AJPMHS GLOBAL RESEARCH NETWORK

AMERICAN Journal of Pediatric Medicine and Health Sciences
Volume 02, Issue 7, 2024 ISSN (E): 2993-2149

COMBINING STEGANOGRAPHY WITH DATA OBFUSCATION: A STUDY ON ADVANCED SECURITY MEASURES FOR CONFIDENTIAL DATA TRANSMISSION

Manu Dev Chhiller
Department of Computer Science Engineering,
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

Vatsalya Pandey
Department of Computer Science Engineering,
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

Jaydeep Patel
Department of Computer Science Engineering,
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

R. Regin
Assistant Professor, Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram, India.

S. Suman Rajest
Professor, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.

Abstract: Steganography, derived from the Greek term meaning "covered writing," is the art and science of concealing hidden messages within seemingly innocuous communications, ensuring that only the sender and the intended recipient are aware of the message's existence. This method provides security through obscurity, differentiating itself from other data-hiding techniques by embedding a secret message within an existing channel of communication. Unlike covert channel techniques that establish a new connection between previously unconnected entities, steganography aims to conceal messages within "harmless" communications, making it undetectable to any potential eavesdroppers or adversaries. The crux of steganography lies in the secret key—a short, easily exchangeable random number sequence. Without this key, an adversary would not even suspect the presence of hidden communication within the observed channel. This technique is particularly relevant in scenarios where encrypted communication is not permitted, such as in certain corporate environments or under specific government regulations. Steganography also intersects with the issue of "hidden channels" in secure operating system design, which involves communication paths that are difficult for access control mechanisms to restrict. In these contexts, steganography provides a viable alternative, allowing covert communication without raising suspicion or violating policies against encrypted messages.

Keywords: Steganography; Health Transmission, Least Significant Bit; Images, Audio, Video; Python; FPGAs and GPUs ;Pillow; Stegano; Opencv

1. Introduction

Steganography involves hiding information to keep it secret from unauthorized individuals, and it has a long history of use dating back to ancient times [1]. With the rise of digital communication, steganography has become more popular, with many applications in watermarking and secret communication. This project will focus on steganography using Python, specifically hiding messages in image files [2-6]. We'll cover different steganography algorithms, their limitations and risks, and strategies for detecting and preventing steganographic attacks. By the end of the project, you'll have a solid grasp of steganography and practical experience using it for secure communication and data protection. Steganography works by embedding secret data within an innocuous-looking cover file, such as an image, audio, or video file [7-15]. The goal is to hide the existence of the secret data so that it cannot be detected by anyone who is not authorized to see it.

In digital steganography, a cover file is used as a carrier for the secret message. The process of hiding data within the cover file involves modifying some of the bits of the cover file in a way that does not significantly alter its appearance or quality [16-22]. This can be done by exploiting the redundancy or noise tolerance of the cover file. Various steganography algorithms can embed secret data into the cover file, such as the least significant bit (LSB) and frequency domain methods. The LSB method replaces the least significant bit of each pixel in an image with a bit from the secret message [23-27]. This method is often used for simple steganography tasks because it is easy to implement and does not require advanced knowledge of image processing. On the other hand, the frequency domain method involves manipulating the cover file's frequency components to embed the secret message. This method can be more complex to implement but more secure because it is less susceptible to visual detection [28-32].

Problem statement

Steganography conceals the existence of a message, ensuring that, if done correctly, it attracts no suspicion. This technique can hide information within various carriers such as images, audio files, text files, videos, and data transmissions. In this study, we propose a new framework for an image steganography system designed to embed the digital text of a secret message within an image. Our approach involves utilizing 7 bits from each pixel in an image to map to the 26 alphabetic English characters (a to z) and some special characters commonly used in secret messages. The primary objective of this method is to hide the text within the image's pixels in such a way that the human visual system cannot detect any difference between the original image and the stego-image. However, a specialized reading machine can easily decode the hidden message. This technique aims to ensure the seamless concealment of information while maintaining the integrity and appearance of the original image [33-36].

Aim of the Project

The aim of a project on steganography could vary depending on the project's specific focus. However, some possible aims could include: Developing an understanding of steganography techniques: A project could aim to explore various steganography techniques, their strengths, and their limitations. This could involve research and analysis of existing steganography algorithms and approaches. Implementing a steganography algorithm: The project could aim to implement a steganography algorithm using a specific programming language. This would involve understanding the algorithm and the technicalities involved in its implementation [37-41]. Evaluating steganography algorithms: A project could aim to compare and evaluate different steganography algorithms to determine their efficiency, effectiveness, and robustness. This could involve developing a testing framework and analyzing the results.

Project Domain

Steganography is a fascinating field with many practical digital security and privacy applications. A steganography project could explore techniques to hide information in digital media, such as images, audio, or videos. The project could focus on developing new steganography algorithms or evaluating the effectiveness of existing ones. One possible domain for a steganography project is information security. In this domain, steganography can protect confidential information, such as trade secrets or personal data, from unauthorized access or interception. Another possible domain is digital forensics, where steganography can be used to hide information to evade detection by forensic investigators. Steganography has a long history of use in military and intelligence operations, making it another potential domain for a project. In this context, steganography can hide secret messages in plain sight, making them difficult for the enemy to detect [42-51].

Scope of the Project

Steganography is a technique for hiding information within digital media, such as images, audio, or video. Its scope is to conceal hidden information while still allowing it to be transmitted or stored seemingly innocently. The scope of steganography includes a wide range of applications, such as secure communication, digital watermarking, and covert data storage. For example, it can transmit secret messages or information without arousing suspicion, as the message is embedded in seemingly ordinary cover media. Digital watermarking uses steganography to embed information, such as ownership details, into digital media to establish its authenticity and protect it from unauthorized use. Additionally, steganography can be used to hide sensitive information on a computer or other digital device, helping to protect it from being discovered by unauthorized users. Steganography has also been used in some historical and modern espionage cases, where the goal was to hide secret information from detection by adversaries. Overall, the scope of steganography is quite broad, and it has a wide range of practical applications in fields such as cryptography, digital forensics, information security, and others.

Methodology

The methodology for a steganography project will depend on the project's specific objectives. However, here are some possible steps that could be followed in a steganography project:

Research and study: Conduct thorough research on steganography techniques and algorithms, their strengths, limitations, and real-world applications. Gather and analyze relevant literature and resources related to the project.
Identify the problem: Clearly define the problem or objective of the project. Determine what information must be hidden and which type of digital media.

Select the steganography technique: Choose an appropriate technique that suits the project's requirements, such as image or audio steganography.

Develop the algorithm: Develop or adapt a steganography algorithm that meets the project's objectives. This involves understanding the technicalities of implementing the chosen technique and creating a working algorithm to embed and extract hidden information.

Implementation: Implement the steganography algorithm using a suitable programming language and test it with various digital media.

Evaluation: Evaluate the effectiveness of the steganography technique by analyzing its robustness, efficiency, and resistance to attacks. Determine the capacity of the media to hide information and the distortion introduced by the hidden information.

Optimization and improvement: Optimize and improve the steganography algorithm to enhance efficiency, robustness, and security.

Results and conclusions: Analyze and report the project's results, including the effectiveness of the steganography technique and any limitations or areas for improvement. Conclude and recommend future research or development.

