A

SEMINAR REPORT

ON

Cryptographic Applications of Artificial Neural Networks (Steganography)

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

BACHELOR OF ENGINEERING
INFORMATION TECHNOLOGY

BY

Nachiket Jadhav
Roll No: 33134
Exam Seat No:

Under the guidance of
Ms. Deepali Salapurkar

DEPARTMENT OF INFORMATION TECHNOLOGY
PUNE INSTITUTE OF COMPUTER TECHNOLOGY
SR. NO 27, PUNE-SATARA ROAD, DHANKAWADI
PUNE - 411 043.
AY: 2023-2024

SCTR's PUNE INSTITUTE OF COMPUTER TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

CERTIFICATE

This is to certify that the Seminar work entitled
Cryptographic Applications of Artificial Neural Networks

Submitted by

Name : Nachiket Jadhav
Exam Seat No: .

is a bonafide work carried out under the supervision of Ms. Deepali Salapurkar and it is submitted towards the partial fulfillment of the requirements of Savitribai Phule Pune University, Pune for the award of the degree of Bachelor of Engineering (Information Technology).

Ms. Deepali Salapurkar
Seminar Guide

Dr. A. S. Ghotkar
HOD IT

Dr. S. T. Gandhe
Principal

Date:
Place:

Acknowledgement

I am highly obliged to the people who have given me the much-needed guidance for the work under seminar. First, I would like to convey a word of gratitude to my guide, Ms. Deepali Salapurkar for guiding us throughout project work and providing me excellent support by valuable guidance and by providing sufficient time for completion of my work. Without their immense help it would have been really difficult to complete this work in time.

I am also extremely grateful to Dr. A. S. Ghotkar, Head of the Department for providing all facilities and every help for smooth progress of project work. I am really thankful to the entire staff, my friend and my parents for their kind support and necessary help provided by them on time.

Name : Nachiket Jadhav

Roll No: 33134

Abstract

Delving into the fusion of cryptography and artificial neural networks (ANNs), this topic details the various possibilities for their integration in areas like encryption, cryptanalysis, steganography and beyond. By leveraging ANN's aptitude for pattern recognition and learning, novel encryption methods can be developed, whereas multimedia files can safeguard hidden information. Besides, these neural networks boast the ability to enable privacy-preserving computations on encrypted data, recover encryption keys, and crack ciphers. Additionally, they ramp up biometric security levels, elevate true random number generation, and bolster the efforts against intrusion detection and malware classification. For robust information protection, ANNs provide a promising opportunity in the evolving landscape of cryptographic applications. Thorough analysis and testing is essential for securing neural network-based cryptographic solutions.

Keywords: Cryptography, Artificial Neural Networks, Steganography, encryption and decryption.

Contents

List of Figures

List of Tables

Abbreviations

ANN : Artificial Neural Networks

1. Introduction

1.1 Introduction

In the age of digital information exchange, data protection has become an important issue. The combination of cryptography and neural networks provides an effective solution to this challenge. The conference ”Encryption Applications of Artificial Neural Networks” explores this encryption technology in depth and reveals its revolutionary potential in secure communications and data protection.

Cryptography, the science of encoding and decoding messages, has long been the foundation of digital security. Artificial neural networks inspired by the human brain are an important part of artificial intelligence, enabling machines to learn and adapt. This workshop explores how these two functions can be combined to create a powerful partnership.

This merger has revolutionized our understanding of data protection, from protecting sensitive financial transactions to protecting confidential communications.

As we embark on this journey, you will gain insight into new and evolving areas of secure data exchange.

1.2 Motivation

There are several important points behind motivation before choosing a topic for this seminar:

Importance: In our digital age, it is important to protect important information due to the threat of cyber attacks and data breaches.

Cutting Edge Fusion: The intersection of cryptography and vulnerable electronics presents an exciting competition between the two technologies, making it important for research.

Professional Development: Studying this topic has allowed me to expand my knowledge of cybersecurity and artificial intelligence, which are sought after in today's business world.

Innovation Potential: This conference provides a platform for us to find new solutions that can revolutionize the way we protect data across businesses.

Education and professional development: It meets the need for knowledge collaboration and puts me at the forefront of areas shaping the future of technology and security.

