REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

AN IMPROVED IMAGE STEGANOGRAPHY SCHEME BASED ON DEEP LEARNING APPROACH AND QUADRUPLE SECURITY LAYERS

Zinah Khalid Jasim JASIM

Doctor of Philosophy

Supervisor

Assoc. Prof. Dr. Sefer KURNAZ

İstanbul, 2025

AN IMPROVED IMAGE STEGANOGRAPHY SCHEME BASED ON DEEP LEARNING APPROACH AND QUADRUPLE SECURITY LAYERS

Zinah Khalid Jasim JASIM

Electrical and Computer Engineering

Doctor of Philosophy

ALTINBAŞ UNIVERSITY

2025

The dissertation titled AN IMPROVED IMAGE STEGANOGRAPHY SCHEME BASED ON DEEP LEARNING APPROACH AND QUADRUPLE SECURITY LAYERS prepared by ZINAH KHALID JASIM JASIM and submitted on 24/01/2025 has been **accepted unanimously** for the degree of PhD in Electrical and Computer Engineering

_____

Assoc. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Committee Members:

Assoc. Prof. Dr. Sefer KURNAZ	Department of Computer Engineering, Altınbaş University	_____
Prof. Dr. Osman Nuri UÇAN	Department of Electrical-Electronic Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering, İstanbul Arel University	_____
Asst. Prof. Dr. Zeynep ALTAN	Department of Software Engineering, İstanbul Beykent University	_____

I hereby declare that this dissertation meets all format and submission requirements for a PhD thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Zinah Khalid Jasim JASIM

Signature

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me through whole research work as well as my family for always assisting me in my hard time.

PREFACE

First and foremost, I would like to thank my supervisor Assoc. Prof. Dr. Sefer Kurnaz for guiding and helping me along the way in writing this dissertation. Discussing my progress, problems, and ideas with my supervisor. Assoc. Prof. Dr. Sefer Kurnaz has been very helpful several times a week and has been very clear in understanding the logic behind the research.

ABSTRACT

AN IMPROVED IMAGE STEGANOGRAPHY SCHEME BASED ON DEEP LEARNING APPROACH AND QUADRUPLE SECURITY LAYERS

JASIM, Zinah Khalid Jasim

Ph.D., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Assoc. Prof. Dr. Sefer KURNAZ

Date: 01/2025

Pages: 101

This thesis intends a fresh approach for the improvement of dataset secreting in images via the ACO algorithm. Digital image steganography requires a balance between two essential goals: this provides the maximum optimization of the concealment of data; it would also reduce the possibility of the image from existence noticed via optimizing the quality of the original image to be concealed. Many current steganographic methods tend to sacrifice the goals above and below at some point. The thesis introduces the "ACO-LSB" approach, which is designed to enhance embedding capacity using a gray-scale shelter image to hold secret dataset through adding an extra bit-pair in byte (b) to make a checksum of the integrity of the image or a check sum of the hidden message. The method encrypts secret information as the pairs of bits and embeds into the uncompressed images in grey scale. The algorithm used in the ACO is the adaptive scanning to find pixel locations and increase the data embedding capacity while decreasing the strong impact on the image quality. Otherwise, the specific pheromone values are changed in a cyclical fashion to avoid problems with stagnation in the context of the overall optimization process – the values should be ideal for proper selection of pixels. The performance results of the ACO-LSB method are outstanding and this research confirms that they enabled enhancement in the subsequent image embodiment, with up to a 30% increase in embedding capacity compared to traditional methods. Technology achieves an average maximum Peak Signal-to-Noise Ratio (PSNR) of (40.5) dB and Structural Similarity Index (SSIM) of (0.98). Furthermore, Methodology shows strong resistance to detection, reducing detection rates by 20%. The model was

implemented using MATLAB R2023a and tested on a publicly available dataset of 1000 gray-scale pictures, providing strong evidence of its effectiveness.

Keywords: Steganography, Steganalysis, Capacity Optimization, Least Significant Bit, LSB, And Ant Colony Algorithm.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

ACO	:	Ant Colony Optimization
DWT	:	Discrete Wavelet Transform
LSB	:	Least Significant Bit
MSE	:	Mean Square Root
PSNR	:	Peak Signal-to-Noise Ratio
SSIM	:	Structural Similarity Index

1. INTRODUCTION

In the digital age, where information is constantly transmitted across open networks, protecting sensitive data has become a pressing concern. Steganography, an ancient practice of hiding information within seemingly ordinary objects, has evolved into a sophisticated digital technique for embedding confidential information within media files like images, audio, and video. Unlike encryption, which makes data unreadable without a decryption key, steganography seeks to conceal the very existence of the data, making it a valuable tool for secure communication and data storage. It admits that digital steganography has inherent problems especially when it comes to the amount of payload it can hide the cover medium's perceptual quality and its ability to withstand a steganalytic attack [1]. Conventional steganographic approaches, which include the most popular LSB to embed payload, hide information in the lower order bits of pixel intensities [2]. This method is straightforward and provides moderate embedding capacity, but it is often constrained by visual distortions that increase the likelihood of hidden data being detected. Moreover, traditional LSB techniques tend to generate statistical patterns or anomalies that steganalysis tools can identify, thereby compromising the security of hidden communication. Just before tackle these restrictions, academics have explored optimization algorithms to enhance the efficiency and robustness of steganographic methods. This research introduces an innovative approach that combines Ant-Colony-Optimization (ACO) with the Least-Significant-Bit (LSB) technique, referred to as ACO-LSB, to enhance image steganography [3]. The ACO algorithm, stimulated thru the incisive behaviour of ants, uses pheromone-based signalling to identify optimal paths, making it well-suited for complex optimization tasks. In this steganographic application, ACO is employed to select optimal pixels within an image for data embedding, aiming to maximize embedding capacity while maintaining imperceptibility [4]. By carefully selecting pixel positions, the ACO-LSB method reduces detectable patterns and minimizes image degradation, thus augmenting the safety and effectiveness of the steganographic procedure [5]. The objectives of this seek are twofold. First, it seeks to upsurge the entrenching ability of image steganography thru up to 30% equated to out-of-date procedures, enabling the concealment of larger data volumes without compromising image quality [6]. Second, it aims to it focuses on improving resistance to steganalysis by reducing statistical anomalies through optimized pixel selection, which is

critical for secure data transmission. The ACO-LSB method ultimately incorporates data integrity checks to identify and report any unauthorized alterations to the embedded data [7]. To assess the effectiveness of the wished-for approach, the ACO-LSB scheme is pragmatic in the direction of a bulky dataset of gray-scale metaphors, specifically using the BOSSbase1.01 dataset, which is widely utilized in digital forensics and steganography research. With estimating criteria insomuch as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and detection resistance, the study demonstrates the advantages of the ACO-LSB technique in preserving high image quality while providing strong security features [8].This comprehensive evaluation underscores the potential of ACO as an effective optimization tool in steganography and lays the foundation for future advancements in secure multimedia communications. In conclusion, this thesis offers a valuable contribution to the field of image steganography by introducing an improved technique that employs Ant Colony Optimization (ACO) to optimize data embedding. The ACO-LSB method presents a promising avenue for researchers and practitioners seeking secure, high-capacity, and robust steganographic methods popular an progressively extra digital and data-centric area [9].

Given the accelerating frequency of data breaches and the growing threats to personal and organizational data security, there has been a notable rise in attention to steganography, cryptography, and data protection techniques popular contemporary periods [7]. During which encryption safeguards information privacy with changing the involving of the idea existence threw, concealment hides the presence plus content of sensitive material [10]. In the works, encryption procedures alter a note into analogous a way that its prototype intending is hidden commencing an unconstitutional person, with the letter is surreptitiously placed in a seemingly innocent shell (or medium) [11]. Although encryption is applicable in protecting transmission networks, it is restricted since conflicting notes raise suspicions trendy the convictions of hackers that can crush the letter [10].Therefore, the proposed beneficiary could non be able to retrieve the letter [12]. A procedure described cryptanalytics also acts as a counter to encryption plus the endeavour of exposing the private letter, thus deterioration the safety, secrecy, and concealment of the letter [13], it provides stealth technology.

Alternative tier of protection towards improves data defence anti unlawful log on with utilize. Privacy technology is operative trendy safeguarding privacy, reliability and disposal [14] .

Rising rates of cyber espionage and a significant acceleration in data transfer speeds over the Internet have led to an increased focus on data security, leading to increased sharing of digital documents [15, 16]. Data security encompasses the implementation of measures to limit access solely to authorized personnel and safeguard information from illicit modification, viewing, sharing, and access [17]. Data concealment is a defensive strategy that attempts to safeguard information by obfuscating its presence from potential adversaries [18]. However, it is critical to improve this methodology to thwart an adversary's ability to obtain data if concealed information becomes apparent via analytical techniques [19].

Several subfields of security technology are concerned with the preservation of confidential data; cryptanalysis and cryptography stay binary of the utmost essential machineries trendy this regard [20]. categorize the preliminary methodology as the study of secrets, or cryptography. The document includes protocols for encoding and decoding information. The means of renovating ordinary transcript mad about an inaudible arrangement stays established as encryption. It requires the originator to encode the message using an encryption key prior to transmitting it over an unsecured public channel [21]. Reproducing the original message is contingent upon the recipient possessing the decryption key. refer to the process of decrypting encrypted data into ordinary text, which is readily comprehensible and readable [22].

The succeeding procedure is known as cryptography, which grips cloaking a secret letter among the bits of a cover file, making it undetectable. cover file might consist of an appearance, acoustic sleeve, or movie sleeve. Confidential material often replaces unnecessary or insignificant parts in image files [23].

Steganography and cryptography differ in their methods: the latter employs strategies to hide data, whereas cryptography employs techniques to render it incomprehensible [24]. The objective of this inquiry stays on the way to augment statistics protection thru operating steganography procedures on the way to rawhide the records plus reliability boost introduces to detect any changes or variations functioned via intruders [25].

Data has become the most valuable commodity of the contemporary era. Ensuring the security of data from unauthorized listeners and malicious individuals is of utmost importance [26]. Steganography is a method concealing information inside other information trendy insomuch as an avenue that individual sender and recipient can detect continuation of hidden statistics. Audio, video, picture, or text files can conceal confidential information [27]. The term steganography comes from a combination of two ancient Roman words, First steganos and second graphia [28]

The basic principle of image hiding involves using a protect picture to hide a restricted letter. refer to the unique picture file as protect picture and call the image sleeve acquired with the data wallop procedure the cover picture [29]. This model consists of two basic components. The procedures entail the transmitter concealing confidential information in an image and the recipient retrieving this information [30].

This steganographic technique has historically been one of the most impactful methods for concealing information.

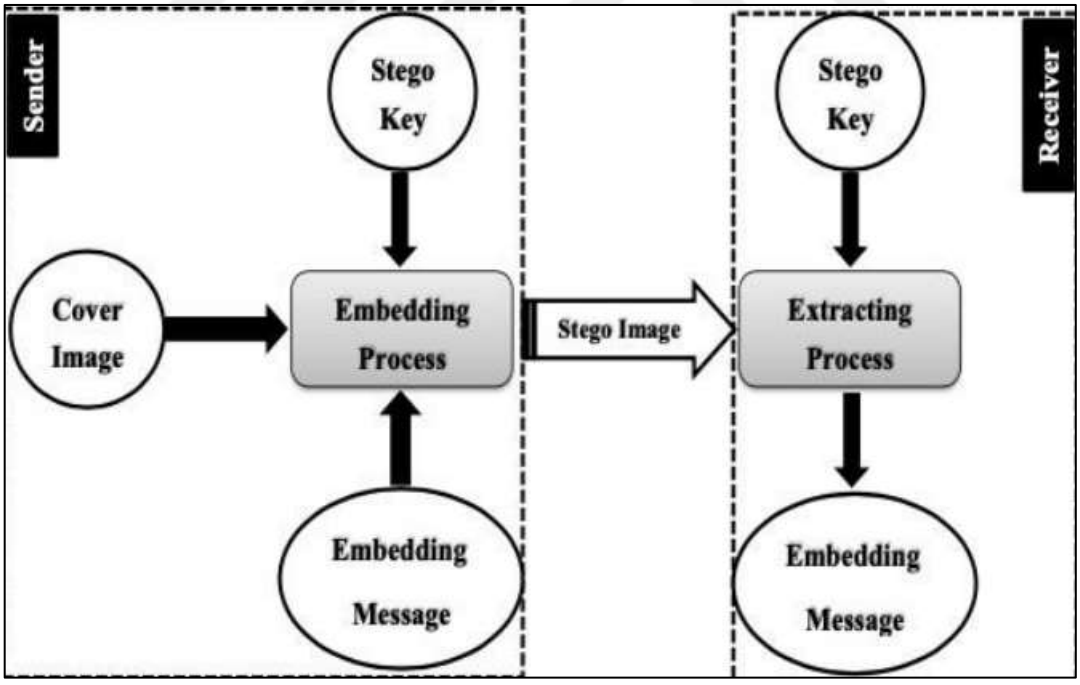

Figure 1.1: Model of Steganography [28] .

Currently, there is genuine necessity to improve steganography methods to securely embed data across various forms of media [31]. Embedding capability and imperceptibility are

crucial characteristics for any steganography software [32]. These two features are related. It is challenging to enhance capacity while preserving imperceptibility.

Studying steganography methods and algorithms presents five obstacles.

a. The size of the payload in secure communication and transmission, managing the amount of information is crucial and often difficult.
b. ensuring the confidentiality of communication.
c. Enhancing peak signal-to-noise ratio (PSNR) and ability to include with reduce. mean square root (MSE).
d. Alterations to cover image can significantly affect steganography techniques, such as filtering and smoothing.
e. maximizing data concealment and maintaining the integrity of the covering medium to minimize detection.

The process of detecting concealed data, identifying suspicious packages, and determining the presence of secret material is known as steganalysis [33]. Steganography offers an advantage over cryptography in terms of its virtually limitless choice of possible media, in contrast to cryptography's limited selection of algorithms and keys [34]. Moreover, since steganography involves both the extraction of the cover data and the analysis of the hidden pattern, the procedure becomes more complex [35]. Although steganography provides good security measures, advanced high-speed calculations, aided by AI automation, can decrypt most of the state of art methods [36]. AI combines ML and DL networks to analyse patterns. This integration blurs the distinction between machine learning, Artificial intelligence, and information security [37]. As a result, an increasing number of businesses are adopting mechanisation afterwards intellectual computation toward boost the success of their confidence instruments [38]. Yet, with brightness comes inevitable darkness. A rerecording to a recent study by ESET, the potential use of AI as a projectile against enterprises partakes controlled to a substantial proportion (75%) of IT conclusion-fabricators in the U.S anticipating an growth fashionable the quantity of attacks they must identify and whereas Figure 1.2 illustrates how the two main fields of information security, cryptography and data concealment, encompass a broad array of subjects. Both fields strive to guarantee security for transmitting data via public networks [39].Through reorganization, cryptography obfuscates the substance of messages. Encrypting communication is not an effective means

of data protection, as hackers can often circumvent encrypted communication [40]. A key drawback of using cryptography to ensure data security is that, despite the use of incomprehensible text, other parties are always aware of the connection [41].

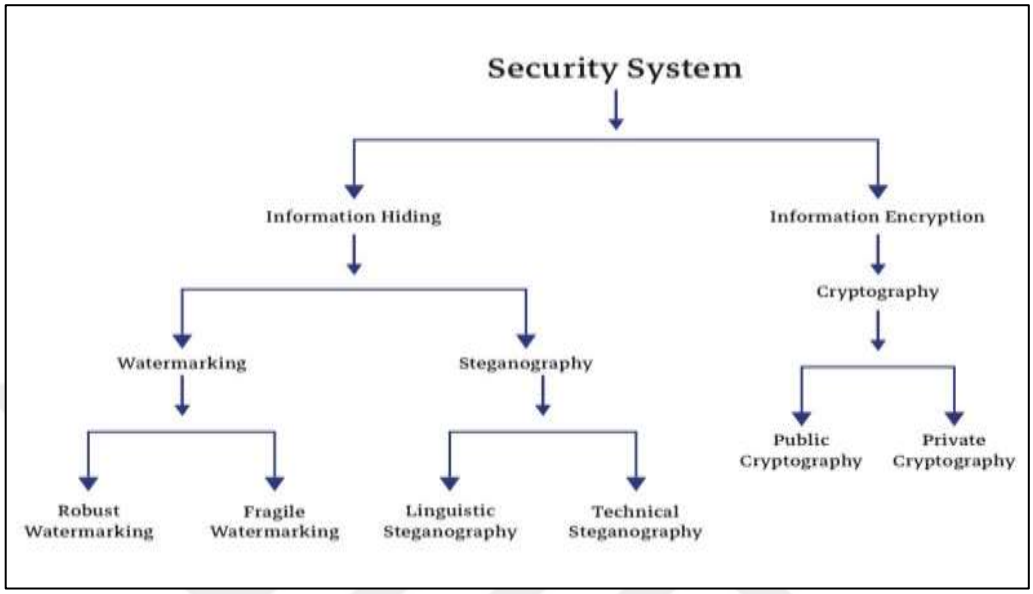

Figure 1.2: Information Security Classification.