Literature Review

S.No	Title	Author	Methodology	Technical Gap
1.	Appealing Side of News Consumption [52]	Pallavi Dewan & Payel Das	The paper explores the dynamics of media convergence between legacy media and new media industries, examining the transformations they have undergone to adapt to changing times. Additionally, it assesses the evolving user reading patterns in response to these shifts.	Needs fast internet speed
2.	A concept on IOS NewsApp [53]	Thurman	A site that "aggregates news and enables users to personalize their news stream based on their interests," and The New York Times-backed News me, which	Paid application

			"uses artificial intelligence to…learn what people like to read and provides articles and links of interest".	
3.	Android News App [54]	Brijesh Joshi & Nehal Patel	This paper utilized an API to aggregate various news sources into one centralized location. Upon sending a request, the API responds with data in JSON format, including the source ID, title, description, and image.	Native news apps can be costly and challenging to maintain due to the need for regular updates, compatibility across different operating systems, and the requirement for specialized development skills.
4.	Mobile news reading interactions for news app personalization [55]	Marios Constantinides, John Dowell, David Johnson, Sylvain Malacria	In this paper, the algorithm should first survey users' news reading preferences and behaviors; analysis revealed three primary types of readers.	Paid Services
6.	Andriod-based News Application [56]	Financial Times	This stage involves defining the app's purpose, the target audience and features, what kind of news they are interested in, and their reading habits	Scifferes
7.	A Study on Centralized News Application Using API call [57]	University of New York Graduate School of Journalism	Define who the user is and how they will interact with the application. This will provide insights into the user's needs and desires and establish how they will take the information they need at each step.	Jeff Jarvis
8.	Growth of News Application [58]	Mark Aiello	Developing and fielding news application technology will increasingly depend on the federal government's support in developing national regulations.	It will be a long time before there is a critical mass of infrastructure capabilities and a percentage of capable applications to make this a viable solution with broad acceptance.
9.	Open Interactive News Application [59]	J.A.Unar	presents a work-in-progress project for developing an open interactive algorithm visualization website.	Limited functionality

10.	Android Application [60]	Ricanek, Karl and Boehnen, Chris	News Shaft and News Platform for News generation" focuses on "visualization", which allows a better understanding of its flow and operation.	Lack of personalization

Existing System

Several existing steganography systems that use various techniques to embed hidden information in digital media are available. Here are a few examples: OpenStego: This open-source steganography software supports image and audio steganography. It uses various algorithms, including LSB (Least Significant Bit) and DCT (Discrete Cosine Transform), to hide data in digital media. Steghide: This open-source steganography software supports multiple file formats, including images and audio files. It uses various algorithms, such as LSB, to hide data in digital media. Outguess: This popular steganography software uses a patented algorithm to hide information in images. It supports JPEG, BMP, and GIF image formats and can embed hidden information in the image's color palette. F5: This steganography algorithm uses a combination of Least Significant Bit (LSB) and matrix encoding techniques to hide information in digital media [61-66]. It is widely used in image steganography applications. S-Tools: This Windows-based steganography software uses the LSB algorithm to hide information in images and audio files. It supports many file formats, including JPEG, BMP, WAV, and MP3. These steganography systems use techniques and algorithms to embed hidden information in digital media. However, they also have limitations and can be vulnerable to attacks like steganalysis. Therefore, it is essential to carefully evaluate the robustness and security of a steganography system before using it for sensitive applications [67-71].

Proposed System

Today, the internet has become an essential tool for everyone. Nearly all payments, including taxes, insurance, bank transactions, healthcare fees, and e-commerce transactions, are conducted digitally using debit or credit cards or e-wallets. People frequently share personal information through social media platforms such as Facebook, Twitter, and WhatsApp. Governments in developing countries are increasingly adopting e-Governance systems to interact with citizens more efficiently [72-79]. The information shared through these applications has become a prime target for intruders. Various techniques have been crucial for information security over the years, with cryptography being a well-known method that keeps message content secret. However, cryptography alone is not entirely sufficient. Watermarking, another technique, hides data to protect copyright information but is also vulnerable as many methods can easily remove watermarks. Consequently, there is a growing preference for systems that conceal the existence of a secret message. Steganography, which emphasizes security through obscurity, has gained prominence [80-85].

The widespread use of digital images for online communication makes them a popular medium for steganography. Several factors contribute to this popularity, including content adaptability, redundancy, the limited power of the Human Visual System (HVS), the continuous advancement of powerful graphics capabilities in computers, and significant progress in digital image processing research. Audio is also considered a viable medium for steganography due to the way amplitudes are represented in real numbers, which causes minimal distortion when embedding bits of target data. Audio possesses unique characteristics, such as gradual amplitude changes rather than sudden ones and the suppression of lower frequency components by higher frequencies. However, the high sensitivity of the Human Auditory System (HAS) makes audio steganography a particularly challenging security technique [86-91].

Advantages

The proposed system is user-friendly due to its fast data retrieval and storage capabilities, ensuring efficient data management. Additionally, the system features a graphical user interface that simplifies user interaction. A news management system is integrated, allowing users to receive news updates tailored to their preferences. All data is promptly incorporated into the application, enabling immediate access to news information. This streamlined process significantly eases the workload, making it convenient to retrieve daily news updates.

Technology Used

Steganography involves concealing information within other information, such as embedding a message within an image or an audio file. Various technologies are employed for steganography, each with unique methods and applications. LSB (Least Significant Bit) Steganography replaces the least significant bit of each pixel in an image with a bit from the hidden message. The alteration is usually imperceptible to the human eye but can be detected using specialized software. Spread Spectrum disperses the hidden message across a wide frequency range within an audio signal [92-101]. A matching algorithm is then used to extract the message by reversing the process. Text Steganography hides a message within text using techniques like null ciphers, where the message is embedded within the text according to a pre-agreed code. Image Steganography hides a message within an image by altering the colors of specific pixels to represent the message. The LSB method is commonly used in this approach. Audio Steganography embeds a message within an audio file by modifying the sound waves in a manner that is undetectable to the human ear. Video Steganography conceals a message within a video file by altering certain frames to include the message. Methods such as LSB or modifying the color values of specific pixels can be used to achieve this. Each of these techniques leverages the unique properties of its respective medium to hide information in a way that is difficult to detect without specialized tools or knowledge [102-111].

Language: Python

Python is a popular language for steganography because it is easy to use, has many libraries for image and audio manipulation, and is widely used in data science. Here are some Python libraries commonly used for steganography:

Algorithms Used

The Least Significant Bit (LSB) algorithm is widely used in steganography, particularly for hiding data within images. It involves replacing the least significant bit of selected pixels in an image with a bit from the hidden message. The change is usually small enough that it is invisible to the human eye, but it can still be detected using specialized software.

Discrete Cosine Transform (DCT) algorithm: This algorithm is used to hide data within images and involves modifying the coefficients of the DCT of an image. The DCT is a mathematical transformation that separates an image into different frequency components, and the algorithm modifies the coefficients of the lower-frequency components to embed the hidden data.

Spread Spectrum algorithm: This algorithm hides data within audio signals and spreads the hidden message over a wide frequency range in an audio signal. The message can be extracted using a matching algorithm to reverse the process [112-117].

Phase Encoding algorithm: This algorithm is used to hide data within digital watermarks and involves modifying the phase of the image or signal to embed the hidden data. The phase of the image or signal is modified in a way that is not noticeable to the human eye or ear.

Text Steganography algorithms: These algorithms hide data within text and involve modifying the text in various ways to embed the hidden message. Examples include null ciphers, which involve hiding the message within the text using a pre-agreed code, and cryptography-based algorithms that encrypt the message before hiding it within the text [118-127].

We are using the MNIST dataset of handwritten digits; using this dataset, we will be training the discriminator. The MNIST dataset consists of 28x28 pixels grayscale images of handwritten digits from 0 to 9. To use them, we will transform them into Pytorch tensors using transforms.ToTensor()

The output will be similar to:

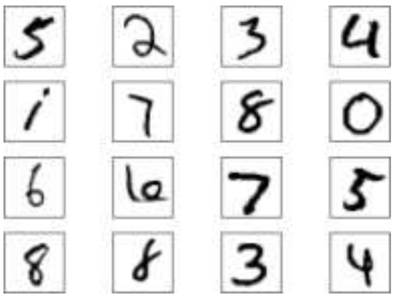

Figure 1: Data Collection

Then, we will split the data into test data and training data (Figure 1).