1.3 Objectives

To leverage artificial neural networks (ANNs) for the development of a robust and secure cryptographic application that enhances data privacy and confidentiality through advanced encryption and decryption techniques

1.4 Scope

The seminar on ”Cryptographic Applications of Artificial Neural Networks” offers a broad scope that encompasses:

Foundational Knowledge: Understanding the basics of cryptography and neural networks.

Integration: Exploring how these fields merge for enhanced security.

Cryptographic Protocols: Examining their role in encryption, secure key exchange, and digital signatures.

Real-World Applications: Securing online transactions, healthcare data, IoT devices, and more.

Emerging Trends: Covering areas like homomorphic encryption, post-quantum cryptography, and blockchain.

Security Challenges: Addressing issues like adversarial attacks and system robustness.

Interdisciplinary Insights: Encouraging diverse participation for cross-disciplinary discussions.

Future Implications: Considering the long-term impact on data security and privacy.

Research and Innovation: Providing a platform for creative solutions and projects in this evolving field.

2. Literature Survey

Table 2.1: Literature Survey.

S.no	Title	Author	Publication year	Seed Idea
1	Quantum Image Steganography Schemes for Data Hiding.	Nasro Min-Allah,Naya Nagy,Malak Aljabri,Mariam Alkharraa, Mashael Alqahtani,Dana Alghamdi,Razan Sabri and Rana Alshaikh	Jan-2022	Leveraging quantum computing for image steganography to enhance data hiding and security.
2	A review Paper on Cryptography	Abdalbasit Qadir, Nurhayat Varol	Jul-2019	Utilizing advanced cryptographic techniques to safeguard digital information and protect privacy in the digital age.
3	CRYPTOGRAPHY BASED ON NEURAL NETWORK	Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek	Jan-2021	Harnessing neural networks to enhance the security and efficiency of cryptographic systems in a rapidly evolving digital landscape.
4	Neural Networks Based Cryptography	Ishak Meraouche, Sabyasachi Dutta, Haowen Tan, and Kouichi Sakurai	2020	Forging unbreakable data fortresses: The avant-garde synergy of neural networks and cryptography.
5	Implementation and Analysis of Image Steganography using Aritifcial Neural Networks	M K Linga Murthy, P Bindu Madhavi, S Asif Ahamad, K Vamsi, Y Mallikarjuna Rao	Nov-2022	Unlocking hidden realms: Innovating data concealment with Artificial Neural Networks in steganography.

3. Methodologies

3.1 Model Architecture

Steganography is the technique of hiding secret data in ordinary data by modifying pixel values that appear normal to a casual observer. Steganography, which is similar to cryptography, helps in secret communication. A cryptography method focuses on the authenticity and integrity of messages by hiding the contents of messages. Sometimes it is not enough to just encrypt the message, but it is also necessary to hide the existence of the message itself. Because it prevents misuse of data, this type of encryption is less suspicious and does not attract attention.

Unlike cryptography, which aims to make a message unreadable, steganography aims to conceal the existence of the message itself.