1.1 PROBLEM BACKGROUND

The addresses the core challenges in traditional image steganography methods, specifically the difficulty of balancing embedding capacity, image quality, and security. In typical steganographic techniques, such as standard Least Significant Bit (LSB) embedding, data can be hidden within images simply, but there are significant limitations. As the volume of embedded data within an image increase, its visual quality typically deteriorates. This decline in quality heightens the probability that alterations will be detected by either an observer or a detection algorithm, thus elevating the risk of exposure [42].

Another problem associated with conventional LSB-based techniques is the problem of detection. The sequences and patterns these methods adopt while embedding data are distinct and always lead to what statisticians' term as outliers or tracks. Owing to this predictability, security of these methods becomes vulnerable which raise important issues especially for sensitive applications that require high levels of confidentiality and resistance to analytical detection [43]. This means the need for more complicated techniques of optimization cannot be overemphasized. Other approaches present iterative and adaptive techniques with better

rates of pixel selection, such as Ant Colony Optimization (ACO). Applying ACO to overall pattern, the problem of embedding process may be optimized to introduce fewer distortions and to decrease statistical artifacts which may attract attention due to their noticeable irregularities, that increases the likelihood of concealing information [44]. The proposed ACO-LSB technique is designed to overcome these specific challenges, with the goal of improving both the competence likewise protection of picture cryptography whereas sustaining visible attribute [45].

The problem background demonstrates the existing shortcomings in using the conventional image steganography techniques especially in view of, the amount of inserting competence, picture superiority, also confidence. Some of the highest valuable attributes of the problem background occur as follows:

a. Balance Between Capacity and Security: Conventional steganographic procedures, insomuch as standard Least Significant Bit (LSB) embedding, offer ease of use and moderate capacity for data storage. However, enhancing the embedding capacity typically results in visual degradation and the formation of detectable patterns, which spreads the vulnerability of the disappeared information to steganalysis plus safety breaches
b. Vulnerability to Detection and Attacks: Traditional LSB based schemes suffer from the problem of detectability since the pattern of embedding is deterministic or bound to cause statistically distinguishable differences from the original data. These vulnerabilities affect the functionality of hidden communications especially in properly secured applications where detection should be minimal.
c. Requirement for Optimization Techniques: To overcome these challenges, there are optimization algorithms such as Ant Colony Optimization (ACO) needed. Thus, the adaptiveness and the iterative characteristic of ACO can contribute to enhance the selection of the pixels to have a higher embedding efficiency, less visibility of the hidden data, and higher robustness against the steganalysis.

To address this issue, the ACO-LSB method is introduced here as the method to achieve this goal that would increase embedding capacity while at the same time maintaining or even surpassing the superiority of the picture plus reducing probability at which picture is to be detected.

1.2 PROBLEM STATEMENT

The research problem focuses on the limitations imposed by existing embedding methods, which often struggle to balance tall entrenching bulk, security, and picture superiority. Conventional procedures insomuch as LSB substitution are vulnerable to detection and can lead to image degradation. Although methods that include discrete wavelet transform (DWT) or optimization algorithms such as particle swarm optimization (PSO) improve robustness, they still face difficulties in improving modulation capacity without compromising image quality or security. To overcome these challenges, the authors presented a modern approach that chains the ant colony optimization (ACO) algorithm amongst LSB, known as the ACO-LSB method. The goal is to expand push in scope and security, reduce the visibility of embedded data and its detectability through stealth analysis, whilst supporting the property of the cover picture.

1.3 RESEARCH GOAL

This research seeks to develop an improved image steganography technique that enhances both the embedding capacity and security of concealed data. Utilizing the Ant Colony Optimization (ACO) algorithm in conjunction with Least Significant Bit (LSB) embedding, the study aims to enable the embedding of larger data volumes in images with minimal quality loss, while also increasing resistance to detection. This approach is intended to make hidden data more secure and less prone to detection by steganalysis tools, thereby facilitating secure and reliable data transmission.

1.4 RESEARCH OBJECTIVE

The main objectives are:

a. Enhancing Embedding Capacity: The aim of the study is to substantially expansion the dimensions of unseen information that can stay embedded trendy images through the application of the Ant Colony Optimization (ACO) algorithm.
b. Improving Security and Resistance to Detection: By optimizing pixel selection through the Ant Colony Optimization (ACO) algorithm, this method decreases the probability of detection via steg-analysis, thus growing the safekeeping of the unseen information and reducing its vulnerability to statistical and visual detection methods.

c. Preserving Image Quality and Data Integrity: The ACO-LSB method ensures the generation of high-quality stego-images with minimal visual distortion, while incorporating mechanisms to verify data integrity and detect any potential tampering.

1.5 RESEARCH SCOPE

a. Algorithm Development and Enhancement: The subject of the given work is the improvement of picture cryptography thru proposed combined ACO-LSB method to increase the data embedding capacity, security, and image quality.
b. Performance Testing and Evaluation: On the way to authenticate the improvements of the planned technique, it is evaluated using a large database of gray images BOSSbase1.01 by the measures of embedding capacity, PSNR and SSIM, and robustness against detection compared with traditional steganographic methods.
c. Application in Secure Communications: The research in the background of the study corresponds to secure data transmission and storage that can make ACO-LSB steganography to offer serious hidden communication methods that cannot easily be seen or heard during multimedia and sensitive data transfer. It covers technical development in steganography and possibility of employing them in practice in hidden communications for security.

1.6 RESEARCH SIGNIFICANCE

The importance of the research lies in various key areas:

a. Advancing Steganographic Techniques: Altogether the design stands an endeavor to combine the conventional LSB cryptography with the new ACO algorithm making it possible on the way to defeated the limitations of the aforementioned procedures.

b. Improving Security in Digital Communications: The research also improves the effectiveness of the second hidden channel to make it more difficult for any other person to decipher or decipher the insight that has been placed in the materials. It has crucial significance in secure data transfer especially while it extends to information safety and information integrity environment.

c. Contributing to Steganography Research and Applications: The offered ACO-LSB method has shown potential to spur expand the field of steganography and to investigate other optimization algorithms for mounting concatenation data embedding. From this work, improved methods and techniques for safe and successful hiding of data could be developed across several disciplines including computer security, multimedia communication and digital forensics.

All in all, the above research offers a significant contribution to theoretical development in and practical realization of secure and covert data communications.

1.7 CONTRIBUTIONS

The key contributions are:

a. Development of an ACO-LSB Steganography Method: This article is designed to introduce a novel strategy for applying the ACO algorithm in conjunction with LSB Steganography and to expand the coverage density of data hiding level and the superiority of the picture used, increased entrenching ability can make the ACO-LSB method thirty percent larger than other methods which do not utilize this system.

b. Enhanced Detection Resistance: When applying ACO in selecting pixels, more random embedding pattern are produced – in the same manner it increases hidden ability to resist steganalyse. In doing so, it reduces the impact of statistical variations that other LSB techniques offer and thereby improving the security aspects as the information hidden becomes far less distinguishable.

c. Improved Data Integrity Verification: Checksums and decoy bit pairs, for instance, are incorporated into the article in an attempt to enhance the data integrity checks. All these elements help in the early detection of any change or an attack on the hidden data making the data more secure and reliable which is transmitted.

d. Comprehensive Evaluation of Grayscale Images: To ensure that the concept of the proposed ACO-LSB is workable, a number of experiments is conducted on a large set of grayscale image called BOSSbase1.01 and the result compared to those obtained using the simple LSB method and results in far better outcome in terms of PSNR, SSIM and

purposely incorporated detection resistance. They have Appreciate this method and describing the simplicity, the efficiency as well as the viability of the method for use in further implementation in real secure communication.

1.8 MOTIVATION

The reason for this research is based on the weaknesses of regular image steganography algorithms which, in most cases, could not optimally provide large capacity, good quality image, and security. Conventional methods such as simple LSB embedding where the data is encoded in a seemingly arbitrary manner as evident by predictable patterns, and statistical deviation make the data vulnerable to detection hence reducing data security. As with the continued advancement of threat to the content and importance of encrypted message to meet rightful demands, there is a powerful need for steganographic techniques which can hide greater measures of message without being detected. This study utilizes the adaption and optimization of Ant Colony Optimization (ACO) in response to these challenges to produce a high capacity, secure, and robust steganography solution.

1.9 RESEARCH QUESTION

In what ways could image steganography be improved to maximize data embedding capacity along with security and minimal detectability? More precisely, it aims to establish if and how the proposed combining of the Ant Colony Optimization (ACO) algorithm with Least Significant Bit (LSB) technique can enhance the selection of the pixels for data embedding to make it possible to increase the size and, thus, enhance the security of the hidden information while minimizing the impact on the visual quality and the detectability of the data. This question leads to the consideration of how ACO-LSB can avoid the problems that some traditional steganographic approaches imply.

1.10 THESIS ORGANIZATION

The Dissertation is consolidated as arises:

Introduction: To orient the reader on the issues and limitations of prior art in ISM, this section provides a brief background on the capacity, security, and deterministic detectability constraints of conventional ISM. It also gives potential remedy in the shape of proposed ACO-LSB solution technique.

Methodology: In the article the authors present the ACO-LSB approach and indicate in what way ACO is utilized to improve picture element collection for information hiding. These are the techniques of embedding and extraction and the performance measures used in steganography, and the check for the steganography security added to the process.

Results and Discussion: Within this part overall, tentative setup is explained as well as results of the method ACO-LSB applied on a set of grey-tone images has been put forwarded. The improvement in performance is then analysed by calculating the PSNR, SSIM and the detection resistance to validate the technique proposed.

Conclusion: The final part introduces the general conclusion of the research with a special emphasis on capacity, security, and non-detectability advancements. It also provides the opportunity for future research to enhance the computational effectiveness of the work described and discuss the possibility of using a combination of the analysed approaches. It has the structure of doing so that every aspect within the research which include the background, and the method used, the findings and the implications are well addressed.

2. LITERATURE REVIEW

2.1 INTRODUCTION TO STEGANOGRAPHY

Steganographic is the ability of covering messages that are in most instances only understood by the person doing the signalling and the receiver. The term steganography, which originally referred to hidden writing, has its roots in the Greek language. The period steganography stays a amalgamation of the confrontations writing or graphy besides secret or covered, which refers to the act of concealing hidden communications in a desired location[46]. Steganography is a term that incorporates a variety of explanations; however, its fundamental concept is the concealment of sensitive or classified information beneath a different form of media, such an image, a video file, text, or audio [47]. Steganography technology's primary goal is to prevent the transfer of confidential information from drawing attention. Uncertainty in the document's contents reduces the likelihood of effectively concealing a secret within it. An observer will try to reveal hidden information if they notice a change in the sent document [48].

Image steganography has gained popularity recently [49]. picture take convert vital media for hiding clandestine letters exclusive of varying pictorial structures plus/or else individualities. So a consequence, picture are widely used in stealth owing on the way to the mark of termination related beside them[50]. Completely picture folder structures are fitting for stealth [51]. Folder structure varieties involving TIFF, JPEG, PNG, GIF and BMP are suitable for utilize [14]. It should be noted that individually picture information arrangement must its own returns plus difficulties whilst used on behalf of confidential reasons. Because picture element principles stay used on behalf of cryptography on images, there are sometimes differences fashionable picture element amounts concerning the fundamental overlay plus hidden picture [52]. However, the intensity difference is so subtle that the situation stays unnoticeable and imperceptible to the individual visible structure [53].

The similarity of images used in disinformation has made images vulnerable to many targeted cyberattacks, embracing graphic coupled with arithmetic disinformation occurrences [54]. These incidents can detect hidden messages in images using spoofing algorithms. Statistical confounding capabilities to reveal veiled information trendy picture involve hidden data exposure, descent, adaptation, and demolition [55]. Instruments plus

practises utilized intended for such facilities consist of lossy firmness, denoising, picture heightening procedures, picture guesstimate procedures, besides geometric transformation [49]. These instruments besides procedures interpretation visual spoofing defencelessness in digital landscape images, making images prime targets for cybercriminals.

picture steganography procedures trinity foremost conventional procedures (i.e. longitudinal field, renovation field, and adaptive field) for information entrenching [56]. It includes a spatial domain approach. Directly embedding confidential communication obsessed by the picture element principles of the image. This approximate includes Many techniques involving the LSB inserting procedure [57]. Quantization-based procedures, histogram-based procedures [58], prediction error [59], Structure methods also exhibit various additional varieties. Spatial area systems require exceptional responsive quality, minimal change effects, and high variation capabilities. Conversely, the spatial realm becomes less robust, rendering it prey to mobility and many types of assaults. [53]. Steganography technology works to hide data, within other data known only to sender and receiver. Scientific steganography in stems via the Latin words "steganography," meaning "permitted," as well as "diagram," meaning "to create." Our voices shall regard this information as the letter, and the container we shall also refer to as the container [60].

2.2 RELATED WORK

Current analyses concentrate on particular aspects of mathematical picture steganography, hence constraining the applicability of strategies designed to counteract the mathematical examination of steganography. For example, Hussain et al. [61] Provided a comprehensive description of empirical picture steganography, emphasizing geographic domain methodologies. The research emphasizes novel methodologies within the geographical realm known as statistical picture steganography, encompassing problems along with tendencies. Girdhar and Kumar [62] Additionally, an introduction to mathematical steganography strategies utilizing 3D pictures was offered. Multiple 3D area methodologies look at.

Incorporating topological, location, and symbolic areas while assessing each based on cargo, threat opposition; as well as the inverse. Reviewed by Meng et al. [63], Probabilistic image steganography method utilizing an in-depth training system. Diverse advanced machine

learning algorithms have been researched as well as analyzed. The artificial intelligence techniques employed for concealing concealed knowledge, mathematical incidents, and hydrostacks are thoroughly examined while explained. Chen et al [64] Thoroughly examined steganographic procedures applied to unaltered photos. The study presented a comprehensive analysis of the diverse methodologies in addition tactics employed in covered picture confidentiality, underscored current advancements in the domain, until determined that exposed photo protection demonstrates robustness despite subtle assaults. Botto et al [65] Additionally, they concentrated their study on opposite picture steganography methodologies. The investigated procedures including methodologies encompassed value of the pixels inequality, distribution modification, echo-based steganography, accessible essential cryptography, prediction-based approaches, additionally visual extraction processes.

Khan S et al [66], The Ant Colony Optimization (ACO) technique serves as the foundation for detecting intricate areas beneath a specified header photo. Upon identifying such locations, the process employs a minimum major bit (LSB) substitute mechanism to individually inlay obscured details within every one in such intricate areas. The Ant Colony Optimization technique. Develops an odor a structure derived from the behavior of mimicked insects, influenced through specific fluctuations in pixels strength. This approach allows hiding secret information in the main image by using corresponding message bits to replace the least significant pixel bits in complex regions.

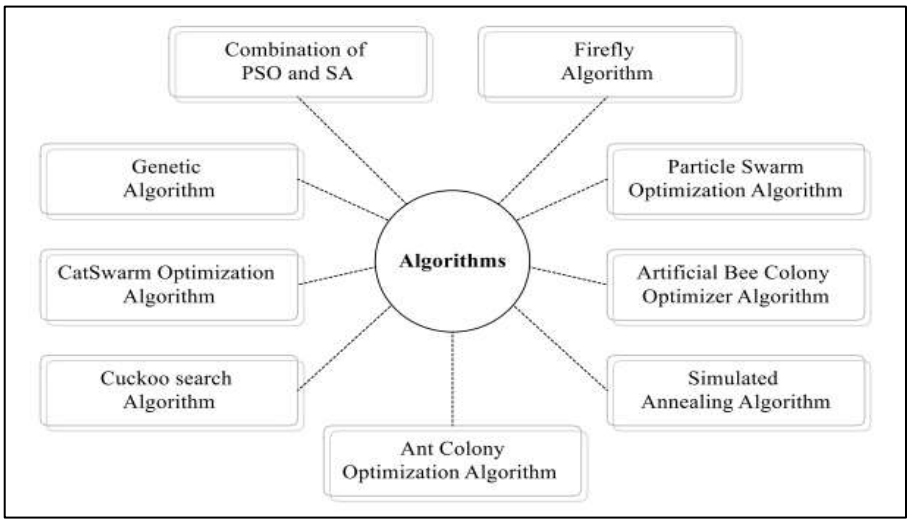

Figure 2.1: The Steganogamic That has been Incorporated in the Steganography of Images.

Loukhaoukha K et al [67] focuses on analysing the watermarked results where LWT, MO-ACO and SVD are used. This integration utilizes ACO engineering to enhance the conveying procedure of the watermark as a way of enhancing the transparency level as well as durability of the conveyed watermark. Accompanying ACO with LWT and SVD guarantees that the watermark information is well concealed in the image and also immune to any adversaries. This study subtly demonstrates how the introduction of ACO improves watermarking results while reducing the probability of false positive watermarks.

Banharnsakun A et al [68] This program is built on the Artificial Bee Colony optimization to solve block allocation in complex synthetic optimization problem. This novel technology also experiences noise attacks in the resultant storage image. In more detail, every segment of the main picture fits into a segment of the second picture with the help of permutations technology. This transfer, the method of transferring of the hidden image will remain inconclusive unless the exact order is known. The enhancement algorithm, known as the ABC algorithm, brilliantly and intelligently perform this optimization to safely and powerfully hide messages in noise and fortify the method against menace. The applicability of the ecological approaches such as ACO and ABC are also illustrated by their integration to the repository.