Step 1: Data Collection

i) in this case, the discriminator is an MLP neural network that receives a 28 × 28-pixel image and provides the probability of the image belonging to the real training data.

```
class Discriminator(nn.Module): def init    (self):
super().      init    () self.model = nn.Sequential(
nn.Linear(784, 1024), nn.ReLU(),
nn.Dropout(0.3),

nn.Linear(1024, 512), nn.ReLU(),
nn.Dropout(0.3), nn.Linear(512, 256), nn.ReLU(),
nn.Dropout(0.3), nn.Linear(256, 1), nn.Sigmoid(),
)
def forward(self, x):
x = x.view(x.size(0), 784) output = self.model(x) return output
```

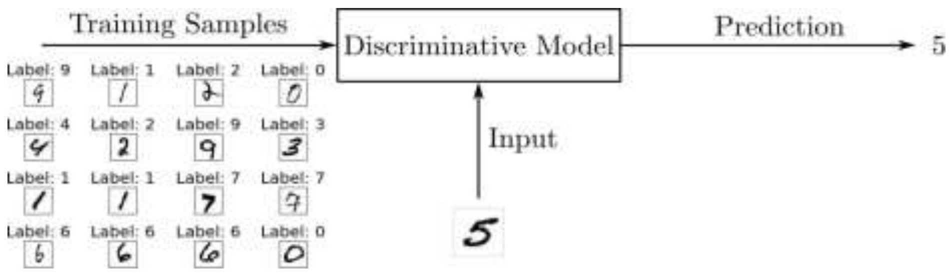

Figure 2: Processing of data

Step 2: Processing of data (Figure 2)

Since the generator will generate more complex data, increasing the dimensions of the input from the latent space is necessary. In this case, the generator will be fed a 100-dimensional input and will provide an output with 784 coefficients, organized in a 28 × 28 tensor representing an image [128-133].

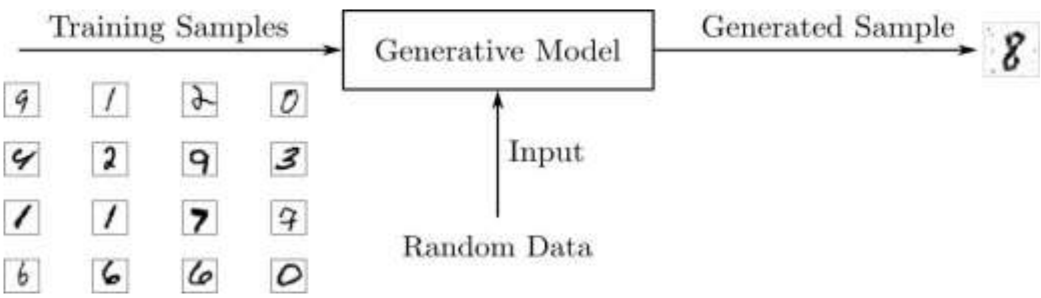

Figure 3: Training the models and checking the Samples Generated by the GAN

Step 3: Training the models and checking the Samples Generated by the GAN (Figure 3)

To train the models effectively, it is essential to define the training parameters and optimizers. Decreasing the learning rate and setting the number of epochs to 50 can yield better results and reduce the training time. For generating handwritten digits, you need to take random samples from the latent space and feed them to the generator [134-139]. When plotting `generated_samples`, move the data back to the CPU if it is running on the GPU, and ensure to call `.detach()` before using Matplotlib to plot the data. After fifty epochs of training, several generated digits should resemble the real ones [140-147]. To further improve the results, consider increasing the number of training epochs. The output should be digits that closely resemble the training data, as illustrated in figure 4.

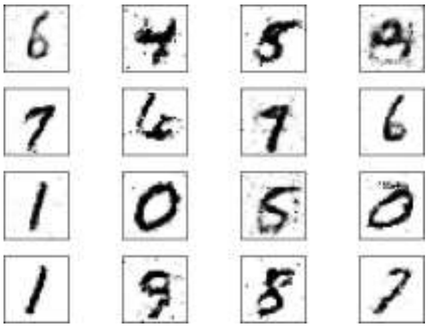

Figure 4: Expected Output

Step 4: Building the Model

The next step involves building the model using machine learning techniques. Regression is particularly significant for Android news applications. TensorFlow Lite is recommended for ML runtime, as it allows for high-performance ML inference in your app via Google Play services, Android's official ML inference runtime [148-149]. To enhance performance further, you can utilize hardware acceleration with TensorFlow Lite Delegates. These delegates, available through Google Play services, enable accelerated ML on specialized hardware such as GPUs, NPUs, or DSPs. This approach can help deliver more fluid, lower latency user experiences by leveraging advanced on-device compute capabilities.

Step 5: Testing the Model

Testing the model is crucial to ensure its predictive accuracy. The first step involves making predictions on the testing set. Regression testing plays a vital role in this phase, especially for mobile apps. Many companies use regression testing to guarantee their apps function smoothly and remain reliable over time. Organizations need to consider several factors while performing regression testing, such as utilizing distributed devices for mobile app testing from any location at any time. Testing your app is an essential component of the app development process. Consistently running tests against your app allows you to verify its correctness, functional behavior, and usability before it is released publicly. This practice ensures that the app meets quality standards and provides a seamless user experience.

Step 6: Implementing the model

Successful news app development relies on effective visualization of news and its features for the user. Material design greatly enhances Android app development by providing smooth experiences with custom layouts, views, and animations. For this news app, users can select news from different categories, countries, and newspapers. Displaying short news snippets in a list view with a header, brief description, and image helps users quickly identify their desired news before viewing the full article. Utilizing a ViewHolder improves performance and speeds up the list view. Libraries like

Picasso efficiently handle images. This user interface connects to the API and the Admin Panel database, offering full articles in a web view while maintaining the author's integrity.

The News API gathers various news sources in one place. When a request is made, it responds in JSON format, including source ID, title, description, image URL, article URL, author, and time. This JSON data must be handled and parsed into the required string format. The Admin Panel module manages user and writer logins through the database. Writers can add, update, and delete news items. Writers only have access to the admin panel, while the Main Admin has access to the database. The Main Admin can add users, writers, and news, as well as approve, update, or delete entries. This system enables the creation of a local news network, with writers and local admins providing community-level news. A location feature can update local news for different areas or cities.

The application offers several features. Global support provides access to different newspapers worldwide in various languages, allowing users to access global news. News appears in a short format with a title, image, and brief description in a list view, helping users quickly find relevant news. The search option allows users to search for news from one source or many sources available within the API. Users can save news articles as favorites, automatically saving them for offline reading. Additionally, users can easily share news on social media platforms. Users must sign up to access the application, ensuring security. Predicted user error handling with pop-up messages addresses issues such as entering invalid data or not selecting a field before clicking an action button. Screenshots demonstrate the application's functionality as a result of this study.

The model trains using all images from the datasets, saving each image's characteristics. Upon completing training, the MobilenetV2 saves the director model, allowing it to function with the provided input. The application undergoes thorough testing. Unit testing verifies individual bits of code for viability. Integration testing assesses the model's efficiency against functional requirements. Functional testing verifies the output with the provided input to ensure it meets functional requirements. By implementing these features and testing processes, the application ensures a smooth user experience, efficient news delivery, and robust performance.

