Advanced Deep Learning Framework for Secure Transmission of Sensitive Images in National Security Scenarios

Reg.No	Name of the Student	Branch
BL.SC.P2DSC23007	Deheem u Deyar	Datascience
BL.SC.P2DSC23023	Anirud Ramani	Datascience

Project Advisor:
Dr.Suja P / CSE

Introduction

- Proposal of a deep learning-based framework for secure image transmission in national security contexts
- Emphasis on data integrity and confidentiality, particularly concerning warfare and border security.
- Advanced encoding and decoding techniques employed to protect sensitive image data during transmission.

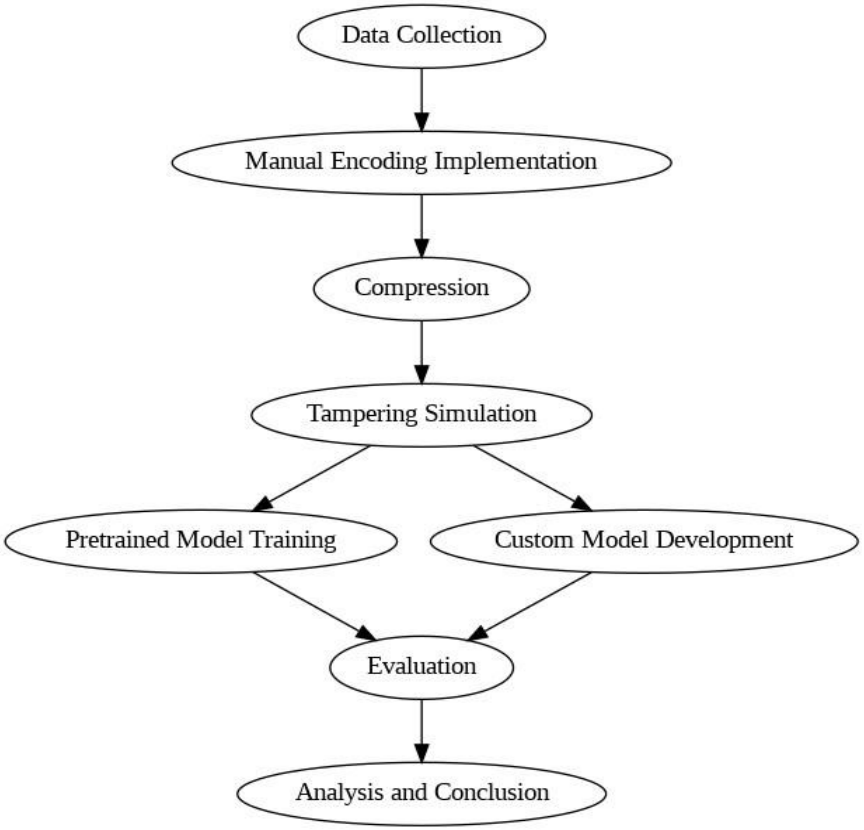
Motivation

- Secure transmission of sensitive data, especially images related to national security like war and border security.
- Traditional encryption methods fall short in addressing modern security threats, requiring more advanced solutions.

Literature Review

- Deep learning-based approaches in diverse fields, like medical imaging and satellite imagery, underscore the importance of securing sensitive data.
- Various encryption schemes utilizing deep learning techniques offer promising avenues for safeguarding image data during transmission and storage.
- Integration of deep learning with traditional cryptographic methods enhances security in image transmission protocols.
- Advancements in deep learning not only improve image classification accuracy but also offer innovative solutions for agricultural and environmental monitoring tasks.

Methodology



Methodology

- **Manual Encoding Implementation**: Utilization of deep learning, specifically the ResNet50 model, for encoding original images with secret codes or messages using LSB modification, ensuring imperceptibility while maintaining integrity.

- **Compression:** Application of compression techniques, including lossy and lossless methods, to reduce file size while preserving the integrity of the encoded information.

Methodology

- **Tampering Simulation:** Simulation of various tampering scenarios, such as Gaussian filtering and blurring, to assess the robustness of encoding and compression techniques against potential attacks.

- **Pretrained Model Training:** Training state-of-the-art deep learning models like ResNet50, Inception_v3, and VGG16 to classify images into tampered and untampered categories using transfer learning.

- **Custom Model Development:** Exploration of architectures such as Attention models, Siamese networks, and Generative Adversarial Networks (GANs) to develop a custom model optimized for detecting tampered images, trained on the same dataset as pretrained models for consistency and comparability.

श्रद्धावान् लभते ज्ञानम्

Summary of Custom Model

Layer (type)	Output Shape	Param #
inception_v3 (Functional)	(None, 5, 5, 2048)	21802784
global_average_pooling2d_15 (GlobalAveragePooling2D)	multiple	0
dense_49 (Dense)	multiple	2049
dense_50 (Dense)	multiple	2049
dense_51 (Dense)	multiple	2049
dense_52 (Dense)	multiple	2049

Total params: 21810980 (83.20 MB)
Trainable params: 21776548 (83.07 MB)
Non-trainable params: 34432 (134.50 KB)

Results And Analysis

Model	Non Encoded Images Accuracy	Encoded Images Accuracy	Encoded Images	
			Lossy Compressed Accuracy	Lossless Compressed Accuracy
ResNet50	86.0%	54.0%	50.0%	50.0%
inception_v3	96.0%	48.0%	51.0%	53.0%
vgg16	100.0%	47.0%	44.0%	51.0%
Custom Model (with Attention Layers)	-	-	60.0%	55.0%

Conclusion

- The study's outcomes underscore the critical role of meticulous model selection and customization, particularly evident in the integration of attention mechanisms for precise image tampering detection.

- The demonstrated effectiveness of varying image manipulations not only advances the sensitive image transmission but also furnishes invaluable insights into the intricate landscape of digital image forensics.

References

- Ding, Yi, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin. "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things." *IEEE Internet of Things Journal* 8, no. 3 (2020): 1504-1518.

- Liu, Y., Zhang, L., & Yang, Q. (2023). Secure Transmission Protocol for Medical Images Using Deep Learning and Cryptography. Journal of Medical Systems, 47(5), 102.

- Chen, S., Wu, H., & Zhou, X. (2023). Hybrid Encryption Approach for Secure Image Transmission Based on Deep Learning and Cryptography. IEEE Access, 11, 75892-75905

- A. Neena and M. Geetha, “Image classification using an ensemble-based deep CNN”, Advances in Intelligent Systems and Computing, vol. 709, pp. 445-456, 2018