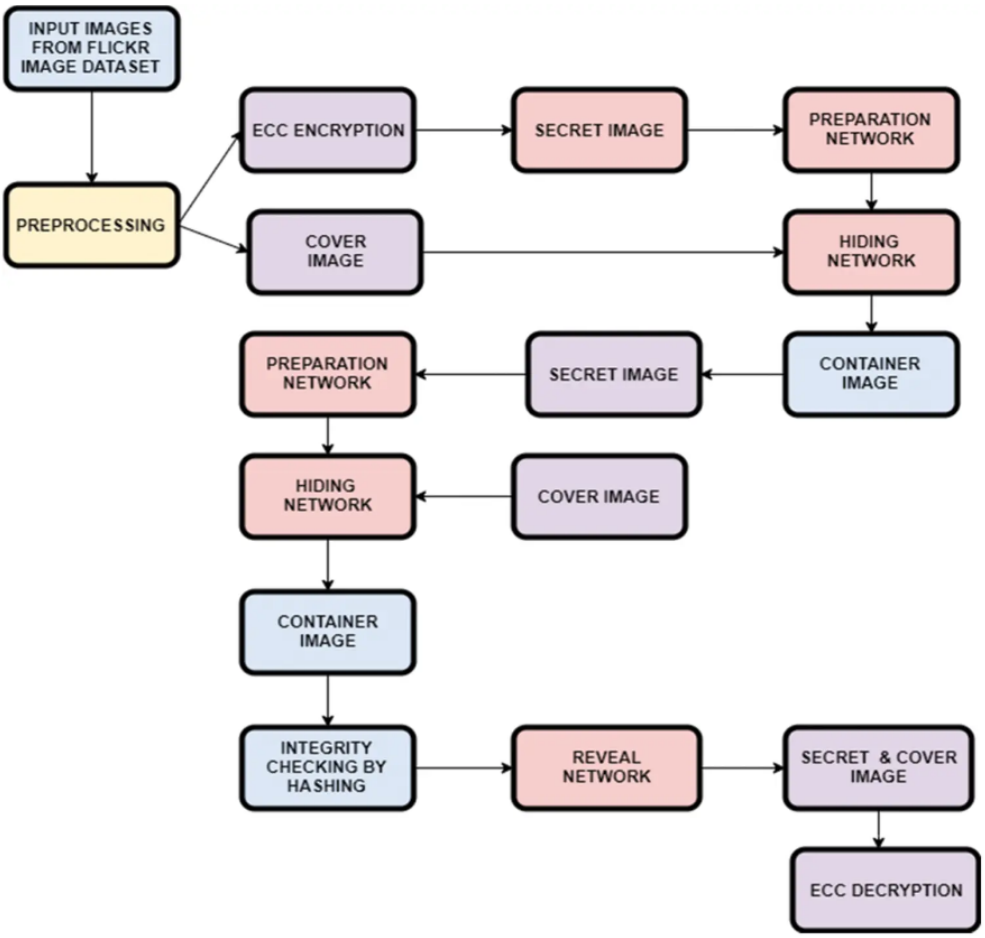

Figure 3.1: Flow chart depicting encryption in Steganography

The input images are preprocessed, resizing and normalizing the Cover and Secret images. Encrypting the secret text by the user is done and then the text is converted into an image which is considered to be the secret image. On the sender side, the Cover and Secret images are

provided as input to the Stacked Autoencoder model, which outputs the container image. The sender then sends this container image to the recipient. The receiver extracts the secret image from the container image and the text is decrypted. The concept of hashing is incorporated to check file integrity. It is used to verify that the container image sent by the sender is the same as the one received by the recipient.