Results and Discussions

The proposed system is user-friendly due to its fast data retrieval and storage capabilities, ensuring efficient data maintenance. The system features a graphical user interface that allows users to interact with it easily. A news management system can be effortlessly generated within the proposed system, enabling users to see news updates according to their preferences. Data is immediately incorporated into the application, allowing news information to be quickly generated. This approach simplifies work processes, making it easy to retrieve daily news statuses.

In contrast, the current framework requires manual entry by students, making it tedious to maintain the status of the news management system. Human effort is significantly higher in this manual system, making the retrieval of weekly and monthly records challenging. Students often need to visit the library to find information about the school or current events, which is time-consuming and inefficient. The proposed framework is more user-friendly because it facilitates quick and efficient data retrieval and storage. The graphical user interface further simplifies interaction, enabling users to manage the system with ease. The news management system can be easily generated within the proposed framework, providing users with updates tailored to their needs. Data is promptly integrated into the application, and news information can be readily produced. This significantly simplifies work processes, allowing daily news status to be retrieved effortlessly.

Regarding potential enhancements, several improvements can be made. Developing new steganography algorithms that are more secure and harder to detect could significantly enhance security. This could involve advanced encryption techniques or novel methods for embedding data within files. Multi-modal steganography, which uses multiple media types such as images, audio, and video files to hide data, could provide an added layer of security by distributing the hidden data across various files. Additionally, machine learning techniques can be leveraged to create more sophisticated steganography models capable of adapting to different data types and identifying vulnerabilities in existing algorithms. Deep learning algorithms, such as neural networks, could further improve the accuracy of steganography models and aid in the development of new algorithms, enhancing overall effectiveness and security.

Cloud-based steganography: Cloud-based steganography involves storing encrypted data in a cloud-based service, which can be accessed and decrypted by authorized users. This could provide an added layer of security, as the data is stored off-site and is not easily accessible to unauthorized users. Integration with blockchain technology: Steganography models could be integrated to provide a more secure and transparent method of storing and sharing sensitive data. Quantum steganography: Quantum steganography is a potential area for future enhancements, as it involves using the principles of quantum mechanics to hide information within quantum systems. This could provide even greater security and confidentiality, as quantum systems are known for their sensitivity to external interference. Adversarial attacks and defenses: Adversarial attacks and defenses involve using machine learning and deep learning algorithms to identify and defend against attacks on steganography models. This could improve the robustness of steganography algorithms and make them more resistant to attacks by hackers and other malicious actors.

Hardware-based steganography: Hardware-based steganography involves developing steganography models that can be embedded directly into hardware devices, such as smartphones, laptops, and IoT devices. This could provide an added layer of security, as the hidden data would be stored within the device itself, making it more difficult for attackers to access or detect. Privacy-preserving steganography: Privacy-preserving steganography involves developing algorithms that can hide data while preserving the privacy of the users who are sending and receiving the data. This could involve using techniques such as differential privacy or homomorphic encryption to protect the privacy of sensitive information. Invisible steganography: Invisible steganography involves developing algorithms that can hide data without altering the original file in any noticeable way. This could be useful in situations where the appearance or integrity of the original file needs to be preserved, such as in legal or forensic contexts.

Conclusion

GANs, or Generative Adversarial Networks, are game-theoretic generative models that have achieved significant success in creating realistic data, particularly images. However, training them remains a challenge. It is necessary to develop models, optimizers, or training algorithms that can consistently and rapidly identify appropriate Nash equilibria for GANs, making them a more reliable technology. The ability of GANs to learn deep, highly non-linear mappings from latent space to data space and vice versa has sparked considerable interest. This capability allows them to handle large amounts of unlabeled image data, which is often inaccessible to traditional deep representation learning techniques. The complexities of GAN training present numerous opportunities for theoretical and algorithmic advancements. Leveraging the power of deep networks, GANs hold potential for a wide range of new applications. GANs generate structured geometric vector spaces for various domains by creating their representations of the data they are trained on. These representations can be used for multiple tasks, such as image synthesis, semantic image editing, style transfer, image super-resolution, and classification. The versatility of GANs in training representations for diverse applications underscores their potential impact across different fields. In conclusion, despite the challenges in training GANs, their ability to handle complex, unlabeled data and generate realistic outputs makes them a powerful tool in deep learning. Continued advancements in their theoretical and algorithmic foundations will likely expand their applicability and reliability, leading to new and innovative uses in various domains.

Reference

1. A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," IEEE Signal Process. Mag., vol. 35, no. 1, pp. 53–65, 2018.
2. P. Shamsolmoali et al., "Image synthesis with adversarial networks: A comprehensive survey and case studies," Inf. Fusion, vol. 72, no.1, pp. 126–146, 2021.
3. A. Thakur, H. Rizvi, and M. Satish, White-Box Cartoonization Using An Extended GAN Framework. vol.5, no.12, p.294-298, 2021.
4. P. P. Anand, U. K. Kanike, P. Paramasivan, S. S. Rajest, R. Regin, and S. S. Priscila, "Embracing Industry 5.0: Pioneering Next-Generation Technology for a Flourishing Human Experience and Societal Advancement," FMDB Transactions on Sustainable Social Sciences Letters, vol.1, no. 1, pp. 43–55, 2023.
5. G. Gnanaguru, S. S. Priscila, M. Sakthivanitha, S. Radhakrishnan, S. S. Rajest, and S. Singh, "Thorough analysis of deep learning methods for diagnosis of COVID-19 CT images," in Advances in Medical Technologies and Clinical Practice, IGI Global, pp. 46–65, 2024.
6. G. Gowthami and S. S. Priscila, "Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach," Int. J. Crit. Comput.-based Syst., vol. 10, no. 4, pp. 355–374, 2023.
7. A. J. Obaid, S. Suman Rajest, S. Silvia Priscila, T. Shynu, and S. A. Ettyem, "Dense convolution neural network for lung cancer classification and staging of the diseases using NSCLC images," in Proceedings of Data Analytics and Management, Singapore; Singapore: Springer Nature, pp. 361–372, 2023.
8. S. S. Priscila and A. Jayanthiladevi, "A study on different hybrid deep learning approaches to forecast air pollution concentration of particulate matter," in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023.
9. S. S. Priscila, S. S. Rajest, R. Regin, and T. Shynu, "Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.