Walia et al [69], a novel stealth mechanism was illustrated, which has used cuckoo search optimization to eliminate the simplistic flaws in LSB security. Unlike the straight-forward technique of steganography where secret messages are directly embedded, this method incorporates security bearing in mind the associated issues of transmission over public channels. In order to enhance the safety of the approach, secret images are encrypted by using randomly generated chaotic maps before being discretely embedded. This encryption increases the domain of the key for the hidden image and is immune from visual degradation though can be protected from RC4 cryptanalysis attacks that are common in other hide-and-seek algorithms. These algorithms give the researchers and practitioners to build a new and more capable steganography for privacy, and perfect pictures. Such improvements as integration of natural process and wave dynamism and other can be considered as improvements and developments in steganography because they signal yet better ways of hiding information. Thus, an improved steganography scheme is proposed and, utilizing the

cuckoo search method, the drawbacks of LSB are eliminated. Unlike the encryption approach, this stance is secure because it understands the issues that pertain message broadcast. It does not increase security it is decrypting the secret images and randomly generated chaos card before making an escape. This decryption process adds more critical position of the steganographic image as the presence of the effect tougher to be attacked with cryptanalysis techniques attack but simultaneously its effect is shielded with damages visually. Pandey HM et al [70] Since medical data is considered sensitive, the researchers have applied the generalized algorithms (GA) for purposes of security in the exchange of medical data. Of this type of encryption, it offers protection for the data and offers the means through which data can be disclosed and made available only for use by those who have the right to use the data being exchanged, in a secure manner. This research depicts the increasing inclination of researchers to SIG BIO inspired optimization techniques such as WORM search, Genetic Engineering Technique and Path Clustering in solving issues of confidentiality and data security. This way, through studying new technologies and algorithms, one can construct Operational and durable patterns for encryption and information transfer, For medical information interchange and security of numerous assets, as well. The combination of the chaos map and privacy increases the database security against both general and censorship attacks. More advanced aspects of bioinspired technologies can expand the arsenal of solutions needed for further development of fuzzing science in the context of safe and secure communication during Computer Science. Javadpour A et al [71] The noisy water system is enhanced utilizing a synergy of SAPSO with QWT. This method seeks for the ideal equilibrium amongst confidentiality goals, including openness along with vagueness, around the efficacy throughout resilience of the watermarking procedure. The endurance of each suggested strategy is evaluated across various information transformation techniques as well as discrepancy attacks.

S. Yin et al [72]Conventional healthcare picture identification procedures pose difficulties because of the extensive quantity of information including colour duplication. Simulated annealing (SA) and particle swarm optimization (PSO) are integrated to develop an effective dynamic stochastic approach to vital flow formation. The result serves to obscure the graphic, while the histogram of the cropped image is calibrated across various assaults to enhance confidentiality for healthcare picture hiding.

2.3 ANT COLONY ALGORITHM OPTIMIZATION

The Ant Colony Optimization (ACO) algorithm is inspired by the natural foraging behaviour of ants. In nature, ants leave pheromone trails along paths to food sources. Over time, shorter paths accumulate more pheromones, as they are travelled more frequently, guiding other ants toward these optimal routes.

In the ACO algorithm, artificial "ants" explore a solution space to find the shortest or best paths using pheromone trails and heuristic information. These artificial ants deposit virtual pheromones on promising paths, influencing the choices of subsequent ants. This cycle makes it possible for the algorithm to learn the best solutions to routes based on positive feedback, pheromone reinforcement, and negative feedback, pheromone evaporation. The basic ACO has developed into Multiple Objective ACO (MOACO) to solve several objective functions where one function may be against the other such as cost, performance and efficiency. It is noted that a MOACO maintains a range of Pareto optimal solutions that allows objectives to be traded off against one another [73]. This approach involves several pheromone trials for a range of purposes and applies other methods, like weighted sum or Pareto optimality, for the assessment of solutions. The Ant Colony Optimization (ACO) is a modern probabilistic technique for solving complex computational optimization problems derived from the natural foraging behavior of the ants. It mimics how ants plan working paths to get a food source [74]. The ants that go to scout for food at distant places mark the trail through chemical secretions which are deposited in higher concentrations when the ants successfully react to the signals from the nest and move along that chemical trail back to the nest. This gives the idea of a natural solution and finding of the shortest path from one point to another, for instance from the nest to a source of food as an example, this is an incredible natural way of solving problems and optimizing methods [75]. Component-based reasoning is consistent with the indicated natural approach and enhances it with ACO as a strong computational procedure. The basic idea of ACO algorithm is to simulate the process of stigmergy of ant colonies optimization in search of the best solution to an optimization problem by invoking a group of artificial ants that locate possible solutions and modify and improve the search by reinforcing some form of pheromonal communication that represents probable solution paths [75]. It therefore clearly brings out ACO's strength of adaptability and identifying optimum solution where there is WI and WO environment. It is this kind of

flexibility that mimics real ant behaviour that shift their course in reaction to some changes in the environment via barriers that may have been dropped in front of them. ACO is most favourable for solving a wide spectrum of optimization problems, including the problems related to routing and logistics, scheduling, and networks. Furthermore, as in an ant colony each of the artificial ants in ACO is an independent unit while working together to provide the final solution. This feature improves the stability of the algorithm and enables the expansion of the model, a property fundamental for solving large-scale optimization problems. ACO is a general algorithm of six steps and each of those steps will be described in the subsequent sections [76]. However, it must be noted that the explanation here results from the direct solving of the algorithm to the Traveling Salesman Problem [77].

Step 1: Parameter Initialization

This is the initial phase where configuration of many important fixed parameters that are necessary to run the ACO algorithm are determined. These include They include the size of the colony (N); maximum number of iterations (MaxItr); and rate of pheromone evaporation (ρ); and finally, the parameters regarding the pheromone level and desirability (α and β, respectively).

Step 2: Constructing the Pheromone Matrix

To mimic the pheromone action, a matrix of pheromone quantity related to each edge is designed. The τ matrix given by Equation 8 holds this pheromone matrix and has dimensions of v × v that scales up to the full size of the vertices. For example, $\tau_{1,2}$ stands for the amount of pheromone which appeared on the edge of the first and the seconvertices.

$$\tau = \begin{bmatrix} \tau_{1,1} & \tau_{1,2} & \cdots & \tau_{1,v} \\ \tau_{2,1} & \tau_{2,2} & \cdots & \tau_{2,v} \\ \vdots & \cdots & \cdots & \cdots \\ \tau_{v,1} & \tau_{v,2} & \cdots & \tau_{v,v} \end{bmatrix} \quad (2.1)$$

The set of matrix entries are computed using Formula 9, wherein ρ represents the vaporization percentage, alongside i as well as j denote the intersections of connections for $i = 1, 2 \ldots v$ along with $j = 1, 2 \ldots v$. Additionally, $\Delta\tau_{ki,j}$ indicates the quantity of fragrance deposited upon by the kth ant on edge i, j.

Additionally, to get the whole quantity, we aggregate the fragrance sprayed on cutting-edge i, j via every ants between k = 1 to N, whereby N denotes the total quantity of ants in the colony.

$$\tau_{ij} = (1-\rho)\tau_{ij} + \sum_k \Delta\tau_{ij}^k \quad (2.2)$$

Step 3:

Supply remedies (establish a community) By light of the issue, N answers have been created as pathways, wherein probabilities influence the selection of one option against another. Consequently, the possible outcome for selecting edge i,j is computed below:

$$p_{ij} = \frac{(\tau_{ij}^{\alpha})(\eta^{\beta}{}_{ij})}{\sum(\tau_{ij}^{\alpha})(\eta^{\beta}{}_{ij})} \quad (2.3)$$

Step 4:

Measure the Fitness Value: The expense with any remedy has been assessed by a fitness function (impartial variable).

Step 5:

Determine the Optimal Solution (the Queen Ant): Under light of the expense associated with any approach, especially because this is a reductive optimized issue, a reduced consumed ratio signifies a superior strategy. Consequently, the treatment without the minimal cost is referred by the term the royal ant answer.

Step 6:

Assess the Determination Criteria: Steps 2 through 5 are reiterated recursively til the dismissal criteria gets fulfilled. This stage could entail a specific amount of revisions, which upon convergence to the queen ant, the resultant answer is derived as the ultimate fix to this issue..

Procedure: The Phases of Ant Colony Improvement

1: Input: Problem-specific parameters

2: Output: Optimal or near-optimal solution

3: Step 1: Initialization of Parameters

4: Define the quantity for ants N, the upper limit of repetitions $MaxItr$, plus an amount for vaporization ρ.

5: Define the pheromone influence factor α and the heuristic influence factor β.

6: Initialize the pheromone matrix τ with initial values.

7: while the termination condition is not met do

8: Step 2: Update Pheromone Matrix

9: Update τ according to the pheromone update rule.

10: Step 3: Solution Construction (Colony Formation)

11: for each ant k=1k=1 to NN do

12: Construct a solution based on the pheromone levels and heuristic information.

13: end for

14: Step 4: Fitness Evaluation

15: for each ant k=1k=1 to NN do

16: Evaluate the solution using the objective function.

17: end for

18: Step 5: Identify the Best Solution

19: Identify the solution with the highest objective function value.

20: Update pheromone levels based on the quality of the solutions.

21: Step 6: Termination Condition Check

22: If the maximum number of iterations is reached or another stopping criterion is satisfied, terminate.

23: end while

24: return the best solution found

2.4 PHEROMONE MATRIX

A Pheromone Matrix refers to a data structure used in certain algorithms, such as ant colony optimization, to store information about the concentration of pheromones on different edges or paths. It is updated through two processes, pheromone evaporation and pheromone deposition, where the latter can be challenging due to potential conflicts when multiple ants

attempt to deposit pheromones on the same edge simultaneously. The fragrance refresh comprises 2 phases: fragrance dissipation as well as fragrance implantation. Dopamine ablation involves fundamentally a process for the vector modification, making it manageable [78]. Nonetheless, the simultaneous perfume dumping by various ants over an identical surface presents a challenge [79]. Fragrance implantation allows for immediately executed via tiny operations so as to avoid ethnicity situations during accessibility within the fragrance array. Although the utilization of tiny actions appears to reduce speed, empirical from experiments indicated which the simplistic tiny instruction-based simultaneous execution surpasses the suggested intricate chemical-free method [80].

A system of data employed in specific methods, including ant colony optimization, to retain statistics regarding the quantity of fragrances across distinct edges or pathways. Employing fragrances for guiding movement during the ant colony algorithm, execute the procedure for many iterations as well utilize the outcomes of the preceding iteration to inform the movement strategy in the latest iteration, hence minimizing duplicated spreading [77].

LSB is a widely used steganographic technique in which data is embedded in the least significant bits of pixel values [81]. ACO is combined with LSB embedding to strategically select pixels that allow higher data capacity and improved security without degrading visual quality.

Least Significant Bit (LSB) embedding is one of the simplest and most commonly used techniques in image steganography. It involves hiding information in the least significant bits of pixel values within an image. In an 8-bit grayscale or color image, each pixel's intensity or color value is represented by a sequence of bits (typically 8 bits per color channel). By altering the least significant bit(s) of each pixel, data can be embedded with minimal change to the overall appearance of the image, making the hidden information less detectable to the human eye [80].

2.5 DETAILED WORKING OF LSB EMBEDDING

a. Pixel Representation: In an 8-bit grayscale image, each pixel is represented by an 8-bit binary value, ranging from 0 to 255. In color images, each pixel has three channels (red, green, and blue), each represented by 8 bits, giving a total of 24 bits per pixel [82].

b. Least Significant Bit Selection: The least significant bit is the smallest binary digit in the pixel's binary representation. Changing this bit has the least impact on the pixel's intensity or color. For example:

   i. Original pixel value in binary: 10110101 (181 in decimal)

   ii. If we change the LSB (the last bit) from 1 to 0, it becomes 10110100 (180 in decimal)

The difference is so small (1 out of 255) that it's visually undetectable in most cases.

a. Data Encoding Process:

   i. Binary Conversion: The data to be hidden, such as a text or an image, is first converted into a binary sequence.

   ii. Bit Replacement: Each bit from the binary sequence is embedded into the LSB of a pixel in the cover image. For an 8-bit grayscale image, only one bit per pixel is altered; for a 24-bit color image, up to three bits (one per color channel) can be modified per pixel.

   iii. Sequential or Patterned Embedding: The bits can be embedded sequentially in each pixel or according to a predetermined pattern, depending on the desired security and resistance to steganalysis.

b. Embedding Capacity: The capacity of LSB embedding depends on the number of bits changed in each pixel and the size of the image. For example:

   i. In a 512x512 grayscale image (262,144 pixels), embedding one bit per pixel allows for hiding approximately 262 KB of data.

   ii. In color images, the capacity triples if one LSB per color channel is used, allowing up to 786 KB of data in the same image size.

c. Data Extraction: During extraction, the embedded information can be retrieved by reading the least significant bits of each pixel in the same sequence or pattern used during embedding. The LSBs are extracted and reconstructed to retrieve the original binary data, which can then be decoded back into its original form[83].

Example of LSB Embedding in a Grayscale Image

Suppose we want to hide the character "A" (ASCII value 65, binary 01000001) in the first eight pixels of a grayscale image. Here's how it would look:

a. Original pixel values (in binary): 11001000, 10101101, 11100011, 11011100, 10100111, 10011001, 10111011, 11010010

b. Data to embed: 01000001

c. After embedding LSBs: 11001000, 10101100, 11100010, 11011100, 10100110, 10011000, 10111010, 11010011

In this case, only the LSBs were modified, resulting in visually imperceptible changes.

2.6 ADVANTAGES OF LSB EMBEDDING

a. Simplicity: LSB embedding is straightforward and computationally inexpensive, making it suitable for real-time applications.

b. High Capacity: It offers significant embedding capacity, especially in color images, without noticeable visual distortion.

c. Low Detectability: LSB embedding is less visible since small changes in the pixel intensities are hardly visible.

2.7 LIMITATIONS OF LSB EMBEDDING

a. Vulnerability to Steganalysis: Unfortunately, the LSB embedding is easily recognizable by statistical steganalysis since the LSB change can produce patterns or disturbances.

b. Sensitivity to Image Processing: LSB-embedded data can be easily lost by image processing operations such as, compression, resizing or noise addition, etc., because these may change the pixel values.

c. Limited Security: Since the LSB pattern is predictable, it lacks robustness against attacks unless combined with other techniques like encryption or adaptive embedding.

2.8 ENHANCEMENTS TO LSB EMBEDDING

To overcome the shortcomings, LSB embedding can be integrated with optimization algorithms (as in the case of ACO) or can be used in the adaptive process where LSBs of only those pixels are selected for embedding based on the nature of the image [29]. This may enhance the method ability on resisting to the process of detection and retain the image quality of the method. The proposed ACO-LSB steganography technique is comprised of the following major steps that has enabled high level data embedding security and data integrity. These components include:

a. ACO-LSB Embedding Algorithm: This is the core component where the Ant Colony Optimization (ACO) algorithm is combined with the Least Significant Bit (LSB) embedding technique. ACO algorithm is employed to select the appropriate pixels, to enable data embedding with high capacity and include enhanced security by minimizing noticeable patterns. In this process information to be hidden is inserted into the microscopic part of given grayscale cover image.
b. Data Integrity Verification (Checksum and Decoy Bits): This is done to guarantee the accuracy of the embedded data and hence the method contains a checksum value and decoy bit pairs. Checksum values generated prior to the embedding process of the original host data are saved into the stego image. While extraction, the checksum is again calculated with reference to which it will be contrasted to ensure that the data has not been altered in any way. Moreover, dummy bit pairs are also incorporated along with the information bits and through comparison of the differences in the encoded pairs, identify interference.
c. Image Quality and Detection Resistance Metrics: The method incorporates image quality assessment metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) to measure how well the steganographic image maintains the quality of the visuals after embedding. These metrics contribute to achieving a near-optimal number of bits for data capacity and security within the P2P, while the Steganography's payload information remains hidden within the P2P and is highly immune to steganalysis.
d. Data Extraction and Validation Module: This component involves extraction of hidden data from the stego image and checking on the data integrity. Applying ACO-

guided extraction, this module extracts the data, and the values of checksums and decoy bits coupled with them. The module then compares with the original checksum to validate integrity as well as utilize the decoy bit pairs to assess each extracted bit for integrity.

e. These components work in concert to achieve a high-capacity, secure, and quality-preserving steganography method that effectively hides data while protecting it against detection and tampering.

Steganography systems are composed of the following fundamental components: To perform steganography, a key and two data samples specifically, a cover and a message are required.

a. Cover message: A cover is the element that obscures sensitive information. By employing a methodical approach to cover selection, one can augment the efficacy of steganography while simultaneously heightening the challenge of deciphering the concealed data. The data is merely concealed using steganography, unless hybrid methods combining steganography with, and encryption are employed. However, the modification of the data occurs during the encryption process. This is the case because a hacker or intruder may expose the data if they learn about it. A multitude of cover types including text, image, video, and audio influence the steganography procedure.

b. Secret message: To ensure accurate concealment, the message must possess the ability to precisely fit within the designated area. In image steganography pixel, count in cover image and hidden message, image may be identical. We present an illustration of the fundamental steganographic paradigm below.

c. Key: Steganography may entail the use of covers, messages, secret keys, embedding keys, and other components. It is utilized to control access to hidden information.