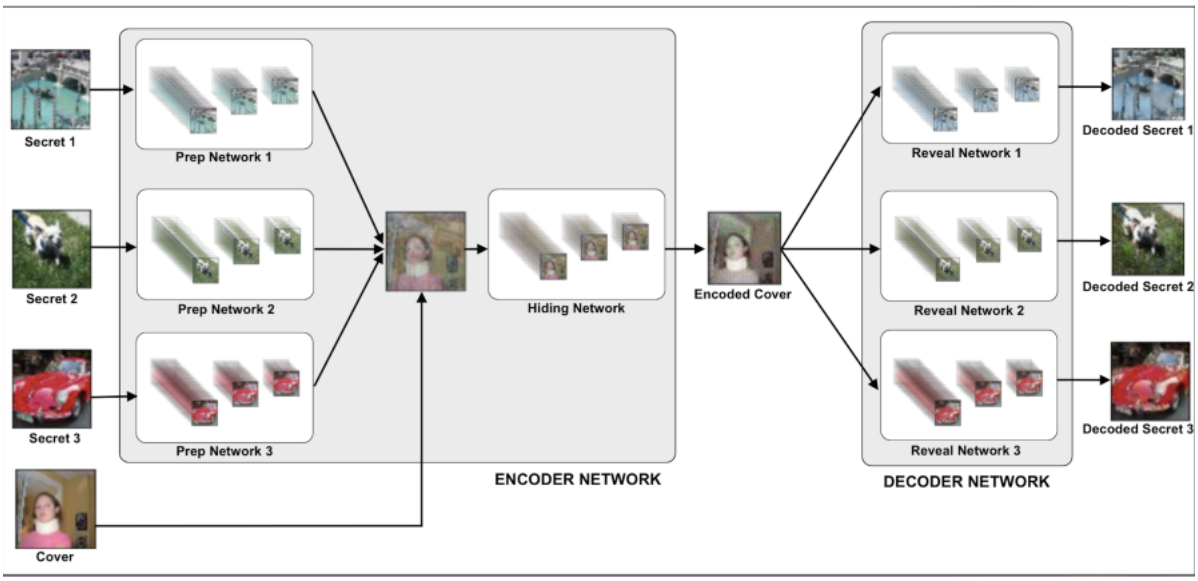

Figure 3.2: Model Architecture

3.2 Autoencoder

An autoencoder is a type of artificial neural network that is used for unsupervised learning to encode data. The goal of an autoencoder is to train the network to capture the most significant bits of the input image in order to learn a lower dimensional representation (encoding) for the higher dimensional data, often for dimensionality reduction. Using a neural network to reproduce an input may seem straightforward, but the size of the input is reduced during the replication process, resulting in a smaller representation. Because an autoencoder copies data from an input to an output without supervision, it is also known as a replicator neural network. Autoencoders consist of the following three parts:

Encoder: A module that compresses input data into an encoded form.

Bottleneck: The most important element of a network because it contains compressed representations of knowledge.

Decoder: A module that helps the network decompress the knowledge representations and reassemble the data from its encoded state. The output is then compared to the original data.

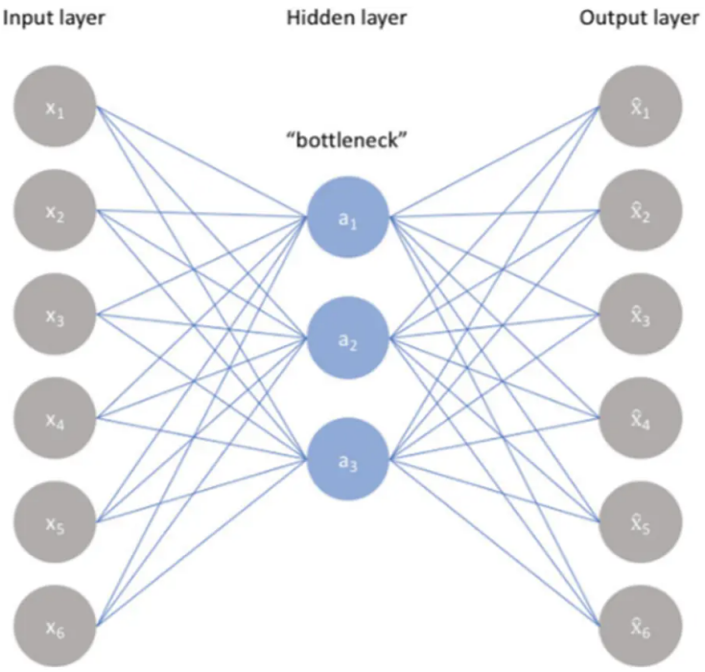

Figure 3.3: Basic Architecture of Auto Encoder

3.3 Discussion

Here we describe the method of training the model. At first it looks like a standard coder and decoder model. However, training works this way: First, we train the encoder and leave the decoder parameters as untrainable. This helps the coder to learn and create the encoded hidden image. This model is evaluated using the loss for all the revealed images as well as the hidden image.

After getting the output from the encoder, we train the decoder (consisting of three detection networks). This decoder is evaluated based on detection loss only.

Now the parameters of the deocer networks are shared with the detection networks while the encoder is being trained.

This ideally helps the network to learn much better, as the encoder and decoder network becomes smaller and the task is much more focused on optimization instead of training the entire model together.

4. Implementation

4.1 Dataset and Parameters

The dataset used in this paper is the Tiny ImageNet dataset. This dataset also contains some The gray image was removed by running the create dataset.py script. this Scripts are used to generate training and validation datasets. Sample 10 images of each Four images for training and testing from 200 classes from the ImageNet Small dataset. Overall, There are 2000 training images and 800 test images.