10. S. S. Priscila and S. S. Rajest, "An Improvised Virtual Queue Algorithm to Manipulate the Congestion in High-Speed Network"," Central Asian Journal of Medical and Natural Science, vol. 3, no. 6, pp. 343–360, 2022.
11. S. S. Priscila, S. S. Rajest, S. N. Tadiboina, R. Regin, and S. András, "Analysis of Machine Learning and Deep Learning Methods for Superstore Sales Prediction," FMDB Transactions on Sustainable Computer Letters, vol. 1, no. 1, pp. 1–11, 2023.
12. R. Regin, Shynu, S. R. George, M. Bhattacharya, D. Datta, and S. S. Priscila, "Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting," Int. J. Bioinform. Res. Appl., vol. 19, no. 3, 2023.
13. S. Silvia Priscila, S. Rajest, R. Regin, T. Shynu, and R. Steffi, "Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.
14. S. S. Rajest, S. Silvia Priscila, R. Regin, T. Shynu, and R. Steffi, "Application of Machine Learning to the Process of Crop Selection Based on Land Dataset," International Journal on Orange Technologies, vol. 5, no. 6, pp. 91–112, 2023.
15. T. Shynu, A. J. Singh, B. Rajest, S. S. Regin, and R. Priscila, "Sustainable intelligent outbreak with self-directed learning system and feature extraction approach in technology," International Journal of Intelligent Engineering Informatics, vol. 10, no. 6, pp.484-503, 2022.
16. S. S. Priscila, D. Celin Pappa, M. S. Banu, E. S. Soji, A. T. A. Christus, and V. S. Kumar, "Technological frontier on hybrid deep learning paradigm for global air quality intelligence," in Cross-Industry AI Applications, IGI Global, pp. 144–162, 2024.
17. S. S. Priscila, E. S. Soji, N. Hossó, P. Paramasivan, and S. Suman Rajest, "Digital Realms and Mental Health: Examining the Influence of Online Learning Systems on Students," FMDB Transactions on Sustainable Techno Learning, vol. 1, no. 3, pp. 156–164, 2023.
18. S. R. S. Steffi, R. Rajest, T. Shynu, and S. S. Priscila, "Analysis of an Interview Based on Emotion Detection Using Convolutional Neural Networks," Central Asian Journal of Theoretical and Applied Science, vol. 4, no. 6, pp. 78–102, 2023.
19. Sumeet Hangargi, Amit Swamy , R.Gowtham Raj, et al (2023), Enhancement of Kevlar fiber-polypropylene composite by the inclusions of cotton stalk and granite particle: characteristics study. Biomass conversion and Biorefinery, Springer – 04 Sept 23.
20. Swamy A and Achanta CR. (2023) An investigation of Gastrointestinal infections using prediction model. 14th International conference on advances in computing, control and telecommunication technologies, ACT 2023, 2023-June, pp 2660-2666
21. Swamy A and Achanta CR (2022). Innovative Technology for gastrointestinal polyps detection. ICOSNIKOM 2022 – 2022 IEEE International conference of computing science and information technology: Boundary free: Preparing Indonesia for Metaverse society, 2022. Indonesia, October 20-22, 2022.
22. Swamy A and Achanta CR (2022),.'Design and development of innovative integrated technology for endoscopic surgeries'. Neuro Quantology: An interdisciplinary journal of neuroscience and Quantum physics. September 2022, Vol 20 (11): 2389 – 2398:
23. Swamy A, (2022), "An investigation into the efficient Engineering study using Project based Learning", Journal of Positive School Psychology, 2022, Vol. 6, No 5, 6291 - 6297.
24. B. Singh, A. Swamy, S. Khurram, R. Regin, S. K. S and P. Poonkuzhali, (2021) "Detection and Localization of Early-Stage Lung Tumor Using K-Means Clustering and Object Counting," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, Proceedings of IEEE, pp. 1641-1644.

25. Swamy A, Zebenay TA (2021), "An elephant foot analogy: Design and development of landing gear". ASEAN Journal of science and engineering, version 1 (3) pp 145-152.
26. Abidin S, Swamy A, Ramirez-Asis E et al. (2021), "Quantum Cryptography techniques: a way to improve security challenges in mobile cloud computing", Materials today: Proceedings.
27. Amit Swamy, C. Shamitha, Manoj Kumar Singh, Moti Lala Rinawa, K.V. Pradeep kumar, Sami Al Obaid, Mahadeo A Mahadik, Saleh Alfarraj, Mebratu Markos, (2022) " Experimental Investigation on wear behaviour of Eutectic Al-7075/CNT/Graphite Composites manufactured by a combination of two stage stir and squeeze casting techniques", Journal of nanomaterials, Vol 2022, 8 pages, Paper ID: 7995261.
28. Swamy A, (2021), "Shape memory wires as artificial muscles: An experimental approach", Turkish Journal of computer and Mathematics education, Vol.12 No.11, p.3590- 3603.
29. R. Babu and E. S. Reddy, “A Comprehensive Survey on Semantic based Image Retrieval Systems for Cyber Forensics,” International Journal of Computer Sciences and Engineering, vol. 6, no. 8, pp. 245–250, 2018.
30. R. B. Putchanuthala and E. S. Reddy, “Image retrieval using locality preserving projections,” J. Eng. (Stevenage), vol. 2020, no. 10, pp. 889–892, 2020.
31. R. Babu and E. S. Reddy, “A Novel Framework design for Semantic based Image retrieval as a Cyber Forensic Tool,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 2801–2808, 2019.
32. R. Babu, P. E. S. Reddy, “A design of eigenvalue based CNN tool for image retrieval,” Int. J. Eng. Adv. Technol., vol. 8, no. 6, pp. 2230–2236, 2019.
33. P. R. Babu, R. Nandhi Kesavan, A. Sivaramakrishnan, and G. Sai Chaitanya, “EmoGAN Label-Changing Approach for Emotional State Analysis in Mobile Communication using Monkey Algorithm”,” ICTACT Journal on Communication Technology, vol. 14, no. 4, pp. 3050–3056, 2023.
34. D. C. J. W. Wise, S. Ambareesh, R. Babu, D. Sugumar, J. P. Bhimavarapu, and A. S. Kumar, “Latent Semantic Analysis Based Sentimental Analysis of Tweets in Social Media for the Classification of Cyberbullying Text”,” Int J Intell Syst Appl Eng, vol. 12, no. 7s, pp. 26–35, 2023.
35. Y. K. Aluri, B. Devi, N. A. Balaji, V. Dakshinamurthi, R. Babu, and S. Rajeyyagari, “Dry Eye Disease Classification Using AlexNet Classifier”,” Int J Intell Syst Appl Eng, vol. 12, no. 7s, pp. 263–271, 2023.
36. M. Srinivasan, K. Hc, S. Govindasamy, M. A. Rasheed, R. Babu, and P. Sultana, “Energy Efficient Routing Using Support Vector Machine in Wireless Sensor Networks”,” Int J Intell Syst Appl Eng, vol. 12, no. 7s, pp. 320–325, 2023.
37. B. S. Rao, K. Meenakshi, K. Kalaiarasi, R. Babu, J. Kavitha, and V. Saravanan, “Image Caption Generation Using Recurrent Convolutional Neural Network ”,” Int J Intell Syst Appl Eng, vol. 12, no. 7s, pp. 76–80, 2023.
38. P. T. Anitha, W. Dibaba, and R. Boddu, “Mitigation of Attacks Using Cybersecurity Deep Models in Cloud Servers,” in 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, pp. 202–205, 2023.
39. D. Kavitha, S. Shobana, S. Rajkumar, G. R. Reddy, R. Babu, and P. Mukherjee, “Hyperspectral Image Classification Using Dimensionality Reduction Deep Networks”,” Int J Intell Syst Appl Eng, vol. 12, no. 7s, pp. 81–86, 2023.