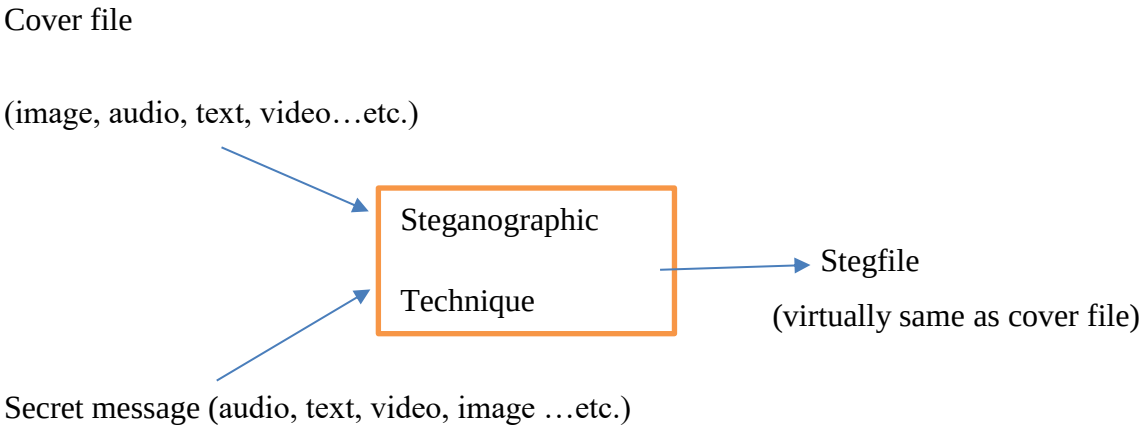

Figure 2.2: Basic Steganography Model.

The decoding formula consists of covers, messages, and secret keys and is responsible for extracting the message via the embedded key[84]. The following components are described: steganography key, steganography message, covert object, and embedded data.

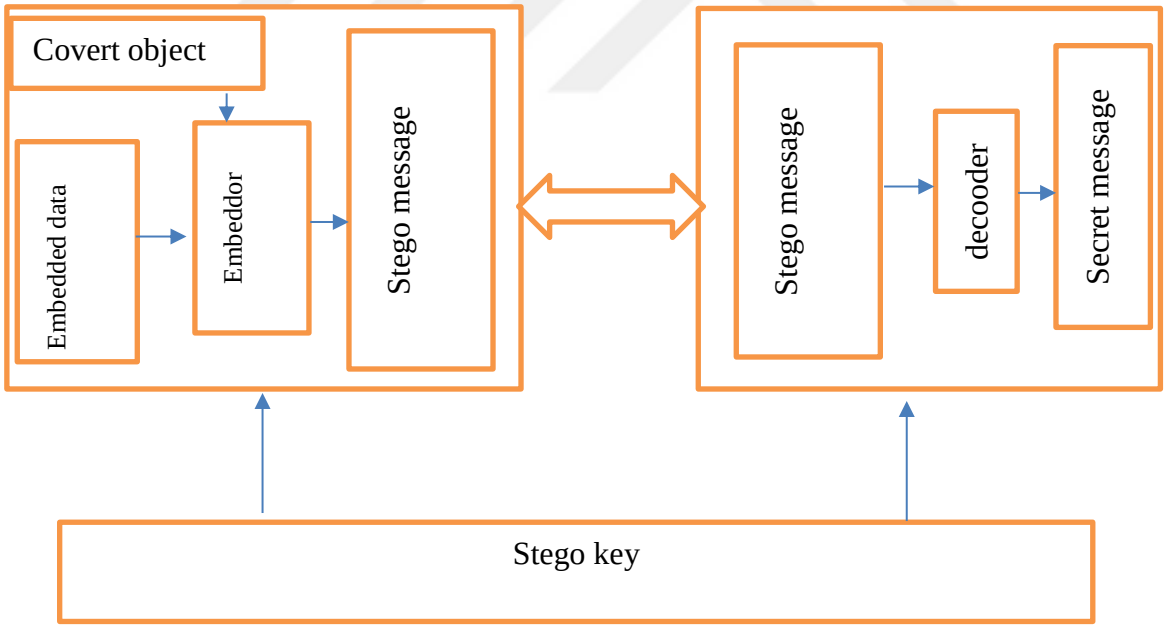

Figure 2.3: Terminology Utilized in Steganography Fundamentals.

Describes the fundamental processes of steganography. The steganography key will encrypt the data within the image[85]. use a medium to transmit this image. The recipient must obtain the covered data using the steganography key. This image serves as the medium in and of

itself. We can codify the following statement as an equation. The steganography message is composed of a key, a cover, and a message.

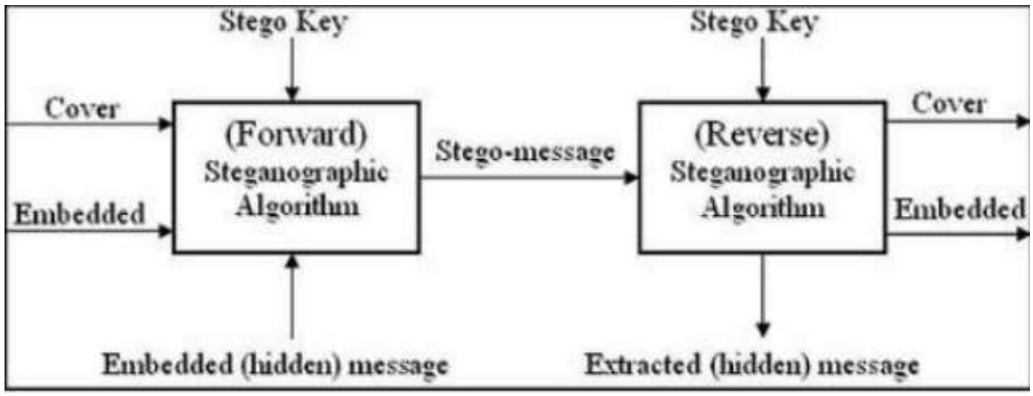

Figure 2.4: General Steganography.

2.9 STEGANOGRAPHY SYSTEM SCENARIO

Steganography System Scenario how data can be securely hidden within images and transmitted without detection[86]. This scenario outlines the complete process of embedding, transmitting, and extracting hidden information within a digital image while maintaining data integrity and security.

The system scenario includes:

a. Data Embedding: The article explain that how hidden data were put into the grey scale image using a new approach ACO-LSB (Ant Colony Optimization-Least Significant Bit). This embedding process accord the best pixel positions for hiding data The goal is to maximize that hiding capacity and minimize the discrepancies that may indicate that data is hiding.

b. Transmission and Storage: Subsequent to the embedding of the data, the ‘stego image’ (actual image containing the hidden data) is then forwarded for transmission or storage. The system scenario considers potential threats during this phase, such as unauthorized access or image manipulation. Meaningful checksums and decoy bits are used with the aim of validating integrity in a transmission process.

c. Data Extraction and Integrity Verification: At the last stage of the contemplated scenario the embedded data is at some point extracted from the stego image. The data’s validity is checked by the extraction module whereby the checksum is recalculated and the

changes indicated by the presence of the decoy bit pairs are identified[87]. This means all that we extract is exactly 100 percent of the original data without any contamination.

Thus, each of the above phases is captured in the steganography system scenario described here however, specific focus is on the embedding of the speech signal, its secure transmission and extraction; advantageous features include high capacity, good image quality, and data protection.

a. Embedding algorithm: This method is used widely to hide important information in the framework of the steganography of the cover message.

b. Retrieving algorithm: The process involves removing hidden information from Stego file.

The sender must initially select a suitable message carrier, such (an image, video, an audio, or a text), before beginning the concealment procedure in a steganography system. Subsequently, the sender is required to select a secure password and select efficient secret messages, both of which the recipient is presumed to be aware of The choice of an appropriate and effective steganography algorithm is critical for encoding the message in a way that improves security[86]. Subsequently, the sender has the option to disseminate the Stego file via email, messaging, or other contemporary methods. The term Stego file refers to a cover document that holds confidential information[88]. After receiving the message, the recipient can decode it using the extraction technique and the sender's password.

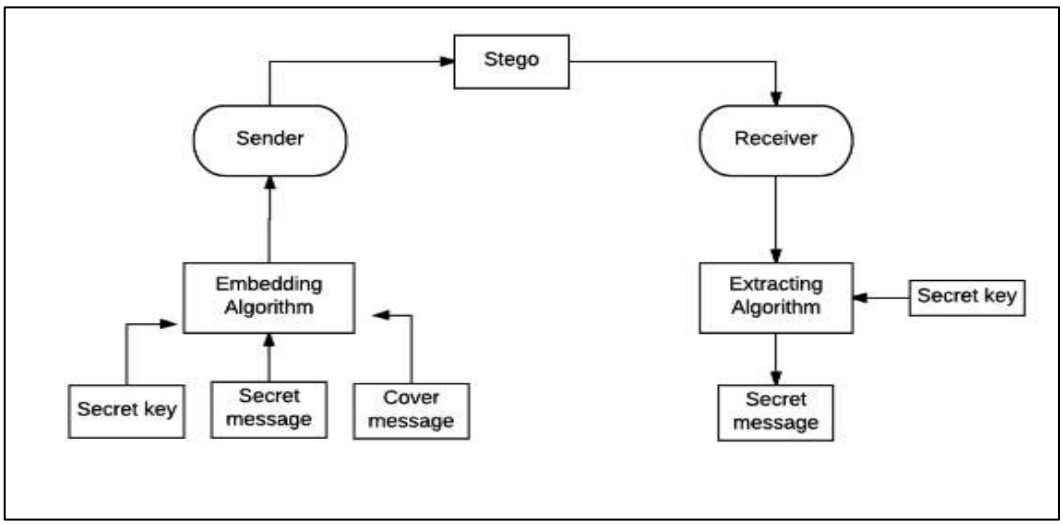

Figure 2.5: Stealth System, Scenario.

2.10 ATTACKS USING STATISTICAL STEGANALYSIS

Privacy analysis approaches deconstruct the defensive features of a technique known as via spotting concealed conversations inside photos to figure out the content along with evaluate its scope or quantity. Steganography of secret images has become significant for concealing sensitive material including analyzing such photos. It seems to function as a safeguards. Photo stereoscopic investigation employs digital imaging practices including cropping, filtering, along with blurring for revealing concealed stuff..

Internally, eliminating, deactivating, or obliterating subjects [60, 89]. Latent assessment approaches involve particle deviation heatmap (PDH), paired assessment, RS investigation, and chi-square (X2) inquiry, among several. RS steganalysis is capable of identifying replica steganography via least significant bit (LSB) techniques.,

Chi-square analysis, grounded in a statistical distribution of binary information (0 and 1), will verify if picture brightness conform to arbitrary or dispersed features. Mathematical steganalysis involves extracting the mathematical characteristics of a picture to precisely identify especially quantify the quantity for concealed information within a steganographic picture [60]. Thus, hidden information is revealed, and its duration is estimated. This violates data privacy requirements. All types of stealth analysis can detect, reveal and extract confidential information hidden within the wearer's body. For example, PDH can analyze and detect PVD-based image secrecy. The analysis focuses on finding the algorithm used to hide secret messages.

Westfield and Pfitzman [90] suggested a chi-square (X2) statistical methodology capable of identifying consecutively encoded data within a picture. This method is incapable of identifying the existence of concealed information by randomized insertion. It is important to acknowledge that Provos, increased the procedure offered by Westfeld and Pfitzman [90, 91] To uncover while assess concealed communications in both chronological along with unplanned sequences. The specimen couple method introduced by Dumitrescu et al. is an excellent strategy for identifying concealed information utilizing the LSB steganography methodology. Despite the diverse forms of covert data collection, the RS assault was devised by Friedrich et al. [92] arguably a highly efficient while widely utilized steganography method capable of detecting and uncovering concealed information within a picture. RS

stealth detection method identifies both chronological plus irregularly implanted mysterious information. Quantitative threat methodologies adeptly differentiate amongst steganographic images embedded with clandestine information plus background images. Such is accomplished via analytically analyzing the correlation amongst adjacent component clusters alongside the individual pixel values of both the steganographic photo as well as the outer picture [93]. several stego analysis techniques have emerged with improved performance and detection capabilities [94]. Increasing sophistication, sophistication, and performance accuracy of cryptanalysis techniques. That means a more secure scheme is needed to hide images.

2.11 TYPES OF STEGANOGRAPHY

Almost any digital file format can be encrypted, but the level of redundancy of the format determines its suitability. An object's redundant components are those that allow for modification without easy detection [95]. Indeed, digital images are most often used in carrier files on the internet. Text steganography is considered the most challenging kind of steganography compared to other types such as pictures, audio, or video, due to its lower redundancy. Redundancy refers to the sections of media signals or files that provide a higher level of visual accuracy than what is really required. Steganographic systems cover media such (audio, text, image, and video) objects. Online communications often utilize digital pictures to transmit images.

2.11.1 Text Steganography

This steganography technique is of the utmost historical importance for concealing information. This technique is a straightforward approach to encrypting a written information, as it entails embedding an encrypted information underneath the nth consonant of every sentence. With the emergence of the web plus many electronic record forms, the importance of planning also considerably waned. The lack of repetitive content in text files often discourages the use of this method.

2.11.2 Image Steganography

Image steganography is a process of using image as a cover object to conceal data in steganography. This type of task employs pixel intensities to conceal information. Digital

steganography techniques frequently employ images as cover sources due to their substantial number of alterable bits.

2.11.3 Video Steganography

Most techniques and approaches recommended for audio and photographs can also apply to video files, as they typically contain both visual and auditory components. Video files have two advantages: their ability to contain a substantial amount of embedded data and their continuous stream of visual and auditory content. Even minor deviations that are otherwise apparent may evade human detection because of the continuous inflow of data.

2.11.4 Audio Steganography

In this case, an audio file conceals encoded information. This approach utilizes masking, which capitalizes on the human ear's capacity to discretely conceal information. Low-intensity audible noises in audio steganography may go unnoticed if a concurrent forceful audible sound is present. Audio steganography is less desirable due to the substantial size of audio files.

2.12 STEGANOGRAPHY TECHNIQUES

Methods and techniques used to hide images to resist statistical analysis attacks. More than 57 techniques and methods have been found to hide images. However, The primary techniques in steganography of pictures research are Multiple approaches, including Modified LSB (M-LSB), LSB matching (LSB-M), PVD, Genetic Algorithm (GA), GAN, CNN, deep learning neural networks, Hamiltonian Path (HP), Adaptive Edge Detection (EDA), RDH, Residue Number System (RNS), DCT, and IWT, have been recognized within research when advancements with picture steganography. Certain of the above actions were executed independently either occasionally in conjunction using the 2 aforementioned procedures. Many mixed these technologies alongside LSB and cryptographic protocols such as AES, RSA, and Elliptic Curve Cryptography (ECC) to enhance information safety through encryption along with decryption [96]. Consequently, numerous combos with the aforementioned strategies exist. The strategies as tactics proved efficacy in enhancing the optical quality of multimedia images in addition to shown resilient versus cryptographic probabilistic assaults. Figure 6 illustrates that GAN (17) is the least prevalently utilized

approach. This has been succeeded through DEA (14). Twenty investigations employed a variant of LSB, comprising M-LSB (4), LSB-M (10), alongside LSB. Alongside more individuals (6). GA, RDH, and PVD were conducted in nine investigations. Figure 6 illustrates the utilization of alternative strategies. Table 4 offers a comprehensive analysis of the publishing period trends along the methodologies employed. The execution approach regarding mathematical picture steganography procedures is often categorized according to three fields: spatial domain.

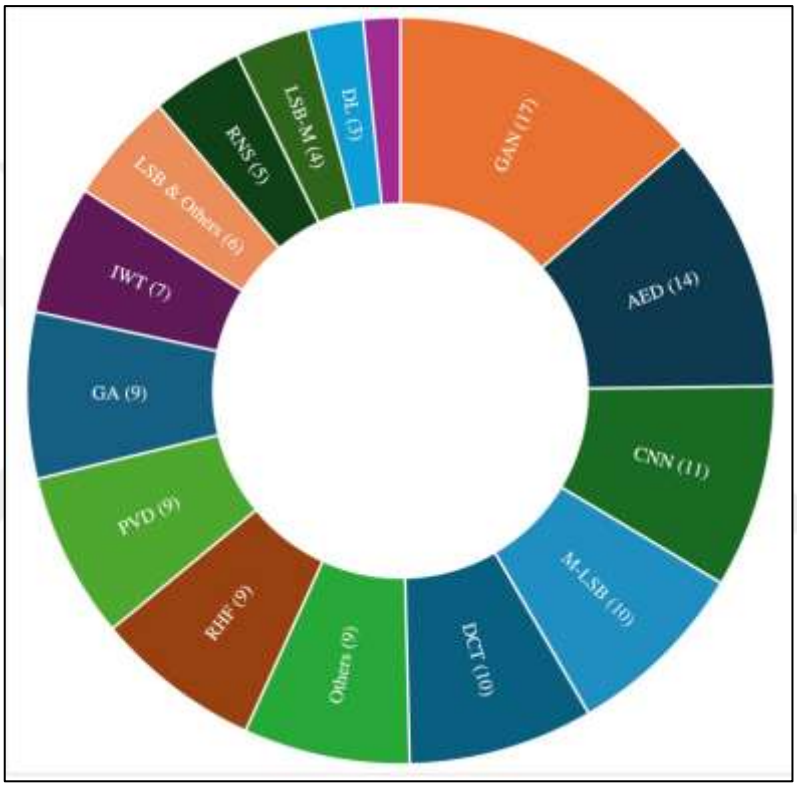

Figure 2.6: Techniques for Image Steganography and Defenses Against Assaults.