Here are the parameters which we have used for training the networks are:

- Image Size
- Learning Rate
- Cover Loss Weight
- Secret Loss Weight
- Size of the training batch
- Size of the valid batch
- Decoder Loss Weight

4.2 Algorithm

Algorithm for Multi-Image Steganography Using Artificial Neural Networks (ANN):

Data Preparation:

Prepare a collection of multiple cover images. Encode the secret data you want to hide in a suitable format (e.g., binary data). Split the secret data into chunks based on the number of cover images.

Training Neural Networks

Design and train neural networks that are capable of hiding and extracting data from images. This typically involves two networks, one for hiding (encoding) and one for extracting (decoding) data. Training data: Use pairs of cover images and corresponding secret data chunks for training. The networks should learn to embed the data into images in a manner that is not easily detectable.

Embedding data:

For each cover image and corresponding secret data chunk: Apply the encoding neural network to embed the data into the cover image. Repeat this process for all cover images.

Data Extraction:

To extract the hidden data from the multi-image steganography: Use the decoding neural network to extract the data from each cover image. Reassemble the extracted data chunks to reconstruct the original secret data.

Verification:

Verify the integrity and correctness of the extracted data. Error-checking or error-correction codes may be used to ensure data integrity.

Testing and Evaaluation:

Assess the quality of the steganography algorithm by testing it on various cover images and secret data types. Evaluate the algorithm's performance in terms of data capacity, imperceptibility, and robustness against detection.

Security Measures:

Consider incorporating encryption of the secret data before embedding it to enhance security.

Optimization and fine tuning:

Continuously optimize and fine-tune the neural networks and the steganography process to improve efficiency and security.

Deployment:

Implement the algorithm for practical use, ensuring that it meets the security and quality requirements for real-world applications.