40. Sunil Kumar Sehrawat, “Transforming Clinical Trials: Harnessing the Power of Generative AI for Innovation and Efficiency”, Transactions on Recent Developments in Health Sectors, vol. 6, no. 6, p. 1-20, 2023.
41. Sunil Kumar Sehrawat, “Empowering the Patient Journey: The Role of Generative AI in Healthcare”, International Journal of Sustainable Development Through AI, ML and IoT, vol. 2, no. 2, p. 1-18, 2023.
42. Sunil Kumar Sehrawat, “The Role of Artificial Intelligence in ERP Automation: State-of-the-Art and Future Directions”, Transactions on Latest Trends in Artificial Intelligence, vol. 4, no. 4, 2023.
43. Sudheer Kumar Kothuru, “Impact of Artificial Intelligence and Machine Learning in the Sustainable Transformation of the Pharma Industry”, International Conference on Sustainable Development, Machine Learning, AI and Iot, 2024.
44. Sudheer Kumar Kothuru, “Advancing Healthcare Outcomes through Machine Learning Innovations”, Cross-Industry AI Applications, Vol. 15, pp. https://www.igi-global.com/book/cross-in, 2024.
45. Sudheer Kumar Kothuru, “Blockchain Revolution in Pharmaceutical Industry: A Comprehensive Study”, Transactions on Recent Developments in Health Sectors, vol. 6, no. 6, p. 1-23, 2023.
46. Sudheer Kumar Kothuru, “AI-Driven Innovations in Healthcare: Improving Diagnostics and Patient Care”, International Journal of Machine Learning and Artificial Intelligence, vol. 4, no. 4, p. 1-13, 2023.
47. Sudheer Kumar Kothuru, “Emerging Technologies for Health and Wellness Monitoring at Home”, FMDB Transactions on Sustainable Health Science Letters, vol. 1, no. 4, p. 208-218, 2023.
48. Hassan, M.M. (2020). A Fully Bayesian Logistic Regression Model for Classification of ZADA Diabetes Dataset. Science Journal of University of Zakho, 8, 105-111.
49. Hassan, M.M., & Taher, S.A. (2022). Analysis and Classification of Autism Data Using Machine Learning Algorithms. Science Journal of University of Zakho, 10, 206-2012.
50. Hassan, M.M. (2018). Bayesian Sensitivity Analysis to Quantifying Uncertainty in a Dendroclimatology Model. 2018 International Conference on Advanced Science and Engineering (ICOASE), 363-368.
51. Ismail, H.R., & Hassan, M.M. (2023). Bayesian deep learning methods applied to diabetic retinopathy disease: a review. Indonesian Journal of Electrical Engineering and Computer Science, 30, 1167-1177.
52. Hassan, M. M., & Ahmed, D. (2023). Bayesian Deep Learning Applied To Lstm Models For Predicting Covid-19 Confirmed Cases In Iraq. Science Journal of University of Zakho, 11(2), 170–178.
53. S. Agarwal, "Machine Learning Based Personalized Treatment Plans for Chronic Conditions," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 1127-1132.
54. S. Agarwal, “The Interplay between Natural Language Processing (NLP) and Clinical Data Mining in Healthcare: A Review”,” Int J Intell Syst Appl Eng, vol. 12, no. 3, pp. 4161–4169, 2024.
55. S. Agarwal, “Optimizing product choices through A/B testing and data analytics: A comprehensive review,” International Journal of Advanced Research in Science, Communication and Technology, vol.3, no.1, pp. 550–555, 2023.

56. S. Agarwal, "Validating Clinical Applications of Digital Health Solutions and Managing Associated Risk Management," FMDB Transactions on Sustainable Management Letters., vol. 1, no. 4, pp. 134-143, 2023.
57. M. Senbagavalli and G. T. Arasu, "Opinion Mining for Cardiovascular Disease using Decision Tree based Feature Selection," Asian J. Res. Soc. Sci. Humanit., vol. 6, no. 8, p. 891, 2016.
58. M. Senbagavalli and S. K. Singh, "Improving patient health in smart healthcare monitoring systems using IoT," in 2022 International Conference on Futuristic Technologies (INCOFT), pp. 1-7, Belgaum, India, 2022.
59. M. S. Valli and G. T. Arasu, "An Efficient Feature Selection Technique of Unsupervised Learning Approach for Analyzing Web Opinions," Journal of Scientific & Industrial Research, vol. 75, no.4, pp. 221–224, 2016.
60. Narayan Hampiholi, "Revolutionizing AI and Computing the Neuromorphic Engineering Paradigm in Neuromorphic Chips", International Journal of Computer Trends and Technology, vol. 72, no. 1, p. 7, 2024.
61. Narayan Hampiholi, "Elevating Emergency Healthcare - Technological Advancements and Challenges in Smart Ambulance Systems and Advanced Monitoring and Diagnostic Tools", International Journal of Computer Trends and Technology, vol. 72, no. 1, p. 1-7, 2024.
62. Narayan Hampiholi, "Real-World Deployments of AR In Medical Training and Surgery", Journal of Emerging Technologies and Innovative Research, vol. 10, no. 10, p. 8, 2023.
63. Narayan Hampiholi, "Medical Imaging Enhancement with Ai Models for Automatic Disease Detection and Classification Based on Medical Images", International Journal of Engineering Applied Sciences and Technology, vol. 8, no. 5, p. 31-37, 2023.
64. Narayan Hampiholi, "21st Century Geriatric Care - Matching Advancing Devices to the Needs of the Aging Population", Journal of Emerging Technologies and Innovative Research, vol. 10, no. 10, p. 7, 2023.
65. Narayan Hampiholi, "Through The Lens of Principled Data Practice a Groundbreaking Exploration into Ethical Healthcare Platforms", International Journal of Engineering Applied Sciences and Technology, vol. 8, no. 5, p. 26-30, 2023.
66. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, "Review of the role of nanotechnology in overcoming the challenges faced in oral cancer diagnosis and treatment," Molecules, vol. 28, no. 14, p. 5395, 2023.
67. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, "Review insights on salivary proteomics biomarkers in oral cancer detection and diagnosis," Molecules, vol. 28, no. 13, p. 5283, 2023.
68. P. Natarajan, V. Rekha, A. Murali, and B. Swamikannu, "Newer congeners of doxycycline – do they hold promise for periodontal therapy?," Arch. Med. Sci. - Civiliz. Dis., vol. 7, no. 1, pp. 16–23, 2022.
69. V. Rekha U, P. Mn, and Bhuminathan., "Review on Anticancer properties of Piperine in Oral cancer: Therapeutic Perspectives," Res. J. Pharm. Technol., pp. 3338–3342, 2022.
70. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, "Comprehensive review on development of early diagnostics on oral cancer with a special focus on biomarkers," Appl. Sci. (Basel), vol. 12, no. 10, p. 4926, 2022.
71. V. R. Umapathy et al., "Current trends and future perspectives on dental nanomaterials – An overview of nanotechnology strategies in dentistry," J. King Saud Univ. Sci., vol. 34, no. 7, p. 102231, 2022.