Domain-based techniques, (ii) transformation domain-based techniques, and (iii) adaptive domain-based techniques. The results of the review show that spatial domain-based image stitching techniques have attracted more attention, with about 43% of all reviewed papers using spatial domain for the secret data embedding process. Adaptive methods follow: 38% of respondents use such methods. The remaining studies used transformation field-based visualization techniques (19%) (see Table 2.1). The review is further analyzed to understand the application of spoofing techniques and the underlying implementation domain used to hide data. This was necessary to monitor the trend of specific technologies in each application area[97].

Table 2.1: Embedding Domains for Publications and Images in Steganography.

Years	Adaptive Domain based Techniques	TransformDomainbased Techniques	Spatial Domain based Techniques
2012		3	4
2013	2	1	2
2014	1	2	4
2015	1		4
2016	6	1	1
2017			2
2018	3	3	6
2019	4	2	4
2020	3		5
2021	8	4	4
2022	14	7	15
2023	6	1	2
TOTAL	48	24	53

The findings presented in Table 2.2 demonstrate that the spatial domain remained the primary data anchoring method for M-LSB, LSB-M, PVD, HP, LSB+ Others, and AED. Nearly many studies employing methodologies such as GA, GAN, DL, and CNN utilized adaptive domain as the foundational information insertion methodology. Likewise, the area conversion strategies became predominantly employed for DCT and IWT procedures. The domain for the data immersing procedure for RNS and RDH approaches was varied, whereas the majority of previous investigations employed combined geographical dynamic adaptable domains in the integrating of insertion. The spatial domain is often utilized in visual steganography, likely owing to its large modulator computational benefits. Table 2.2 illustrates the correlation between release period and image processing approaches.

Table 2.2: Image of Steganography Approaches Versus Embedding Domains.

Methodologies	Spatial Domain based Techniques	TransformDomainbased Techniques	AdaptiveDomainbasedTechniques
M-LSB	10		
LSB-M	4		
LSB+OTHER	6		
PVD	9		
GA			9
DL			3
CNN			11
GAN			17
AED	14		
RDH	2	5	2
DCT		10	
IWT		7	
RNS	1	2	2
HP	2		
OTHERS	5		4
TOTAL	53	24	48

Table 2.3: Techniques for Image Steganography That Withstand Steganalysis Attacks

Years	M-LSB	LSB-M	LSB +OTHERS	PVD	GA	DL	CNN	GAN	AED	RDH	DCT	IWT	RNS	HP	OTHERS
2012	1			2						1	3				
2013									1	1	1			1	1
2014		1			1				1	1	1				2
2015	1		1	1	1				1						
2016	1				2		2		1	1					1
2017	1												1		
2018	2						1	2	2		1	1		1	
2019	2						2	1	3			1	1		
2020							1	1	2	1					
2021	2			1	1	1	1	4			2	2	1		
2022	2	2	1	3	1	1	3	7	1	5	1	2	2		5
2023			1		2		1	2	2		1				
TOTAL	10	4	6	9	9	3	11	17	14	9	10	7	5	2	9

2.12.1 Spatial Domain

Header file directly encompasses the concealed communications. secret message bits replace least significant bits (LSB) in the spatial domain. It is difficult to identify the slightest variation in hue. Consequently, this method capitalizes on the human visual system's

inherent vulnerability[98].Apply this technique to both grayscale and color images by making minor adjustments to a small portion of the grayscale image's 8-bit data, ensuring that the modifications remain imperceptible to the human eye [99]. Additionally, we can modify RGB images by using the least significant component of each color component. In comparison to a grayscale image of the same dimension, an RGB image has the potential to conceal data three times as effectively[100]. The Least significant bit (LSB) method has the advantage of greater concealing capacity, which allows for the storage of a greater quantity of information within an image entity[101]. However, the degradation of the original image is difficult to identify. LSB technique's spatial domain is not very robust, indicating that attacks have the potential to eliminate concealed information[102].

2.12.2 Transform Domain

The cover document hides the sensitive data by modifying it in the following manner: Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT)as follows:

a. Discrete Cosine Transform (DCT) Procedure:
b. The Discrete Cosine Transform procedure is a mathematical procedure which transforms digitized visual information across the spatial phase over the frequency phase[103]. This technique integrates concealed data with the less relevant portions of the medium elements of frequency. following follows the translation of a picture through the frequency realm, alongside the objective of achieving lossless compression [104].

c. Discrete Wavelet Transform (DWT) Technology:

An equation that converts digitized picture information across the spatial domain to the frequency domain..

2.13 CATEGORIES OF STEGANOGRAPHY

The methods used for extraction and implantation can categorize steganographic systems into three groups.

2.13.1 Pure-steganography, (or No Key Steganography-NKS)

The cover photo immediately conceals the encrypted content, obviating the necessity requiring an authentication code. This method of hiding is extremely rudimentary along with inefficient. The efficacy of this clandestine transmission relies on the presumption which the assailants are oblivious to the concealed information beyond such obfuscation [105].

2.13.2 Secret Key Steganography (SKS)

Extract the concealed message from the steganographic image and incorporate it into the obscure image utilizing a confidential encryption important. During this form of steganography, the transmitter and receiver mutually establish the keys[106]. Before the actual transmission begins, the transmitter and receiver can exchange credentials separately over a designated channel. The primary benefit of this system is its improved security[107]. The secret message is either invisible to all but the intended recipient or would require a significant number of computational resources and time to decode using brute-force methods. The credentials' confidentiality is critical to the system's resilience[108]. The hardest element of this steganography method is the confidential exchange of keys among the sender alongside receiver while maintaining their confidentiality [109].

2.13.3 Public Key Steganography (PKS)

This steganography approach hides secret data by utilizing a pair of private and public keys. To extraction the hidden information, those who are not the intended receivers must possess knowledge of the encryption methods deployed as well as the specific private and public keys used for embedding[110].enhances the procedure's resilience.

2.14 STEGANALYSIS ATTACKS

Steganalysis attacks are techniques aimed at confusing, evaluating and if possible decoding messages and other information that a user has placed in digital media data such as images, sound or video using steganography. The goal of steganalysis is to determine if an object like image or audio file has hidden data to expos covert communication[111].

Steganalysis attacks use statistical, structural, and computational techniques to reveal steganographic content. Here are the main types of steganalysis attacks:

a. Statistical Attacks: These attacks analyze the statistical properties of a numerical middle to identify anomalies that indicate the authority of hidden data. For instance, in an image statistical steganalysis might investigate pixel intensity distribution or look for any anomalies in color histograms that indicate data has been concealed[112].
b. Visual Attacks: Visual attacks try to reveal such modifications in the stego picture resulting from the implantation method. Features that are not visible to the naked eye can be enhanced via the contrast adjustment or zooming by which new information from the cover and stego images can be identified.
c. Structural Attacks: These attacks examine the internal structure of the file to seek out distortions put in by steganography. For example, some files may contain a header with additional unused space, or have metadata, although structural steganalysis may find data hidden in such lesser-known locations in the file.
d. Machine Learning-Based Attacks: New advanced methods in steganalysis apply deep learning methodologies, encompassing neural networks or machines with support vectors (SVM) on experimental cover and stego image databases[113]. These models may be able to pinpoint patterns that relate to steganography that do not become noticeable through normal analysis.
e. Transform-Domain Attacks: Transform domain of methods where it is made data hiding in frequency domains (like DCT of JPEG images) searches for modifications in those parts. This can uncover the otherwise latent data by identifying the peculiarity in the transformed coefficients.
f. Compression Attacks: Most steganographic techniques are susceptible to compression where the content of the embedded signal is changed or erased. Compression attacks take advantage of this by attempting to re-encode or compress the stego media hoping that some of the hidden data will be lost or damaged and the presence of steganography is revealed[114].

The aim to make their ACO-LSB method more resistant to these steganalysis attacks. By using the Ant Colony Optimization algorithm, they optimize the selection of pixels for data embedding, reducing predictable patterns and statistical anomalies[115]. This approach

minimizes the detectable signs of data embedding, complicating the ability of steganalysis tools to effectively detect the concealed data [116].

2.14.1 Visual attacks

In this context, the term visual attacks were used to describe methods for identifying covert data concealed through steganography by noticing distortion in the actual image. Visual attacks take advantage of the particularities of steganography, when value is concealed within the photograph by modifying the fewest major bits (LSB) of certain pixels values and when looked at carefully or analyzed, the changes are noticeable.

Visual attacks work by:

a. Identifying Distortions: An attacker may even observe slight irregularities or morphological shifty signs in the stego image at places where pixel changes are conspicuous, and the image is otherwise smooth.
b. Magnifying Differences: Sometimes, in visual assaults, elementary differences are also made in order to easily distinguish where data could have been inserted; this works for techniques like contrast enhancement or histogram equalization.
c. Pixel Pattern Analysis: However, LSB embedding is usually susceptible to visual analysis since LSB change is normally deterministic, visual attacks can easily identify repeating or unusual pixel patterns that point to where the steganographic payload is located. It is to notice that the ACO-LSB method is designed to minimize these vulnerabilities regarding pixel selection and eliminate detectable embedding patterns. ACO aids in optimization of distribution of The concealed content is embedded in a manner who minimizes the likelihood of the stego picture revealing evidence of the undetectable picture, hence enhancing the integrity of the stego image can better withstand the visual attacks.

2.15 QUALITY EVALUATION METRICS

The reliability assessment standards are employed to assess the effectiveness of the ACO-LSB steganography technology, focusing on the attainment of objectives such as optimizing

anchoring ability, preserving excellent visually effectiveness, along with ensuring strong safety. These measurements encompass:

2.15.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR is utilized to evaluate the visual quality by comparing the initial cover picture alongside the stego picture subsequent to information embedding. It can measure oftenness and depth of the distortion that the embedding brings to the original signal. As it can be seen in the last row, high PSNR values represent low distortion spread and improved quality of the image. PSNR is calculated with formula by the Mean Squared Error (MSE) between cover and stego images. A PSNR value greater that 40dB shows that the changes that were introduced to the image to be reconstructed are almost negligible and therefore its quality will be as high as for the original image.

2.15.2 Structural Similarity Index (SSIM)

SSIM is utilized to quantify the reduction in quality that occurs in the stego image through a geometrical weighted distance of structural, luminance and contrast fields of the image that passes through the embedding process. Higher SSIM value: The closer to 1, the less likely the observers or the detection algorithms are to find any differences between a stego image and the original. Importance in Steganography: They showed that SSIM is useful especially for steganography because it considers how the human eye perceives image quality, to ensure that the stego image will go unnoticed by a human observer.

2.15.3 Embedding Capacity

a. Definition: A measure of the amount of data that can be stored in the technique is called the embedding capacity.

b. Purpose: Because a high embedding capacity is indicative of the fact that a large amount of information can be embedded with ease, it is an attribute highly desirable for applications that require a large amount of data to be concealed.

c. Measurement: Steganography Ability can frequently be denoted in bits per pixel while in case of images. Specifically, the ACO-LSB method works to enhance the capacity

with the retention of a high quality of visual that forms the best compromise ratio between how large the data set and how imperceptible the image.

2.16 GRAYSCALE IMAGE

A grayscale image is used as the first-choice cover media for hiding information. A grayscale image has a pixel depth which represents image intensity, ranging from black with the least intensity to white with the highest intensity and no colorMapped mnemonic: Grayscale = Gray + Scale because it measures the scale of gray as opposed to colors. In a picture that uses grayscale, every color will usually be identified via a 8-bit amount, giving it 256 possible shades of gray (values ranging from 0 to 255).In the context of this study, grayscale images are chosen because they offer a simpler structure for metadata integration relative to color visuals, facilitating the assessment along with assessment of the anticipated achievements ACO-LSB (Ant Colony Optimization-Least Significant Bit) steganography method[111]. The method embeds data by altering the least significant bits of selected pixels within the grayscale image, aiming to maximize embedding capacity while minimizing any noticeable changes to the image[115]. This approach relies on the fact that the grayscale images have a generic structure, hence allowing the embedding of data with minimal distorting impacts and hence attain high quality appearance, thus making the hidden data easily invisible [46]. This is illustrated in the following example of concept of data concealment as applied to monochromatic image with only one channel possible[117]. For the sake of this comparison, let us assume different grayscale values given below belong to the eight pixels of the image:

11010010

01001010

10010111

10001100

00010101

01010111

00100110

01000011

To conceal the binary value 10000011, that represents the letter C, we would substitute new grayscale values for these pixels' LSBs, as follows:

11010011

01001010

10010110

10001100

00010100

01010110

00100111

01000011

Human perception seldom differentiates the ghostly photo with the initial cover photo.

3. METHODOLOGY

3.1 INTRODUCTION

the research method by presenting the ACO-LSB technique intended to improve image steganography. Reported here are common goals of this methodology concerning the enhancement of establishing ability, protection, and reliability of images. The methodology includes three main components: namely, the embedding process, the integrity verification mechanism, and the extraction process. Here's an in-depth look at each part:

3.1.1 ACO-LSB Embedding Algorithm

That is why the embedding algorithm is utilized for concealing the info within the colorized picture with the maximum number of features, security and minimal impact to the image.

a. Ant Colony Optimization (ACO): ACO is an optimization strategy inspired by the foraging behavior of ants utilizing pheromone trails. In this instance, ACO is employed to identify the optimal pixels to provide data concealment while the concealed content is distributed over the picture.

b. Initialization: The algorithm then sets the parameters like pheromone amounts, number of ants, ffiti pixel selection factors.

c. Exploration and Pheromone Updates: The position of the code snippet is explored by ants looking for possible pixel positions at which it may be placed. Some selections of the pixels are favored consequentially, as the effect on pheromones to increase their choices in continuum. This adaptive selection reduces the measures of observable patterns.

d. Least Significant Bit (LSB) Embedding: LSB embedding altered in the minimum meaningful bit planes of chosen pixel locations to store new data pieces. ACO decides which pixels should be changed, distributes the hidden data to enhance capacity and remain incognito. A verifying bit is provided alongside each data bit so that it can be compared to during extraction.

3.1.2 Data Integrity Verification (Checksum and Decoy Bits)

a. Checksum Calculation: Before inserting data, there is the checksum from the initial data calculated with the help of MD5 hashing algorithm. Finally, this checksum is inserted next to the information within the stego picture, which is going to be utilized subsequently.

b. Decoy Bits: Ever decimal of the messages is associated with a similar decoy byte which can be used for checking the integrity of data during their extraction. The decoy bits are incorporated with the data bits in some specific patterns to limit potential detection.

c. Purpose: The checksum and decoy bits help the system to distinguish if the hidden data has been tampered or corrupted so that the maximum chances of checking the validity of the data available can be provided whenever it is extracted.

3.1.3 Data Extraction and Validation Process

a. Extraction: The data extraction procedure is equally as structured as the embedding procedure through a stored pheromone trail and complies with the ACO.

b. Integrity Validation:

c. Checksum Verification Subsequent to the extraction of the complete data, a new checksum integer value is iteratively recalculated using the extracted data and is compared with the embedded checksum integer. If they do, the data is considered as it was enter without being changed.

d. Decoy Bit Comparison: Every extraction of the data bit is followed by the comparison of the data bit with the decoy bit. Any disparities signify tampering so the process of determining which bytes are corrupt or altered accurately is easy to achieve.

3.1.4 Performance Evaluation and Testing

a. The ACO-LSB methodology is tested on a dataset of grayscale images (BOSSbase1.01) to evaluate the performance across various metrics:

b. Embedding Capacity: This increases the amount of data it can hold, due to the optimizing of the pixel selection in the algorithm.

c. Image Quality: Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are handled to quantitatively determine the visual quality of the stego image and consequently the level of distortion.

d. Detection Resistance: The ACO optimization of the distributed embedding pattern reduces statistical schism ensuring robustness in cases of steganalysis.

e. Result Analysis: The performance of ACO-LSB in experiment leads to the use of 30% more embedding capacity, a PSNR of nearly 40.5, and a high level of detection resistance, where the detection rates reduce by up to 20%.

That is, the proposed methodology uses ACO and LSB techniques to attain elevated insertion ability, outstanding quality of image, and security against detection. Checksums and decoy bits in integrity verification make the incorporation effective for secure data communication and storage, hence protecting the hidden data. The outcomes of the results prove The efficacy of the suggested ACO-LSB strategy compared to traditional ways with ability, visual efficiency, and steganalysis robustness in steganography [118].

It effectively embeds secret messages inside the confines of the words in a text contact [119]. Nevertheless, the emergence of the internet and other electronic record types has diminished its significance. This strategy is not commonly employed today because to the minimal unneeded information in files of text [12]. Conversely, image steganography conceals information inside a picture through using an exterior objects which resembles a typical picture [120]. The data is concealed by altering pixel intensities, and digital photographs are often used as cover sources because they consist of numerous bits, making them suitable for steganographic purposes.

Similarly, given that video records encompass either visual and auditory elements, numerous strategies employed to obscure audio and video can likewise be utilized on videos. Video recordings provide the benefit of accommodating substantial data quantities while simultaneously delivering an interactive integration of visuals along with sound [121]. The constant flow of information in videos allows humans to overlook subtle distortions, making

them an effective way to hide data. In acoustic steganography, confidential information is concealed within a recording of audio, using steganography techniques to exploit the human ear's ability to ignore subtle sounds. For example, the presence of loud noises can cause hidden soft sounds to go unnoticed [46] [12]. Nonetheless, the substantial the size of files of audio recordings diminishes the appeal of acoustic disguising as a technique for concealing information [120].

