Research Journal, vol. 112, no. 2, pp. 89-98, June 2021, doi: 10.23919/SAIEE.2021.9432897.

[3] T. Nakamura, V. Goverdovsky and D. P. Mandic, "In-Ear EEG Biometrics for Feasible and Readily Collectable Real-World Person Authentication," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 648-661, March 2018, doi: 10.1109/TIFS.2017.2763124.

[4] Y. Moolla, A. De Kock, G. Mabuza-Hocquet, C. S. Ntshangase, N. Nelufule and P. Khanyile, "Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics," in IEEE Access, vol. 9, pp. 38269-38286, 2021, doi: 10.1109/ACCESS.2021.3062282.

[5] J. Rao and V. Patil, "Visual cryptography for image privacy protection using diverse image media," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 855-859, doi: 10.1109/ICGCIoT.2015.7380582.

[6] D. Mathivadhani and C. Meena, "Biometric based authentication using wavelets and Visual Cryptography," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2011, pp. 291-295, doi: 10.1109/ICRTIT.2011.5972423.

[7] V. K. P. Kalubandi, H. Vaddi, V. Ramineni and A. Loganathan, "A novel image encryption algorithm using AES and visual cryptography," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2016, pp. 808-813, doi: 10.1109/NGCT.2016.7877521. [8] , N b B . “A s b s NA s q .” J M s s 018 : . .

[8] Slimane, Nabil Ben et al. “An efficient nested chaotic image encryption algorithm based on DNA sequence.” International Journal of Modern Physics C (2018): n. pag.

[9] Zhang, Xuncai et al. “An Image Encryption Algorithm Based on Chaotic System Using DNA Sequence Operations.” International Conference on Bio-Inspired Computing: Theories and Applications (2018).

[10] Ahgue, Augustin Ousmanou et al. “A New DNA-Combining Chaos Scheme for Fast and Secure Image Encryption.” International Conference on Security for Information Technology and Communications (2018).