4.3 Software Requirement Specification

- Python 3

- Pandas
- Jupyter Notebook
- Torch library
- Numpy
- Matplotlib
- Flask

4.3.1 Platform for Implementation and its Specifications

Operating System: Windows 7 and above, Mac, Linux

Processor: i3 or Ryzen 3 and above

4.4 Result

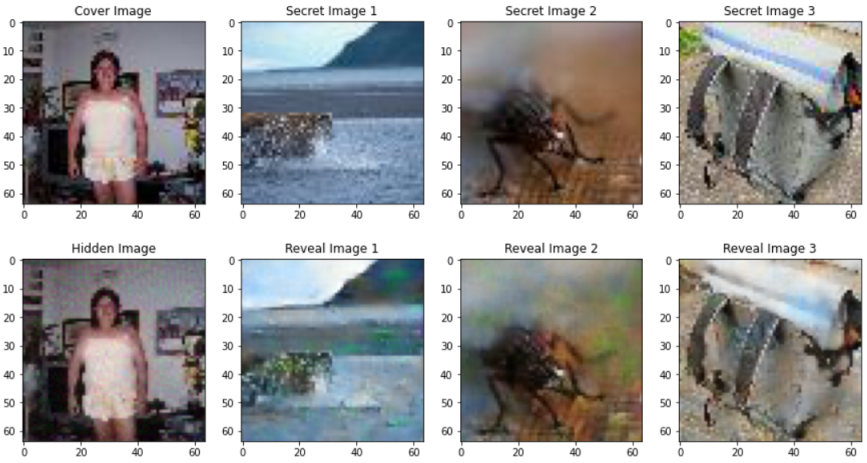

Figure 4.1: Result 1

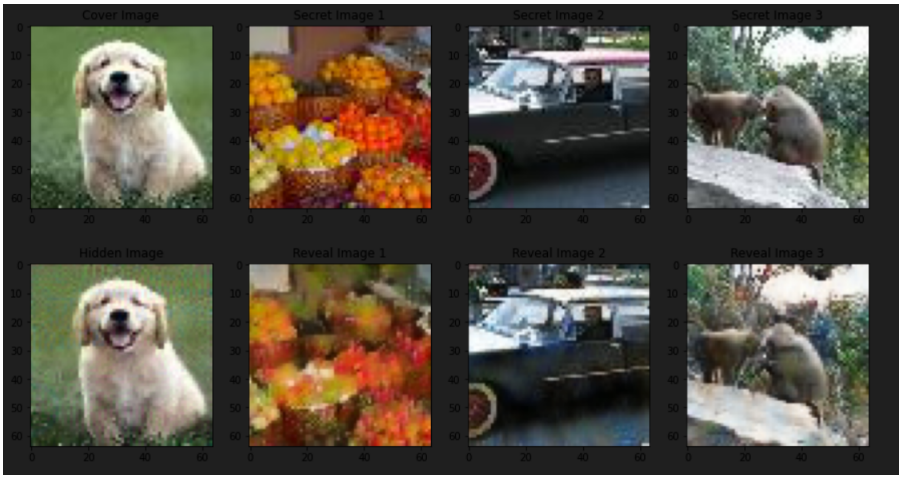

Figure 4.2: Result 2

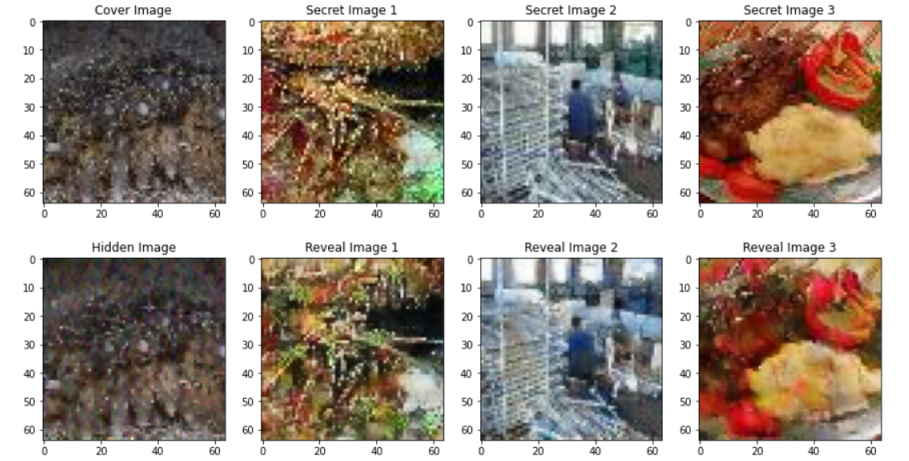

Figure 4.3: Result 3

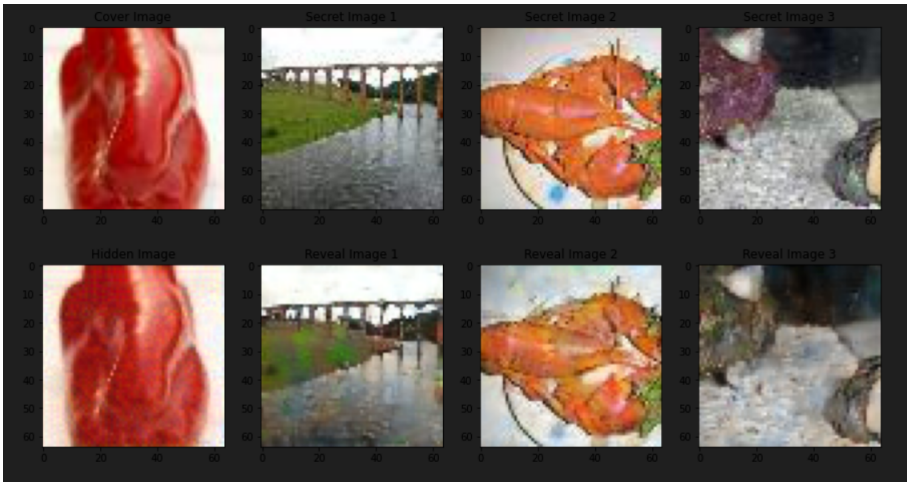

Figure 4.4: Result 4

5. Applications

5.1 Applications

- Copyright Protection
- Digital Forensics
- Secure Communication
- Military and Defense
- Whistleblower Protection
- Journalism and Activism
- Data Protection
- Academia and Research
- Art Authentication
- Cybersecurity
- Privacy Protection
- Entertainment and Gaming

5.2 Challenges

Security vs. Detection: As ANN-based steganographic techniques become more advanced, countermeasures to detect hidden data are also being developed. This creates an ongoing game of cat and mouse, making it challenging to ensure long-term data security.