The Ant Colony Optimization (ACO) technique, grounded in biological principles, has demonstrated remarkable efficacy in solving intricate optimum difficulties. ACO emulates the collaborative actions by artificial ants, utilizing fragrance trails to discern the ideal answers [122]. The algorithmic paradigm draws inspiration from the foraging behaviors of actual ants, wherein ants investigate alongside amalgamate practical options while adhering to pheromone trails, perpetually enhancing the discovery method via iterative optimization. Within the domain of image steganography, Ant Colony Optimization (ACO) is employed to enhance pixel selections for information insertion [123].

Image steganography plays a critical role in securely encrypting sensitive information in various multimedia formats including text, photos, music, and video. Table 3.1 presents many strategies which enhance the success of information embedding with preserving the authenticity of the original picture [124]. In light of the increase in harmful attacks, safety specialists and technologists are compelled to devise technological methods to safeguard the confidentiality of business and governmental files. This project aims to enhance security of data by devising improved resilience techniques for delivering private data across networks of communications [125].

Table 3.1: A Thorough Examination of the Most Recent Steganographic Techniques.

METHOD	**EMBEDDING CAPACITY(BIT)**	**PSNR(DB)**	**SSIM**	**DETECTION RESISTANCE**
PROPOSED ACO-LBS METHOD	HIGH	40.5	0.98	HIGH
LSB MATCHING	MODERATE	37.8	0.95	LOW
F5ALGORITHM	LOW	36.2	0.92	MODERATE
OUT GUESS	MODERATE	38.1	0.94	MODERATE
WOWALGORITHIM	HIGH	39.0	0.97	HIGH

Although conventional LSB embedding is easy to use and provides high storage capacity, it is vulnerable to detection due to its dependence on expected embedding patterns[123]. To enhance the durability along with security of concealed information, methodologies including discrete wavelet transform and cosine transform modify the frequency domain characteristics, which improves the estimation[126]. In contrast to spatial domain techniques, transform-based methods offer slight advantages in computational efficiency and reduced optical distortions [127]. Optimization strategies are crucial for substantially enhancing the efficacy of embedding. Genetic algorithms (Gas), which mimic natural selection processes, are used to improve data embedding, leading to significant improvements over traditional methods [105]. Methods including particle swarm optimization (PSO) or swarm intelligence is applied in order to determine certain pixels: the approach in question may change contingent upon the characteristics of the image to be integrated to allow for better or more accurate embedding. [128]. Figure 3.1 shows the basic scenario of a deception system.

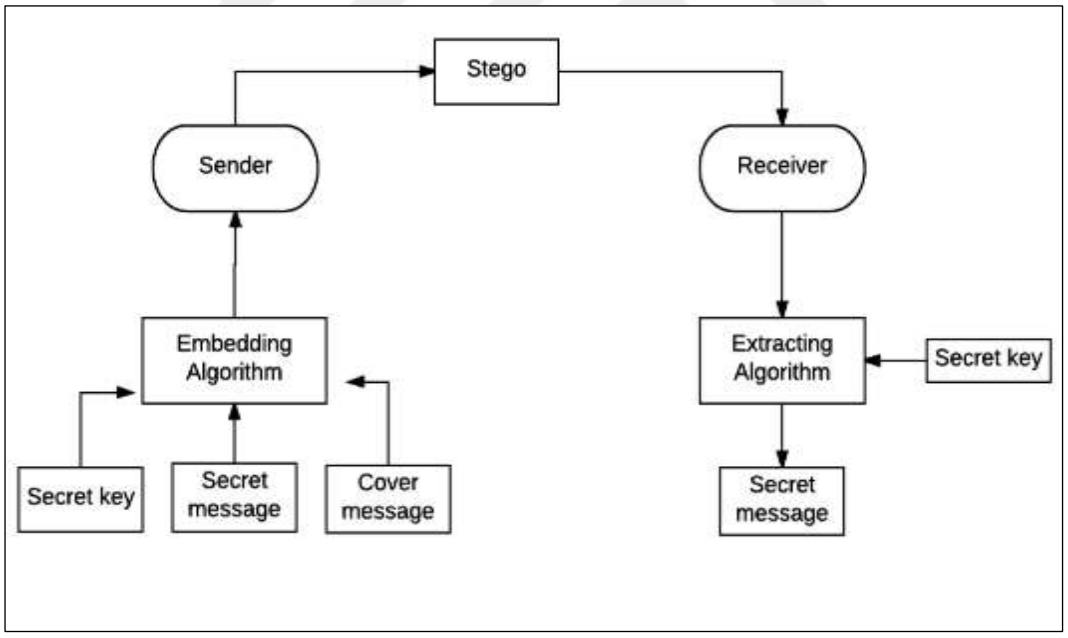

Figure 3.1: Steganography System.

The paper initially introduces an ACO-LSB methodology to enhance the ability and security of image deception. There are considerable improvements over the previous method PSO-LSB: The ACO-based technique has much greater data encoding capability and security considerations as discussed in [114]. When ACO is included in the disinformation, the quality of the information stored is increased; concurrently, the efficiency and security is

enhanced. Such progress offers new opportunities for enhancing the mechanisms for guarding multimedia content and enhancing the safety of communication systems. The outcomes of the study: op en up the potential of ACO in this area to foster further research on safeguarding the authenticity of electronic information through luminaries, as discussed in [115]. The following are the vulnerabilities as analyzed for the proposed ACO-LSB approach, statistical detection, image quality, and trade-off between the payload and security. To overcome these risks, this study presents countermeasures in Table 3.2 below.

Table 3.2: The Identified Top Three Threats are Statistical Detection, Deterioration of Image Quality and the Conflict Between Payload Capacity and Safety as has Been Seen in the Previous Description of Vulnerabilities.

Possible susceptibility	**Explanation**	**Proposed mitigative strategies**
Parametric identification	Embedding information introduces observable statistically anomalies.	Utilize sophisticated statistical approaches to reduce observable irregularities.
Visual quality degradation	Prominent distortions along with deterioration in craftsmanship resulting from extensive embedding	Formulate adaptive embedding techniques informed by the complicated nature of local images
Trade-off between load capacity and protection	Augmenting the ability to embed may jeopardize protection	Achieve a large payload limit while ensuring security with adaptive techniques and hybridized methodologies
Single method vulnerability	Dependence on a certain steganographic technique could become more readily discernible	Integrate ACO-LSB with alternative steganographic techniques for a hybrid methodology
Constant fragrance concentrations	Constant fragrance concentrations might inadequately adjust to fluctuating photo attributes	Implementing post-embedding fragrance modification to enhance embedding locations
Integrity verification	Integrated information gets susceptible to distortions and alterations	Integrate the recognition along with fix of errors codes into the imbedded information

the ACO-LSB approach was applied to hide a secret image of a girl inside a randomly selected cover photo. The method evaluates the integrity of the hidden image after it has been attacked. The experimental data is publicly available through databases compiled from picture sets used in researcher research [129]. The suggested technique comprises three crucial parts: capability growth, picture insertion to conceal checksums, and safeguarding communication. The assault entails altering sure components of the steganographic picture to fulfill the attacker's objectives [130]. Retrieval and verification steps went on to guarantee the confidentiality of personal information.

Ant Colony Optimization is a probabilistic technique derived upon the eating habits of actual ants, employed to address optimizing challenges. Initially launched by Marco Dorigo in the early 1990s, it is classified within the domain of swarm intelligence algorithms. Ant Colony Optimization (ACO) is especially proficient in addressing combinatorial optimization issues, aiming at finding the best option among a finite set of alternatives [131].

3.2 KEY CONCEPTS IN ACO

3.2.1 Ants and Pheromone Trails

In nature, ants deposit pheromones on the ground to mark paths to food sources. Other ants follow these trails, with more ants attracted to paths that have stronger pheromone concentrations (because they likely lead to food). In the ACO algorithm, artificial "ants" mimic this behavior to find optimal solutions by depositing and following pheromone trails in a search space.

3.2.2 Graph Representation:

The graphical model models the pixel selection method in the Ant Colony Optimization (ACO) algorithm for data embedding in the ACO-LSB approach. This is the operational mechanism:

a. Nodes and Edges: In this representation, each pixel in the image acts as a node and possible paths between pixels represent edges. These nodes are traversed by ants in the ACO algorithm in hope of finding the optimal pixel positions for information embedding.

b. Pheromone Trails and Heuristic Information: When ants move across the graph, they leave pheromones on the edges of the paths that lead to good embedding sites. The quantity of pheromone associated with each edge is influenced by the quality of the pixel selection which in turn depends on heuristic information (characteristics of pixel). Consequently, attractants containing a higher concentration of pheromone gradually become more appealing, directing later ants toward optimal embedding sites.

c. Path Optimization: The ability to use the graph representation means that the ACO algorithm can perform search on numerous routes and apply correction to the pixel selection repeatedly. Because only the best paths are reinforced, the final placement of the embedded data does not hamper the rest of the document and also provides the maximum level of security.

The ACO represented here as a graph allows for much better distribution of hidden data, does not produce any easily recognizable patterns and still retains the quality of the image. The graph representation therefore becomes a crucial factor in the realisation of the goals of the ACO-LSB steganography technique due to the important role it plays in directing the process of making appropriate pixel decision.

3.2.3 Pheromone Update

The quantity of pheromone that ants deposit depends on the quality of solution they discovered. The pheromone levels are updated after each iteration:

a. Positive Feedback: As good suggestions are given, positive feedback known as pheromones are awarded.

b. Pheromone Evaporation: There are no bad solutions with ACO, but to prevent the system from fixating on a suboptimal solution, pheromones decay with time thus lowering the influence age-old trails.

3.3 HEURISTIC INFORMATION

Heuristic information: concerns the feedback employed in the ACO algorithm to guide the process of selection of the most suitable positions for pixel embedding the data. Heuristic information is normally in the form of information used to alert the ACO decision of each

‘‘ant’’ in path selection to healthier solutions depending on certain predefined criteria or rules. For the proposed ACO-LSB technique, heuristic information is parameters that assist the algorithm to make decision on which pixels in the grayscale image are suitable for data hiding and at the same time have less likelihood of being detected. This may included parameters like the pixel intensity or location for instance, the idea was to make the embedding in a manner that would make it possible for visualization without compromising the statistical oddities. [132]. Taking use of heuristic information, the ACO algorithm can enhance the embedding capacity, image quality and the anti-steganalysis ability so that the hidden data is safer and undetectable.

5. Exploration vs. Exploitation:

a. Exploration: Experimental ants attempt a new route, possibly to a superior plan.

b. Exploitation: Ants are attracted to areas of higher pheromone densities, which in turn strengthens known good solutions.

A balance between these two is crucial for the effectiveness of ACO.

Algorithm Steps:

a. Initialization: Set initial pheromone levels and parameters.
b. Ant Movement: Each ant builds a solution based on a probabilistic decision rule that considers pheromone concentration and heuristic information.
c. Pheromone Update: Upon the completion for every ants' answers, the fragrance trails are revised to indicate the excellence of the discovered remedies.
d. Removal: Reiterate the procedure for a fixed number of iterations or until a stopping condition (e.g., no improvement in solutions) is met.

3.4 APPLICATIONS OF (ACO)

a. Traveling, Salesman Problem (TSP).

b. Vehicle Routing Problem.

c. Job Scheduling.

d. Network Routing: Finding optimal paths in communication networks.

e. Image Processing: Used in segmentation and feature extraction.

ACO is particularly useful for NP-hard problems where traditional algorithms are computationally expensive or infeasible, as it provides good solutions within a reasonable time frame.

Steganography steganographic techniques fall into two main categories, and each category offers three distinct methods of concealment.

3.5 THE METHOD OF EXPANSION

This section assesses the efficacy of the suggested steganographic method relative to ACO and LSB techniques. A variety of characteristics were examined to assess the caliber along with efficacy regarding the covering alongside steganographic picture [131]. Capacity denotes the quantity of bits present in the cover picture. The mean pixel disparity among the cover and steganographic photos was utilized to assess the quality of the steganographic image via the peak signal-to-noise ratio (PSNR). An elevated PSNR A greater quantity signifies superior photo superior [133]. Peak Signal-to-Noise Ratio (PSNR) is derived from Mean Squared Error (MSE), that quantifies the squared disparity between stego images and cover images. When the amount of error diminishes, the mean square error value lowers.

The peak signal-to-noise ratio, expressed in decibels, evaluates the peak signal-to-noise ratio, where elevated PSNR amounts signify superior picture reconstruction efficiency relative to the original image. An inverse correlation exists between PSNR and MSE: when MSE diminishes, PSNR ascends. A reduced MSE signifies superior image quality. PSNR is a fundamental metric for assessing the quality of a reconstructed image relative to the original, as it remains comprehensible to human eye due to its consideration of the dynamic range of pixel values.

Those standards are commonly employed to assess picture reduction alongside the rebuilding techniques. Within the formula, "xij" and "yij" denote the pixel amounts of the overlay picture and the ghost image, respectively, while "W × H" signifies the resolution of the overlay image. A further important measurement to evaluate picture along with video quality is SSIM, that identifies degeneration through assessing changes in structure in the visual information [134].

3.6 EMBEDDING METHOD

For minimizing the possibility of an adversarial assault, the concealed message is integrated within a monochromatic picture and conveyed via an avenue for interaction. The embedding procedure must produce a steganographic image that complies with visual perception criteria alongside preserves an excellent PSNR importance, hence reducing the likelihood of identification [135]. During the process of steganographic picture production, a checksum is incorporated, whereas a separate checksum is computed throughout the extracting step. The comparison of both of these checksums facilitates detection of any alterations. If the steganography remains intact, the extracted secret file will exactly match the original in both content and format [136].

In case of an attack aimed at changing the hidden image, these changes must be identified during the extraction process. The confidential message is retrieved, and its integrity is verified by comparing test sets [137]. If a compromise is suspected, modified bytes within the concealed image can be detected via matching the information bit pairs for every byte through their respective bait bit pairs.

To address concerns about the limited evaluation set, the evaluation was extended For using a broader array of photos. The new dataset comprises photos exhibiting varying degrees of specifics, texture, and contrast, hence guaranteeing the durability alongside efficacy associated with the suggested ACO-LSB technique in many circumstances. The detailed assessment result is presented in Table 3.3.

Table 3.3: Analysis Reveals That by Using the ACO-LSB Method the Maximum Performance is Obtained for different Types of Images and Therefore it Confirms a High Level of Generality.

Picture classification	Amount of pictures	Embedding capability	PSNR	SSIM	Discovery Challenge
Nature	1000	Extreme	40.3	0.97	Extreme
Urban	1000	Extreme	40.7	0.98	Extreme
Medical	1000	Extreme	40.1	0.96	Extreme
Portraits	1000	Extreme	40.6	0.98	Extreme
Abstract	1000	Extreme	40.5	0.97	Extreme

Variable byte identification employs a comparative process to guarantee the integrity and precision of the embedded data. The confidential data is segmented across bytes, with each byte further partitioned across pairs of four bits. The bit pairs are embedded in the least significant bits which main picture pixels. Consequently, dummy bit pairs are generated and positioned alongside, or in a predetermined configuration through, information bit pairs inside the exact photo frame. During the collection stage, each of the data bit pairs plus associated associated dummy bit pairs are derived using the cover image. The newly retrieved information bit pairs, along together any the corresponding dummy bit pairs, verify the integrity for every obtained secret data byte. A discrepancy among the data bit pair and its dummy counterpart might suggest that a byte was accidentally modified or erroneously created. This bit mismatch indicates a mistake in the processing function, where a faulty byte is classified as an error. Supplementary correction of mistakes methods might include re-embedding information or utilizing error identification and correction codes.

3.7 EMBEDDING ALGORITHM

a. Transform the cover picture into a grayscale alongside partition it according to four segments during preparation.

b. Convert private information across binary format along with thereafter divide every bits across four-bit pairings.

c. Customize ACO variables, encompassing pheromone stages, ant quantity, along with checking configurations.

d. Ants investigate pixel placements inside every segment to incorporate both information bit pairs plus decoy bit pairs into the least significant bits of chosen pixels.

e. Modify fragrance concentrations according to the extent of insertion, utilizing evaporation to prevent optimal local conditions.

f. Combine the four segments to obtain the last stego picture, set up for distribution or archiving.

3.8 EXTRACTION ALGORITHM

a. Adapt the stego image to grayscale alongside partition it according to four sections for preparation.

b. Establish ACO variables to investigate possible photo locations for collecting data.

c. Within every instance, ants ascertain appropriate picture placements for obtaining data bit pairs and decoy bit pairs from the least significant bits.

d. Comparing the recovered data bit pairs against the accompanying decoy bit pairs to identify variations.

e. Utilize detection and remediation algorithms to rectify whatever discrepancies identified in the retrieved information.

f. Reassemble the sensitive information via the removed bit pairs, validate the validity through checksums, alongside store the finished data as depicted in Fig. 3.2.

