ARAB ACADEMY FOR SCIENCE, TECHNOLOGY AND MARITIME TRANSPORT

College of Engineering and Technology

Computer Engineering Department

Deep-Video Steganography Integrating New DeepSteg Paradigms of Machine Learning for Securing Digital Data

By

Sahar Magdy El-Kordy

A thesis submitted to AASTMT in partial

Fulfillment of the requirements for the award of the degree of

PHD'S OF SCIENCE

in

Computer ENGINEERING

Supervisors

Sherin M. Youssef

Computer Department

Engineering

Arab Academy for Science and Technology

Alexandria

Saleh ElShehaby

Computer Department

Engineering

Alexandria University

Alexandria

Karma M. Fathallah

Computer Department

Engineering

Arab Academy for Science and Technology

Alexandria

2024

ACKNOWLEDGMENT

This thesis is the culmination of my journey to PHD degree, which was just like climbing a high peak gradually accompanied with encouragement, hardship, trust, and frustration. When I found myself at top experiencing the feeling of fulfillment, I realized though only my name appears on the cover of this dissertation, a great many people including my family members, well-wishers, my friends, colleagues and various institutions have contributed to accomplish this huge task.

I thank all whom in one way or another contributed in the completion of this thesis. First, I give thanks to GOD for protection and power to finish this work.

I would like to express my sincere gratitude to my advisor Prof. Dr. Sherin Youssef for the continuous support of my thesis study and research, for her patience, motivation, enthusiasm, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my PHD study.

My sincere thanks and deepest gratitude go to my second advisor Dr. Karma Fathallah for her support, help, interest and valuable hints. Her insightful suggestions, comments and encouragement helped me in the time of writing and research of this thesis.

I would also like to express my deepest gratitude to Prof. Dr. Saleh ElShehaby, for their invaluable guidance, support, and encouragement throughout the course of my research. Their expertise and insight have been instrumental in shaping this work. Thank you for being a source of inspiration and for believing in my potential. Last but not least, I would like to extend my heartfelt gratitude to Prof. Dr. Magdy Abd ElAzim, for their unwavering support and guidance throughout the course of my research. Thank you for providing an inspiring environment and for believing in my potential.

Besides my advisors, I would like to thank my Mom for her everlasting support and devotions that encouraged me to pursue my academic career. I'm grateful for her patience, attention and continuous understanding that helped me move forward and chase my dreams no matter how impossible they seem.

I owe thanks to a very special person, my twin and best friend, for showing faith in me and for her selfless love, care and dedicated efforts, which contributed a lot for completion of my thesis. Thanks for always being there for me encouraging me to be better.

I consider myself the luckiest in the world to have such a lovely and caring family, standing beside me with their love and unconditional support.

ABSTRACT

In today's world, securing digital data and ensuring its confidentiality is crucial. the exponential increase in data transmission over the internet necessitates robust methods for ensuring data security and confidentiality.

Military organizations are extensively employing steganography techniques, similar to intelligence services, to conceal their communication. Unauthorized leaking of classified information can have severe implications for national security. The medical industry has also gained advantages from the utilization of steganography. The World Health Organization (WHO) predicts a shortage of healthcare experts by 2030. Consequently, digitized medical records are now vulnerable to security breaches, making them a much more profitable target for criminals compared to financial data. According to the U.S. Department of Health and Human Services, there were 11 significant health data breaches affecting over 70.3 million individuals in the year 2023.

To address these challenges, there is a need for a method that can securely conceal data within a digital medium in such a way that the existence of the hidden data remains undetectable to external adversaries. Video steganography serves a critical role in this purpose, as it provides higher embedding capacity compared to images. Also, the complex structure of video files are designed to be robust against various attacks and distortions which adds an extra layer of security.

In this study, a cascaded deep video steganography framework is proposed, integrating Crypto-Steganography and deep video detection and tracking, where data is embedded at numerous tracked objects so the secret data location will be different from frame to frame ensuring the security of the data. The proposed model comprises three phases, detection of multi-objects, tracking the detected objects and using steganography to embed the data into the tracked objects.

The detection phase is critical for successful tracking. It lays the foundation by identifying the target, allowing subsequent tracking algorithms to monitor its motion over time. A new methodology is proposed integrating the advantages of both LiDAR 3D points and Camera sensors suppressing their disadvantages in detecting multi objects. Deep learning Aggregation (DLA-34) with its hourglass shape is used to extract then a parallel network of the Pyramid Split Attention (PSA) PSA model is employed to fuse the features before passing through the Feature Pyramid Network (FPN) for detecting multi objects.

The detected objects are transferred to a novel tracking phase named E_SS architecture. To ensure the efficiency of the tracking module, an improved efficientNetV2 architecture named DAR_EfficientNetV2 was based on DARNet Attention module. Finally, the tracked objects are cropped from the frame, where the steganography technique which is based on Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) is employed to embed the secret data whether it is images or text using Particle Swarm Optimization (PSO).

The detection phase achieved an improvement of 3% in detected vehicles and trucks in the Nuscenes dataset, while motorcycle object detection improved by 9.5% in terms of mAP. Moreover, the E_SS tracking technique achieved an improvement rate of 2.1%.in tracking cars in KITTI Dataset. Additionally, E_SS achieved an improvement rate of 7% than previous state-of-arts. Furthermore, the deep Steganography technique was evaluated on multiple dataset ensuring its imperceptibility, high hiding capacity and robustness against noise. Average PSNR of 73.57 was achieved along with average PSNR of 70.84 achieved under noise attack.