Security vs. Detection: Achieving a balance between high data hiding capacity and robustness (the ability to withstand signal processing and compression) is a difficult challenge. Increasing payload capacity often leads to increased detectability.

Training Data: The effectiveness of ANN-based steganography often depends on access to diverse and representative training data. Collecting and maintaining a comprehensive dataset for training can be a time- and resource-intensive task.

Adversarial Attacks: As in other AI applications, ANN-based steganography is vulnerable to adversarial attacks. Attackers may attempt to manipulate the steganography process to reveal hidden data or render the steganography method ineffective.

Computational and Resource Intensity: Training and implementing ANN models for steganography can be computationally expensive, which may limit their real-time applicability in some scenarios.

Ethical and Legal Concerns: The use of ANN-based steganography raises ethical concerns in terms of privacy and security. It can be used for both legitimate and malicious purposes, posing legal and ethical dilemmas.

...

6. Conclusion and Future Scope

In conclusion, the integration of Artificial Neural Networks (ANN) with steganography has shown great promise in increasing the security and efficiency of data hiding techniques. ANN-based steganography methods have demonstrated their ability to embed information in multimedia files with reduced detectability, thereby increasing the secrecy of sensitive data. The use of ANNs enables adaptive and intelligent embedding and improves the overall robustness of steganographic algorithms.

Looking to the future, the scope for ANNs in steganography remains clear. As neural network technologies continue to advance, we can expect even more sophisticated and robust steganographic methods. ANN-driven steganography has potential in various applications such as cyber security, digital forensics, and secure communication. Additionally, the integration of ANNs with emerging technologies such as deep learning and reinforcement can further expand the horizons of data hiding techniques. It is imperative to continue research in this area and explore innovative ways to harness the power of artificial intelligence to better hide and protect data in an increasingly digital world.

Bibliography

[1] Quantum Image Steganography Schemes for Data Hiding: A Survey by Nasro Min-Allah,Naya Nagy,Malak Aljabri,Mariam Alkharraa, Mashael Alqahtani,Dana Alghamdi,Razan Sabri and Rana Alshaikh, Jan- 2022

[2] Neural Networks Based Cryptography: A Survey by ISHAK MERAOUCHE, SABYASACHI DUTTA, HAOWEN TAN, and Kouichi SAKURAI, 2020

[3] CRYPTOGRAPHY BASED ON NEURAL NETWORK by Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, Jul-2021.

[4] A review Paper on Cryptography, Abdalbasit Qadir, Nurhayat Varol,June 2019.

[5] Implementation and Analysis of Image Steganography using Aritifcial Neural Net- works M K Linga Murthy, P Bindu Madhavi, S Asif Ahamad, K Vamsi, Y Mallikarjuna Rao Nov-2022

Savitribai Phule Pune University, Pune
Third Year Information Technology (2019 Course)
314449 : Seminar

Teaching Scheme:	Credit Scheme:	Examination Scheme:
Practical (PR) : 01 hrs/week	01 Credits	TW : 50 Marks

HOME

Prerequisites:

1. Project Based Learning
2. Software Engineering

Course Objectives:

Seminar should make the student attain skills like:

1. To gather the literature of specific area in a focused manner.
2. To summarize the literature to find state-of-the-art in proposed area.
3. To identify scope for future work.
4. To present the case for the intended work to be done as project.
5. To report literature review and proposed work in scientific way.

Course Outcomes:

On completion of the course, students will be able to–

CO1: Understand, interpret and summarize technical literature.

CO2: Demonstrate the techniques used in the paper.

CO3: Distinguish the various techniques required to accomplish the task. CO4: Identify intended future work based on the technical review.

CO5: Prepare and present the content through various presentation tools and techniques in effective manner.

CO6: Keep audience engaged through improved interpersonal skills.