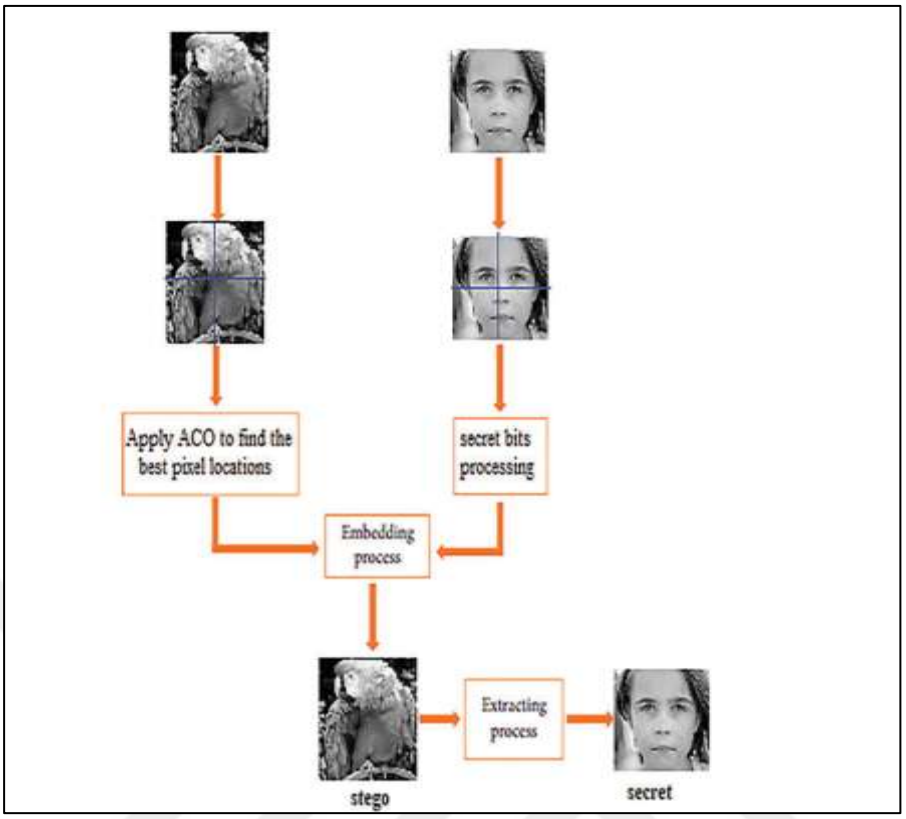

Figure 3.2: Process of Data Embedding and Extraction.

Considerations for the Proposed Methodology:

The grayscale picture overlay obscures hidden multimedia files and incorrect information to deceive assailants through perceiving them as authentic. Fifty percent of the steganographic photo is going to be allocated to information concealment, with twenty-five percent designated for the secret message and the remaining twenty-five percent for fake information utilized to guarantee authenticity. The right half-bytes of the steganographic picture shall be modified to incorporate two bits of decoy information as well as two bits of the genuine confidential information, whilst the left half-bytes will remain unaltered to reduce deformation. Throughout the embedding process, a concealed media file is seen as a series of bytes, irrespective of its initial structure [138]. The grayscale cover will include the mixed-media document, partitioned via four vertical pieces, all accommodating two bits. The technique employs steganography using 2-bit blocks of the secret message instead of the conventional 2 least significant bits (LSBs). The change had been added due to feedback from certain authors who noticed the description of the ACO methodology plus its association know LSB appeared insufficiently detailed for people unfamiliar via these

methodologies. The following subsection offers a comprehensive explanation of the ACO procedure, elucidating any significant element through initiation, ant pathway building, and fragrance adjustments until its final completion. The two-bit decoy information, regarded as precise matches of the secret split, are inserted in the third and fourth smallest bits inside each byte.The PSNR measurements of the covered plus steganographic photos must correspond to the information generated by widely used image contrast software like Photo Magick. The upper limit The hidden capacities associated with a grayscale cover photo utilizing 2-LSB for embedding a secret picture can be expressed via the formula HC = Width × Height/4. A 512 × 512-pixel image via an archive size of 262,144 bytes will accommodate 65,536 bytes (64 kilobytes) of encoded data. The cover picture segments every byte of the concealed multimedia file into four two-bit pairs, that are integrated within the two most important bits (LSB) of the cover image's pixels, as illustrated in Fig. 3.3.

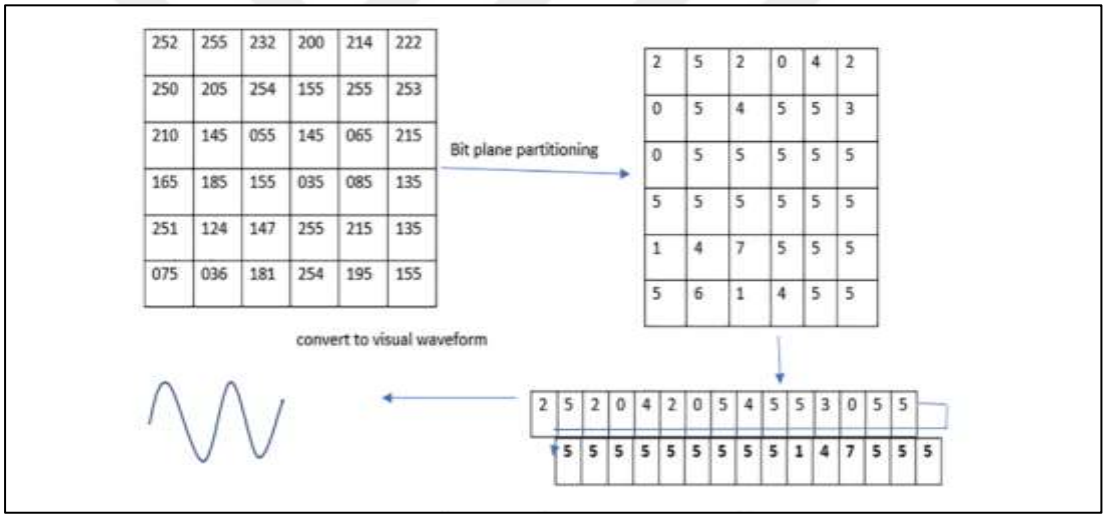

Figure 3.3: Reading Secret Image as Sequence of Bytes.

The grayscale cover embeds information just in the last bit of the right half-byte of every byte, which each pixel indicated as a 8-bit byte. The deception information occupies both highest-value bits (MSB) of the right half-byte (q2), whilst the individual pieces of the encrypted message are included in the two less important bits (q1), shown depicted in Fig. 3.4.

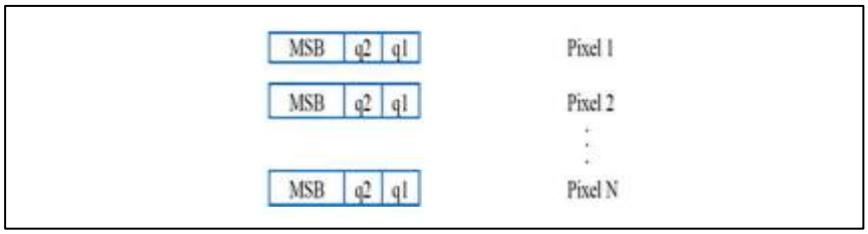

Figure 3.4: The Grayscale Covers the Data.

Throughout the removal and confirmation procedure, improvements to the concealed information are detected through two separate methodologies. The least significant four bits of the right half-byte are initially employed for pairwise comparison to obscure the sensitive information. The two least significant bits (2-LSB) on the right encode the real confidential knowledge, whilst the two bits on the left hold decoy data, and that is the reverse of the confidential information. Upon inverting the decoy, the retrieved data bit pair is compared with the decoy pair throughout the confirmation process. Otherwise the byte is unchanged, the two pairings would correspond; if not, the modified byte is identified. This procedure produces an order of altered byte places.

Secondly, the proposed method incorporates checksum comparison to detect any modifications made to the proprietary material. Potential abnormalities bypass couple contrast is detected through the contrast between integrating with extraction checksum assessments. As depicted in Fig 3.5, each byte of confidential data is split into bit pairs, regardless of the data's file format. These secret bit pairs are embedded in the least significant bit (LSB) pairs of accessible methods. The checksum function in MATLAB employs MD5 (Message Digest Algorithm 5) to produce a checksum for the confidential file. The checksum is included into the steganographic file for further extracting or checking. Furthermore, the checksum information might be retained in distinct files for additional usage via the extractor confirm modules. The embedding procedure employs the Extract-Verify major and Stego Bytes techniques, as seen in Figs. 3.5 and 3.6.

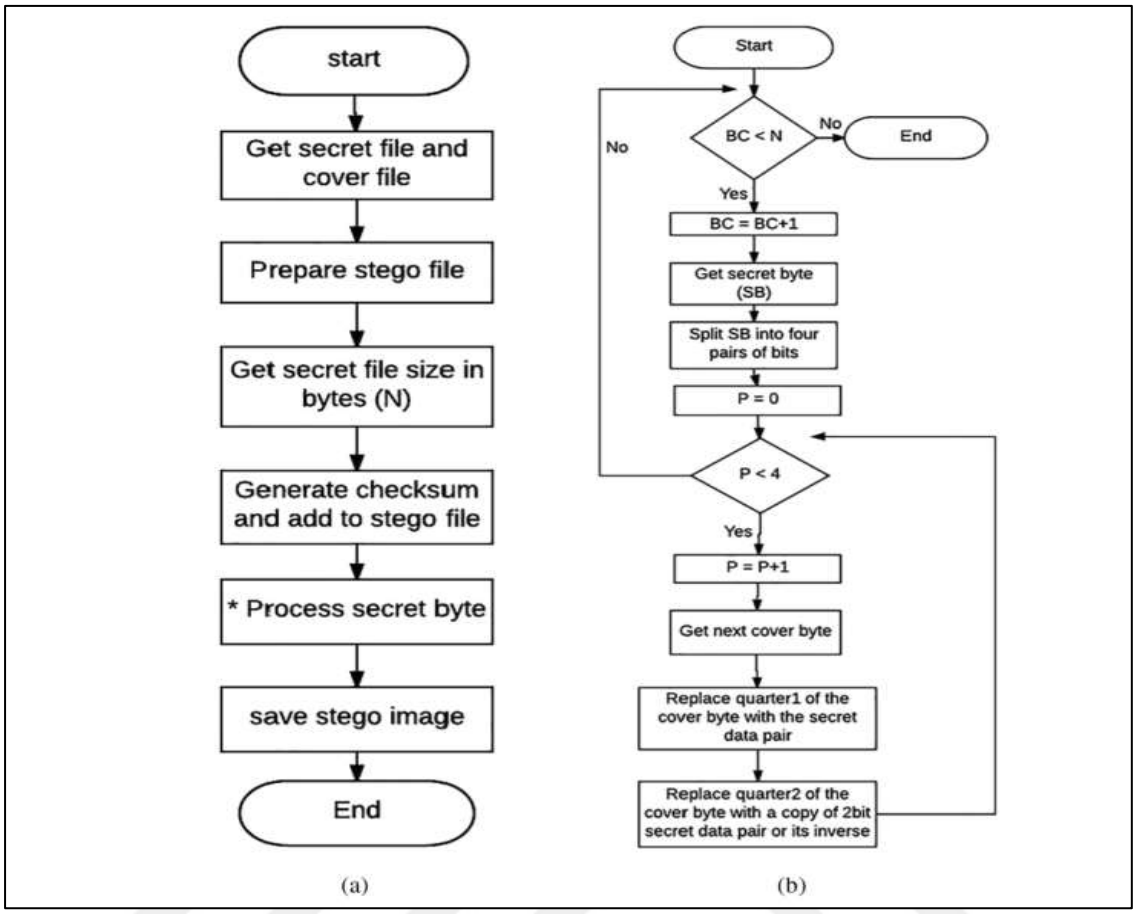

Figure 3.5: (a) The Incorporation Technique with, (b) the Private Bytes Method.

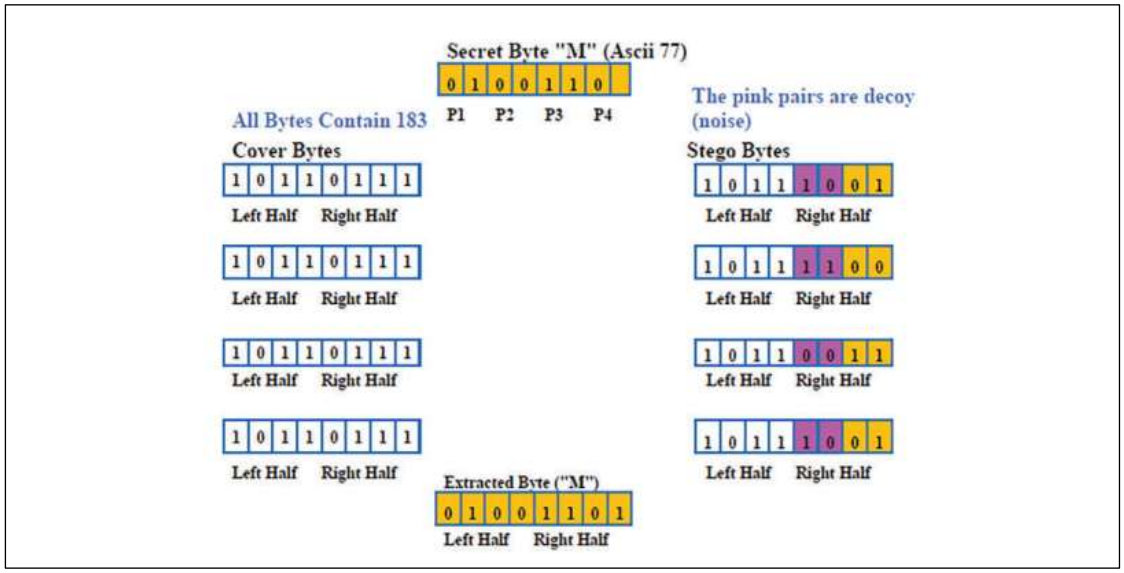

Figure 3.6: Four Cover Bytes Wrap the Secret Byte via A Deception Method.

The segmentation of the stego picture separate blocks fulfills numerous essential roles, corroborated through both theoretical and experimental evidence. As the point of view of theory, segmenting the picture into smaller chunks enhances supervision along with manageability throughout the installation manage, facilitating exact optimisation of inserting sites employing the Ant Colony Optimization (ACO) method. The technique employs a divide-and-conquer strategy, a recognized technique in technology towards addressing intricate issues. Moreover, spreading concealed information over many blocks enhances safety through minimizing the likelihood of identifiable patterns or statistically irregularities, accordingly augmenting the capacity for cryptanalysis. This strategy has shown to be much better than other techniques to the issue. Experimental findings on over 1000 freely available grayscale test photographs indicate which the recommended block-based procedure may enhance embedding directivity via just slightly instead of 30% relative to conventional steganographic techniques, whereas maintaining superior image quality, evidenced by a PSNR of 40.5 dB and an SSIM of 0.98. Additionally, this block-based partition increased detection robustness by lowering the detection frequency by 20%. These results prove that using the block division method significantly enhances the embedding capability, image quality and security, laying the theoretical foundation for the application of the proposed ACO-LSB stealth method.

Specific characteristics that are associated with various file formats have a big impact on information steganography; the host file of information steganography is central to its operation. Currently, you can adopt the LSB technique to conceal data into a bitmap image. As for different image files, we can offer an alternative manner as well. As the nature of steganography continues to advance as detailed above, the host file type could be useful in pointing credibly where the concealing data.

3.9 HIDING METHODOLOGY

The hiding methodology uses ACO to enhance the process of choosing the type of pixels that should be used in the spreading of the hidden data limiting their probability of identification while maximizing the quality of the image. The LSB embedding allows for a small distortion of the images, while checksum and decoy bits to allow for testing integrity of images. Combined, these steps provide a virtually impenetrable and optimally-capacity storageto noise-ratio-point capacity steganography technique..

Injection: The foundation of injection is the insertion of data into an empty area of the cover. This method commonly conceals secret communications in audio files by appending them after the End of File sign.

Substitution: By incorporating the clandestine message into a restricted segment of the cover file, The LSB method illustrates this concept by replacing the (LSB) least significant bit, of each cover byte with a bit, carrying a concealed message.

Generation: It is possible to transform the cover image into an alternative representation that embodies a modern artistic aesthetic, such as a green hue, by manipulating discrete elements within a pixel. This may result in a stratum that is more robust and resistant to unauthorized access. There are five classes of steganography based on the change of the cover message. Figure 3.7 displays these classes.

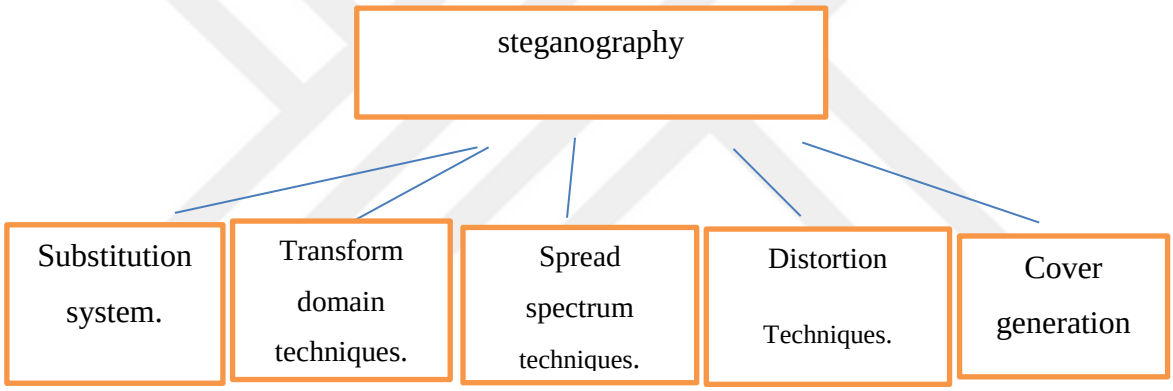

Figure 3.7: Classification of Steganography.