72. V. R. Umapathy et al., “Emerging biosensors for oral cancer detection and diagnosis—A review unravelling their role in past and present advancements in the field of early diagnosis,” Biosensors (Basel), vol. 12, no. 7, p. 498, 2022.
73. P. M. Natarajan, V. R. Umapathy, A. Murali, and B. Swamikannu, “Computational simulations of identified marine-derived natural bioactive compounds as potential inhibitors of oral cancer,” Future Sci. OA, vol. 8, no. 3, 2022.
74. P. M. Natarajan, V. R. Umapathy, A. Murali, and B. Swamikannu, “Computational simulations of identified marine-derived natural bioactive compounds as potential inhibitors of oral cancer,” Future Sci. OA, vol. 8, no. 3, 2022.
75. P. Manickam Natarajan, “Dental Bioinformatics – Current Scope and Future perspectives,” Res. J. Pharm. Technol., pp. 2351–2356, 2022.
76. B. Juala Catherine Jebaraj, P. Birla Bose, R. Manickam Natarajan, and A. Gurusamy, “Perception of dental interns on the impact of their gender during training period and future dental practice-cross sectional survey in dental colleges in Chennai,” India. Journal of Positive School Psychology, vol. 2022, no. 5, pp. 1045–1050.
77. V. R. Umapathy et al., “Emerging biosensors for oral cancer detection and diagnosis—A review unravelling their role in past and present advancements in the field of early diagnosis,” Biosensors (Basel), vol. 12, no. 7, p. 498, 2022.
78. V. R. Umapathy et al., “Current trends and future perspectives on dental nanomaterials – An overview of nanotechnology strategies in dentistry,” J. King Saud Univ. Sci., vol. 34, no. 7, p. 102231, 2022.
79. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, “Comprehensive review on development of early diagnostics on oral cancer with a special focus on biomarkers,” Appl. Sci. (Basel), vol. 12, no. 10, p. 4926, 2022.
80. V. Rekha U, P. Mn, and Bhuminathan., “Review on Anticancer properties of Piperine in Oral cancer: Therapeutic Perspectives,” Res. J. Pharm. Technol., pp. 3338–3342, 2022.
81. P. Natarajan, V. Rekha, A. Murali, and B. Swamikannu, “Newer congeners of doxycycline – do they hold promise for periodontal therapy?,” Arch. Med. Sci. - Civiliz. Dis., vol. 7, no. 1, pp. 16–23, 2022.
82. B. B. Bose, P. M. Natarajan, A. L. Kannan, J. C. Jebaraj, R. Jagannathan, and T. M. Balaji, “Evaluation of block allograft efficacy in lateral alveolar ridge augmentation,” J. Contemp. Dent. Pract., vol. 23, no. 8, pp. 807–812, 2022.
83. J. Pei et al., “A comprehensive review on bio-based materials for chronic diabetic wounds,” Molecules, vol. 28, no. 2, p. 604, 2023.
84. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, “Review insights on salivary proteomics biomarkers in oral cancer detection and diagnosis,” Molecules, vol. 28, no. 13, p. 5283, 2023.
85. V. R. Umapathy, P. M. Natarajan, and B. Swamikannu, “Review of the role of nanotechnology in overcoming the challenges faced in oral cancer diagnosis and treatment,” Molecules, vol. 28, no. 14, p. 5395, 2023.
86. S. I. Ansarullah, S. Mohsin Saif, S. Abdul Basit Andrabi, S. H. Kumhar, M. M. Kirmani, and D. P. Kumar, “An intelligent and reliable hyperparameter optimization machine learning model for early heart disease assessment using imperative risk attributes,” J. Healthc. Eng., vol. 2022, pp. 1–12, 2022.
87. S. I. Ansarullah, S. M. Saif, P. Kumar, and M. M. Kirmani, “Significance of visible non-invasive risk attributes for the initial prediction of heart disease using different machine learning techniques,” Comput. Intell. Neurosci., vol. 2022, pp. 1–12, 2022.

88. M. M. Kirmani and S. I. Ansarullah, "Classification models on cardiovascular disease detection using Neural Networks, Naïve Bayes and J48 Data Mining Techniques," International Journal of Advanced Research in Computer Science, vol. 7, no. 5, 2016.
89. M.M. Kirmani, & S.I. Ansarullah, "Prediction of heart disease using decision tree a data mining technique". Int. J. Comput. Sci. Netw, 5(6), 2016.
90. E. Zanardo and B. Martini, "Secure and Authorized Data Sharing among different IoT Network Domains using Beez blockchain," in 2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN), 2024, pages 122–129.
91. E. Zanardo, "Learningchain. A novel blockchain-based meritocratic marketplace for training distributed machine learning models," in Software Engineering Application in Systems Design, Cham: Springer International Publishing, 2023, pp. 152–169.
92. E. Zanardo, B. Martini, and D. Bellisario, "Tokenized intelligence: Redefine network optimization in softwarized networks," in 2024 IEEE 10th International Conference on Network Softwarization (NetSoft), 2024.
93. E. Zanardo, "Bitnocolo -anti money laundering (AML) tool for blockchain transactions." Unpublished, 2020.
94. E. Zanardo, G. P. Domiziani, E. Iosif, and K. Christodoulou, "Identification of illicit blockchain transactions using hyperparameters auto-tuning," in Principles and Practice of Blockchains, Cham: Springer International Publishing, 2023, pp. 27–38.
95. Reddy, A. R. P., & Ayyadapu, A. K. R. (2021). Securing Multi-Cloud Environments with AI And Machine Learning Techniques. Chelonian Research Foundation, 16(2), 01-12.
96. Reddy Ayyadapu, A. K. (2022). Privacy-Preserving Techniques in AI-Driven Big Data Cyber Security for Cloud. Chelonian Research Foundation, 17(2), 188-208.
97. Ayyadapu, A. K. R. (2022). Secure Cloud Infrastructures: A Machine Learning Perspective. International Neurourology Journal, 26(4), 22-29.
98. Ayyadapu, A. K. R. (2023). Enhancing Cloud Security with AI-Driven Big Data Analytics. International Neurourology Journal, 27(4), 1591-1597.
99. Reddy Ayyadapu, A. K. (2023). Optimizing Incident Response in Cloud Security with Ai And Big Data Integration. Chelonian Research Foundation, 18(2), 2212-2225.
100. Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.
101. Reddy, A. R. P. (2021). Machine Learning Models for Anomaly Detection in Cloud Infrastructure Security. NeuroQuantology, 19(12), 755-763.
102. Reddy, A. R. P. (2021). The Role of Artificial Intelligence in Proactive Cyber Threat Detection In Cloud Environments. NeuroQuantology, 19(12), 764-773.
103. Reddy, A. R. P. (2022). The Future of Cloud Security: Ai-Powered Threat Intelligence and Response. International Neurourology Journal, 26(4), 45-52.
104. Reddy, A. R. P. (2023). Navigating the Cloud's Security Maze: AI and ML as Guides. International Neurourology Journal, 27(4), 1613-1620.
105. B. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Lecture Notes in Computer Science, Singapore: Springer Nature Singapore, 2023, pp. 22–39.
106. B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 1, no. 100019, p. 100019, 2023.

107. B. Senapati et al., “Wrist crack classification using deep learning and X-ray imaging,” in Proceedings of the Second International Conference on Advances in Computing Research (ACR’24), Cham: Springer Nature Switzerland, 2024, pp. 60–69.
108. A. B. Naeem et al., “Heart disease detection using feature extraction and artificial neural networks: A sensor-based approach,” IEEE Access, vol. 12, pp. 37349–37362, 2024.
109. R. Tsarev et al., “Automatic generation of an algebraic expression for a Boolean function in the basis ∧, ∨, ¬,” in Data Analytics in System Engineering, Cham: Springer International Publishing, 2024, pp. 128–136.
110. R. Tsarev, B. Senapati, S. H. Alshahrani, A. Mirzagitova, S. Irgasheva, and J. Ascencio, “Evaluating the effectiveness of flipped classrooms using linear regression,” in Data Analytics in System Engineering, Cham: Springer International Publishing, 2024, pp. 418–427.
111. E. Geo Francis and S. Sheeja, “An optimized intrusion detection model for wireless sensor networks based on MLP-CatBoost algorithm,” Multimedia Tools and Applications, 2024,
112. E. Geo Francis and S. Sheeja, “SHAKE-ESDRL-based energy efficient intrusion detection and hashing system,” Annals of Telecommunications, 2023,
113. E. Geo Francis and S. Sheeja, “Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review,” Engineering and Applied Science Research, 2023, vol. 50, no. 6, pp. 633–645,
114. E. Geo Francis and S. Sheeja, “A Novel RDAE Based PSR-QKD Framework for Energy Efficient Intrusion Detection," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-6.
115. E. Geo Francis and S. Sheeja, “Towards an Optimal Security Using Multifactor Scalable Lightweight Cryptography for IoT," 2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4), Bangalore, India, 2022, pp. 1-6.
116. E. Geo Francis, S. Sheeja and Joseph Jismy, “A Three-layer Convolution Neural Network Approach for Intrusion Detection in IoT," 2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 2023, pp. 261-268.
117. E. Geo Francis, S. Sheeja and E. F. Antony John, “IoT Intrusion Detection Using Two-Tier-Convolutional Deep-Learning Model," 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2023, pp. 1-7.
118. D. K. Sharma and R. Tripathi, “4 Intuitionistic fuzzy trigonometric distance and similarity measure and their properties,” in Soft Computing, De Gruyter, 2020, pp. 53–66.
119. D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. Kalyan Chakravarthi, “Applications of two separate methods to deal with a small dataset and a high risk of generalization,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
120. D. K. Sharma, B. Singh, M. Anam, K. O. Villalba-Condori, A. K. Gupta, and G. K. Ali, “Slotting learning rate in deep neural networks to build stronger models,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
121. K. Kaliyaperumal, A. Rahim, D. K. Sharma, R. Regin, S. Vashisht, and K. Phasinam, “Rainfall prediction using deep mining strategy for detection,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
122. I. Nallathambi, R. Ramar, D. A. Pustokhin, I. V. Pustokhina, D. K. Sharma, and S. Sengan, “Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach,” Environ. Pollut., vol. 304, no. 119182, p. 119182, 2022.