Guidelines for Seminar Selection and Presentation

1) Student shall identify the area or topics in Information Technology referring to recent trends and developments in consultation with industry (for their requirement) and institute guide.
2) Student must review sufficient literature (reference books, journal articles, conference papers, white papers, magazines, web resources etc.) in relevant area on their topic as decided.
3) Seminar topics should be based on recent trends and developments. Guide should approve the topic by thoughtfully observing different techniques, comparative analysis of the earlier algorithms used or specific tools used by various researchers in the domain.
4) Research articles could be referred from IEEE, ACM, Science direct, Springer, Elsevier, IETE,CSI orfrom freely available digital libraries like Digital Library of India (dli.ernet.in), National Science Digital Library, JRD Tata Memorial Library, citeseerx.ist.psu.edu, getcited.org, arizona.openrepository.com, Open J-Gate, Research Gate, worldwidescience.org etc.
5) Student shall present the study as individual seminars in 20 – 25 minutes in English which is followed by Question Answer session.
6) Guide should ensure that students are doing literature survey and review in proper manner.
7) Guide should give appropriate instructions for effective presentation.
8) Attendance of all other students in the class for presentation is mandatory.

Timeline is suggested to follow throughout the semester:

1) **Week– 01:** Discussion to understand what is technical paper, how to search, where to search?
2) **Week– 02:** Download technical papers (minimum four), getting approved from Guide and Prepare abstract summary of all papers downloaded.
3) **Week– 03 & 04:** Read and understand in detail the decided research papers about the problem statement, techniques used, experimental details and results with conclusion from identified papers.
4) **Week– 05:** Review of the studied papers by Guide / Panel.
5) **Week – 06 & 07:** Search / Find equivalent techniques (other than the one proposed in technical paper) so performance / complexities can be improved (by amortized analysis, not actual implementation).
6) **Week – 08 & 09:** Prepare presentation with outline as The topic, its significance, The research problem, Studied solutions (through research papers) with strengths and weaknesses of each solution, comparison of the solutions to research problem, future directions of work, probable problem statement of project, tentative plan of project work
7) **Week – 10:** Write Seminar report.
8) **Week – 11:** Deliver Presentation to Guide/ Panel.
9) **Week –12:** Verification of Seminar report and Submission.

Guidelines for Seminar report

1. Each student shall submit two copies of the seminar report in appropriate text editing tool/software as per prescribed format duly signed by the guide and Head of the department/Principal.
2. Broad contents of review report (20-25 pages) shall be
   - **a)** Title Page with Title of the topic, Name of the candidate with Exam Seat Number / Roll Number, Name of the Guide, Name of the Department, Institution, Year & University.
   - **b)** Seminar Approval Sheet/Certificate.
   - **c)** Abstract and Keywords.
   - **d)** Acknowledgments.
   - **e)** Table of Contents, List of Figures, List of Tables and Nomenclature.
   - **f)** Chapters need to cover topic of discussion-
     - **i.** Introduction with section including organization of the report,
     - **ii.** Literature Survey
     - **iii.** Motivation, purpose and scope and objective of seminar
     - **iv.** Details of design/technology/Analytical and/or experimental work, if any/
     - **v.** Discussions and Conclusions,
     - **vi.** Bibliography/References (in IEEE Format),
     - **vii.** Plagiarism Check report,
3. Students are expected to use open source tools for writing seminar report, citing the references and plagiarism detection.

Guidelines for Lab /TW Assessment:

1. A panel of reviewers constituted by seminar coordinator (where guide is one of the member of the panel) will assess the seminar during the presentation.
2. Student's attendance for all seminars is advisable.
3. Rubric for evaluation of seminar activity:
   - **i.** Relevance of topic - 05 Marks
   - **ii.** Relevance + depth of literature reviewed - 10 Marks
   - **iii.** Seminar report (Technical Content) - 10 Marks
   - **iv.** Seminar report (Language) - 05 Marks
   - **v.** Presentation Slides - 05 Marks
   - **vi.** Presentation & Communication Skills - 05 Marks
   - **vii.** Question and Answers - 10 Marks

   TOTAL: **50 Marks**

Reference Book:

1. Andrea J. Rutherfoord, Basic Communication Skills for Technology, Pearson Education Asia, 2ndEdition.
2. Lesikar, Lesikar's Basic Business Communication, Tata McGraw, ISBN: 256083274, 1st Edition.

Text Book :

1.Sharon J. Gerson, Steven M. Gerson, Technical Writing: Process and Product, Pearson Education Asia, ISBN: 130981745, 4thEdition.