123. H. Sharma and D. K. Sharma, "A Study of Trend Growth Rate of Confirmed Cases, Death Cases and Recovery Cases of Covid-19 in Union Territories of India," Turkish Journal of Computer and Mathematics Education, vol. 13, no. 2, pp. 569–582, 2022.
124. A. L. Karn et al., "Designing a Deep Learning-based financial decision support system for fintech to support corporate customer's credit extension," Malays. J. Comput. Sci., pp. 116–131, 2022.
125. A. L. Karn et al., "B-lstm-Nb based composite sequence Learning model for detecting fraudulent financial activities," Malays. J. Comput. Sci., pp. 30–49, 2022.
126. P. P. Dwivedi and D. K. Sharma, "Application of Shannon entropy and CoCoSo methods in selection of the most appropriate engineering sustainability components," Cleaner Materials, vol. 5, no. 100118, p. 100118, 2022.
127. A. Kumar, S. Singh, K. Srivastava, A. Sharma, and D. K. Sharma, "Performance and stability enhancement of mixed dimensional bilayer inverted perovskite (BA2PbI4/MAPbI3) solar cell using drift-diffusion model," Sustain. Chem. Pharm., vol. 29, no. 100807, p. 100807, 2022.
128. A. Kumar, S. Singh, M. K. A. Mohammed, and D. K. Sharma, "Accelerated innovation in developing high-performance metal halide perovskite solar cell using machine learning," Int. J. Mod. Phys. B, vol. 37, no. 07, 2023.
129. G. A. Ogunmola, M. E. Lourens, A. Chaudhary, V. Tripathi, F. Effendy, and D. K. Sharma, "A holistic and state of the art of understanding the linkages of smart-city healthcare technologies," in 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 2022.
130. P. Sindhuja, A. Kousalya, N. R. R. Paul, B. Pant, P. Kumar, and D. K. Sharma, "A Novel Technique for Ensembled Learning based on Convolution Neural Network," in 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, 2022, pp. 1087–1091.
131. A. R. B. M. Saleh, S. Venkatasubramanian, N. R. R. Paul, F. I. Maulana, F. Effendy, and D. K. Sharma, "Real-time monitoring system in IoT for achieving sustainability in the agricultural field," in 2022 International Conference on Edge Computing and Applications (ICECAA), 2022.
132. Srinivasa, D. Baliga, N. Devi, D. Verma, P. P. Selvam, and D. K. Sharma, "Identifying lung nodules on MRR connected feature streams for tumor segmentation," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), 2022.
133. C. Goswami, A. Das, K. I. Ogaili, V. K. Verma, V. Singh, and D. K. Sharma, "Device to device communication in 5G network using device-centric resource allocation algorithm," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), 2022.
134. M. Yuvarasu, A. Balaram, S. Chandramohan, and D. K. Sharma, "A Performance Analysis of an Enhanced Graded Precision Localization Algorithm for Wireless Sensor Networks," Cybernetics and Systems, pp. 1–16, 2023.
135. P. P. Dwivedi and D. K. Sharma, "Evaluation and ranking of battery electric vehicles by Shannon's entropy and TOPSIS methods," Math. Comput. Simul., vol. 212, pp. 457–474, 2023.
136. P. P. Dwivedi and D. K. Sharma, "Assessment of Appropriate Renewable Energy Resources for India using Entropy and WASPAS Techniques," Renewable Energy Research and Applications, vol. 5, no. 1, pp. 51–61, 2024.
137. P. P. Dwivedi and D. K. Sharma, "Selection of combat aircraft by using Shannon entropy and VIKOR method," Def. Sci. J., vol. 73, no. 4, pp. 411–419, 2023.

138. L. J, A. Manoj, G. Nanma, and P. Srinivasan, “TP-Detect: trigram-pixel based vulnerability detection for Ethereum smart contracts,” Multimed. Tools Appl., vol. 82, no. 23, pp. 36379–36393, 2023.
139. Lohith, K. Singh, and B. Chakravarthi, “Digital forensic framework for smart contract vulnerabilities using ensemble models,” Multimed. Tools Appl., 2023, Press.
140. Lohith J J and Bharatesh Cahkravarthi S B, “Intensifying the lifetime of Wireless Sensor Network using a centralized energy accumulator node with RF energy transmission,” in 2015 IEEE International Advance Computing Conference (IACC), Bangalore, India, pp. 180-184, 2015.
141. S. Parthasarathy, A. Harikrishnan, G. Narayanan, L. J., and K. Singh, “Secure distributed medical record storage using blockchain and emergency sharing using multi-party computation,” in 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2021.
142. G. Kannan, M. Pattnaik, G. Karthikeyan, Balamurugan, P. J. Augustine, and Lohith, “Managing the supply chain for the crops directed from agricultural fields using blockchains,” in 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, pp. 908-913, 2022.
143. R. Singh et al., “Smart healthcare system with light-weighted blockchain system and deep learning techniques,” Comput. Intell. Neurosci., vol. 2022, pp. 1–13, 2022.
144. J. J. Lohith, A. Abbas, and P. Deepak, “A Review of Attacks on Ad Hoc On Demand Vector (AODV) based Mobile Ad Hoc Networks (MANETS),” International Journal of Emerging Technologies and Innovative Research, vol. 2, no. 5, pp. 1483–1490, 2015.
145. R S Gaayathri, S. S. Rajest, V. K. Nomula, R. Regin, “Bud-D: Enabling Bidirectional Communication with ChatGPT by adding Listening and Speaking Capabilities,” FMDB Transactions on Sustainable Computer Letters., vol. 1, no. 1, pp. 49–63, 2023.
146. V. K. Nomula, R. Steffi, and T. Shynu, “Examining the Far-Reaching Consequences of Advancing Trends in Electrical, Electronics, and Communications Technologies in Diverse Sectors,” FMDB Transactions on Sustainable Energy Sequence, vol. 1, no. 1, pp. 27–37, 2023.
147. P. S. Venkateswaran, F. T. M. Ayasrah, V. K. Nomula, P. Paramasivan, P. Anand, and K. Bogeshwaran, “Applications of artificial intelligence tools in higher education,” in Advances in Business Information Systems and Analytics, IGI Global,USA, pp. 124–136, 2023.
148. R. C. A. Komperla, K. S. Pokkuluri, V. K. Nomula, G. U. Gowri, S. S. Rajest, and J. Rahila, “Revolutionizing biometrics with AI-enhanced X-ray and MRI analysis,” in Advances in Medical Technologies and Clinical Practice, IGI Global, 2024, pp. 1–16.
149. S. S. S. Ramesh, A. Jose, P. R. Samraysh, H. Mulabagala, M. S. Minu, and V. K. Nomula, “Domain generalization and multidimensional approach for brain MRI segmentation using contrastive representation transfer learning algorithm,” in Advances in Medical Technologies and Clinical Practice, IGI Global, 2024, pp. 17–33.