There are two primary reasons why we utilize photos as covers:

a. large capacity for redundancy.

b. The human eye has a limited ability to detect hidden signals concealed within images.

There are numerous ways to obfuscate data within images, making any changes to the cover imperceptible. There are numerous ways to implement and utilize familiar strategies, including.

a. Substitution: least significant bit of each pixel is substituted with bit corresponding to the data that is to be concealed in an 8-bit image. In 24-bit (RGB) image, one bit is added to each of the primary color channels.
b. Masking and Filtering.

Goes through stages:

a. Analyzing the image.
b. Determine the best places to further integrate hidden message.
c. With hold data in those regions.

Transform method:

The manipulation of coefficients in the transformation domain conceals the message. We utilize the discrete sine quantization and other transforms to discretize the less significant portions of an image.

Steganography Versus Cryptography:

Both methods essentially transmit data in a secure manner. A closer inspection may reveal the subsequent discrepancies:

a. Steganography is the technique of obscuring the presence of data, while cryptography involves the practice of safeguarding data against unauthorized access.
b. When not employed in conjunction with encryption methods, steganography remains unaltered by the data it obfuscates. Conversely, cryptography may modify the information directly to obscure it.
c. In contrast to cryptography, which centers on the difficulty of deciphering the cryptographic technique, steganography guarantees the absolute concealment of data.
d. Encoding data is an indispensable component of steganography. After mastering the methodology, steganography implementation becomes second nature.

The flowchart for the embedding algorithm in the ACO-LSB image steganography method, the process described the form of an algorithm and Extraction Process:

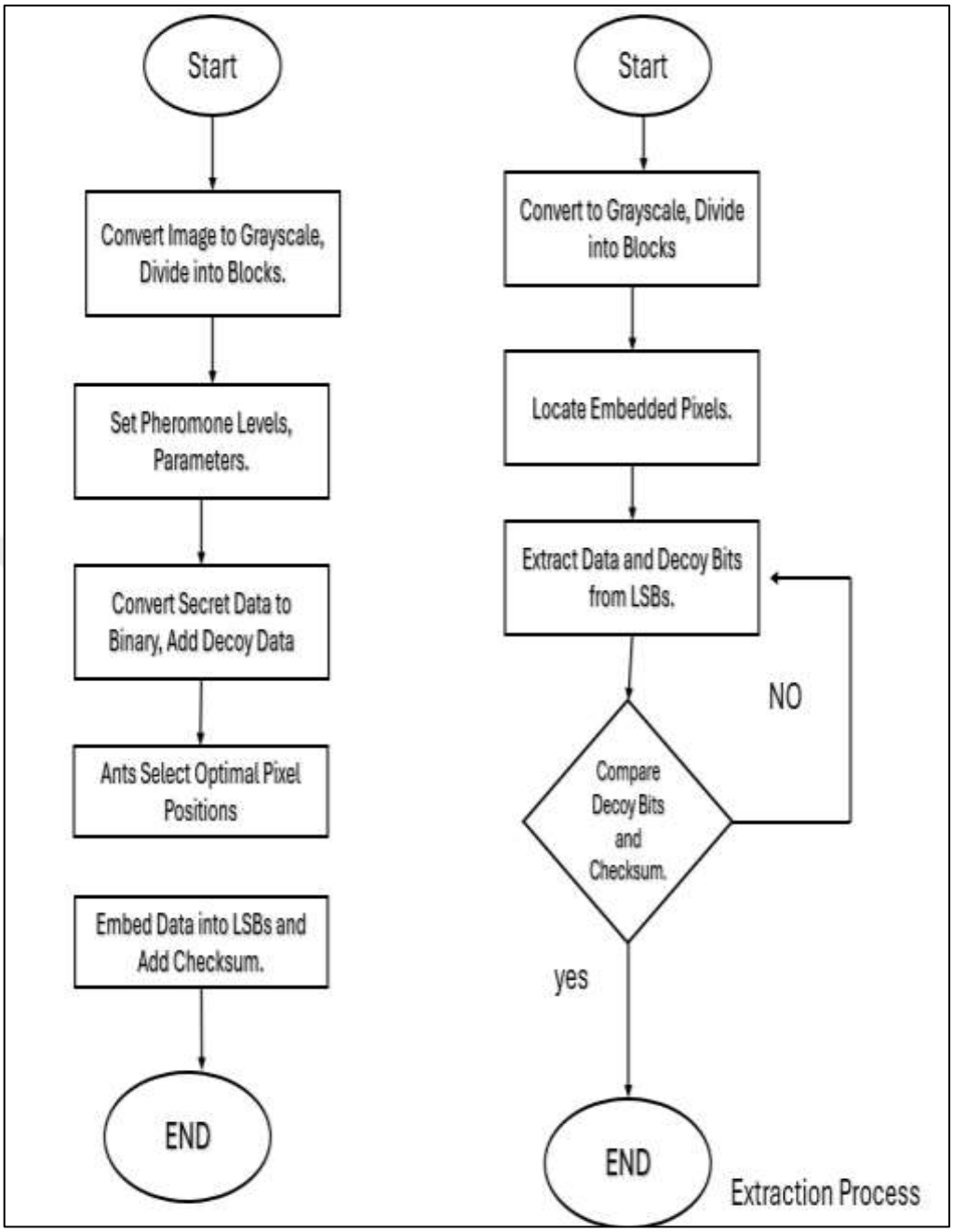

Figure 3.8: (a) Embedding Process, and (b) Extraction Process.

4. RESULTS

The simulation was constructed using the MATLAB R2023a system, using monochrome photos in the bmb format as cover components. Authenticity verification/decoy evidence and private information was introduced via substituting the four smallest bits (LSB) of cover pictures. For assessing the framework's efficacy, two primary indicators were employed: PSNR (Peak Signal-to-Noise Ratio), a measure of the distortion between the steganographic and the initial pristine picture, and recognition rate, that reflects the proportion of modified bytes identified throughout the attack stage. These measurements assist in assessing the system's detection efficacy during investigations.

The system produces specific results related to change detection, including:

a. Include of Identified Couple Examinations: This enumerates the byte places for every alteration’s bytes found in a covert image during an attack, verified in the extract-verify stage. The hash is generated by comparing bit pairs of the authentic private information alongside the falsified information. In the absence of a hash list, the image will be considered offline.
b. Checksum Discrepancy Results: The checksum is computed through the data extraction procedure alongside juxtaposed with the already implanted encrypted checksum. Any difference between these values indicates possible hidden image manipulation. The MATLAB algorithm calculates the checksum value.

The system effectively identifies modifications by employing pair comparisons and checksum analysis to detect alterations in the steganographic content.

4.1 EXPERIMENTAL DATA SET

The functionality of the suggested method was evaluated using BOSSbase1.01, which has 10,000 8-bit PGM grayscale pictures. BOSSbase1.01 is generally acknowledged as a premier photo database in the domains of digital image forensics and statistical analysis. It was designed for comparing steganography and steganalysis and comprises a vast number of grayscale images with the size of 512 × 512 pixels primarily saved in PNG format to avoid compression effects. The dataset is pretty much known for evaluating an ability to hide messages in imageries via various steganographic algorithms, plus intended for assessing

steganalysis methods intended to reveal these hidden messages. As a result, BOSSbase1.01 plays a key role in academic research, offering an essential tool for scientists to evaluate their methodologies as well as technology.

For the experiment, 1,000 images were selected from the dataset. The dataset was accessed on June 1, 2022, via the following

URL: https://dde.binghamton.edu/download/, with access verified on July 21, 2024. The Digital Data Embedding Lab at Binghamton University generated the dataset. Each image, with dimensions of 512 × 512 pixels and a file size of 256 KB, was used to embed the confidential image "Girl.bmp" using the spatial domain LSB method. The image "Girl.bmp," sourced from the USC-SIPI Image Database (2023), has a file size of 59.4 KB and dimensions of 142 × 142 pixels.

4.2 IMPLEMENTATION

Three modules are utilized in experimental work. The embedding module employs four-LSB steganography to hide the secret image within a set of 1,000 grayscale PGM (Portable GrayMap) cover images. Confidential picture information is included in the most essential bits (LSB) of each four-bit pair inside the stego byte. Copies, inverts, while stores the initial couple of bits of the right half-byte of the stego byte as dummy information for the hidden bit couple. The checksum value of the confidential information is then calculated and combined into a stego image.

The assault component alters the covert picture via substituting arbitrary amounts between 0 and fifteen for the bits in the right half of the bytes, that carry confidential information. This is intended to simulate an attack on the steganographic image[139]. A specified number of altered bytes is used to assess detection accuracy by comparing it with the actual number of modifications performed.

Via juxtapositions of the private with counterfeit bits, as well as checksums, the Extract-Verify software obtains the secret picture whilst concurrently confirming its integrity. Through matching the information produced through the gathering operation against the Embedded Checksum significance, it conducts a checksum analysis. Additionally, it creates a list of the places in the secret picture that have been removed wherein altered bytes were

found [68]. To increase the efficacy plus productivity of the embedding approach, the transport picture and the hidden photo are divided across four separate sections throughout the entire embedding procedure. This division is required for a number of causes one of which being easier management. An easier-to-manage hash gives you additionally authority over the embedding and extracting procedures, which lowers the possibility of mistakes and improves concealing data accuracy. Because spreading the concealed information through many bus picture segments, it further strengthens the scheme's security through rendering it easier to identify similarities or abnormalities utilizing embedded methods. Additionally, it maximizes the utilization of hardware capabilities by using smaller blocks, which enable the ant colony optimization algorithm to analyze data while identifying possible embedding locations inside each block. Higher embedding possibilities are achieved whilst preserving picture integrity because to this local improvement.

4.3 RESULTS AND DISCUSSION

In the course of the study, the ghost picture (Girl.bmp) was embedded among 1,000 grayscale photos taken through the (BOSSbase1.01) a database, demonstrating in Figure 4.1. In order for insertion the hidden information, the following procedures were taken: first, a forward bait was introduced; next, an opposite bait was inserted; and lastly, the confidential information was included without any bait, as shown in Figure 4.1.

Figure 4.1: The Hidden Picture.

The PSNR for embedding without a decoy is considerably greater compared to both of the suggested technique and the optimum amount of growth, given that the PSNR3 case

swapped just 2 bits per byte, while the suggested instances supplanted four bits per byte. The peak signal-to-noise ratio (PSNR) for improved ability exceeds which of the original technique, indicating which the suggested strategy offers greater disappearance as well as an improved way of hiding secret data (Table 4.1).

Table 4.1: PSNR Values for (30) of Images.

The cover picture	Embedding PSNR using decoy	PSNR for the PSO-LSB method	PSNR for the suggested strategy ACO-LSB	PSNR for the suggested capacities increase strategy
Girl.bmb1	43.1768	32.7456	29.2348	30.799
Girl.bmb2	43.177	32.746	29.235	30.768
Girl.bmb3	42.961	32.418	29.206	30.737
Girl.bmb4	42.746	32.094	29.176	30.706
Girl.bmb5	42.533	31.773	29.147	30.676
Girl.bmb6	42.320	31.455	29.118	30.645
Girl.bmb7	42.108	31.141	29.089	30.614
Girl.bmb8	41.898	30.829	29.060	30.584
Girl.bmb9	41.688	30.521	29.031	30.553
Girl.bmb10	41.480	30.216	29.002	30.522
Girl.bmb11	41.272	29.914	28.973	30.492
Girl.bmb12	41.066	29.615	28.944	30.461
Girl.bmb13	41.861	29.318	28.915	30.431
Girl.bmb14	40.656	29.025	28.886	30.401
Girl.bmb15	40.453	28.735	28.857	30.370
Girl.bmb16	40.231	28.448	28.828	30.340
Girl.bmb17	40.049	28.163	28.799	30.309
Girl.bmb18	39.849	27.881	28.771	30.279
Girl.bmb19	39.650	27.603	28.742	30.249
Girl.bmb20	39.452	27.327	28.713	30.219
Girl.bmb21	39.254	27.053	28.684	30.188
Girl.bmb22	39.058	26.783	28.656	30.158
Girl.bmb23	38.863	26.515	28.627	30.128
Girl.bmb24	38.669	26.250	28.598	30.098
Girl.bmb25	38.475	25.987	28.570	30.068
Girl.bmb26	38.283	25.728	28.541	30.038
Girl.bmb27	38.091	25.470	28.513	30.008
Girl.bmb28	37.901	25.216	28.484	29.978
Girl.bmb29	37.711	24.963	28.456	29.948
Girl.bmb30	37.523	24.714	28.427	29.918

Table 4.2: Average PSNR Values for (1000) Stego Images.

Embedding PSNR using decoy	PSNR for the [31] strategy	PSNR for the suggested strategy	PSNR for the suggested capacities increase strategy
43.07699	33.42934	29.5795	31.71444

The goal of the ACO-LSB approach is to equilibrium identification opposition, clarity of image, and capacity for incorporation throughout a wide range of situations. The ACO-LSB approach is intended for continuously trustworthy results over a range of picture kinds with embedding contexts, although expected approaches in the literature could perform better in particular situations. Against a focus on metrics including onboarding ability, PSNR, SSIM, and detection obstruction, we conducted further tests evaluating the ACO-LSB approach against a number of current steganographic methods reported in the primarily research. Particularly, the ACO-LSB approach demonstrated its power versus steganalysis by achieving a 15% drop in its identification measure when contrasted with the most recent methodologies.

An enlarged picture is shown in Fig. 8c, a steganographic photo in Fig. 8b, plus a pristine cover image in Fig. (4.2). The distinction among clean and steganographic pictures remains unclear even after the four LSBs have been replaced. Additionally, the stego picture that has the expanded capability that the initial stego image are identical. An alternate implantation technique was implemented to remove all irregularities from the pictures, utilizing two LSBs to encode fake data pairs in alternate bytes. This alternative embedding method uses the cover data picture Bird.jpg to create a steganographic picture, which is shown in Fig. 4.2. The largest amount of the confidential data is lowered approximately 50% while alternative embedding is used as opposed to the 4 LSB approach.

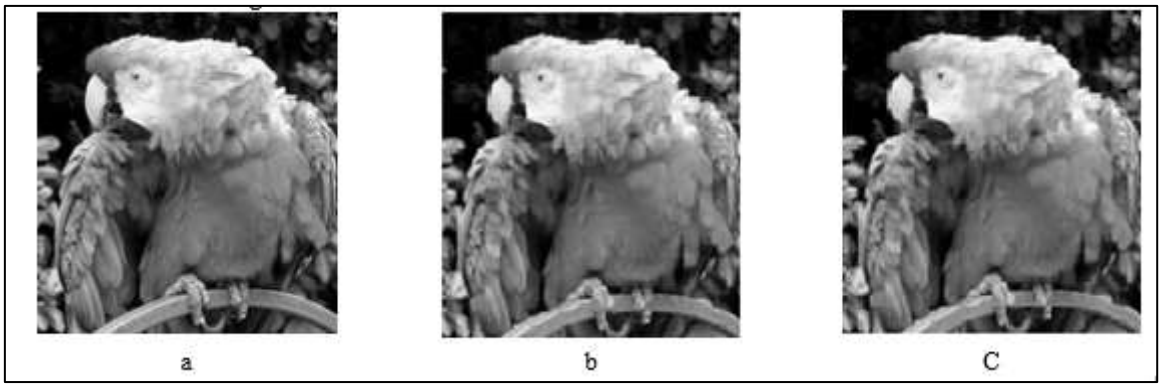

Figure 4.2: Stego Image with (A) Clean Image, Figure, (B) Proposed Approach, and (C) Proposed Expanded Capacity

4.4 ATTACK DETECTION RESULTS

The four least significant bits of each of the 51,200 bytes that were added to each suggested steganographic picture were swapped out for arbitrary numbers ranging from 0 to 15. Thousands of steganographic photographs were altered, along with the hidden message was obtained and made public using the Extract-Verify tool. Potential vulnerabilities in protection. The private picture that was acquired after the assault appears in Fig. (4.3). In the retrieved picture, the impact of the assault is evident, providing an important illustration of a modified file [140]. However, in real-world scenarios, documents assaults may go unnoticed because of differences in layout alongside subject matter.

Figure 4.3: The Extracted Secret Image After the Attack.

A pair-wise comparison was used to assess the first 30 photos' identification probability. The hidden picture made up one-fourth of the 12,800 changed bytes in the steganographic photos. A distinct byte was used to hold each pair of bits from the secret byte. The checksum comparison approach proved to be successful, despite the fact that the pair comparison method failed to detect some threats. The checksum is a crucial component in ensuring the correctness and integrity of the embedded data when secret information is being inserted. This number is used for confirmation throughout the procedure of extraction which is calculated using the confidential information before embedding. The checksum makes it easier to identify mistakes or changes made to the secret data during storage or transportation. A thorough assessment of the suggested ACO-LSB steganographic technique is provided in Table 4.3.

Table 4.3: A Deeper Examination of the Suggested ACO-LSB Steganographic Technique.

The cover picture	Exploit bytes discovered on Stego	Attacking bytes found on the concealed the picture	After growth, an attacking byteson hidden information was discovered.	Probability of identification
Girl.bmb1	38412	12748	12600	0.984375
Girl.bmb2	38600	12745	12530	0.978906
Girl.bmb3	38678	12675	12200	0.953125
Girl.bmb4	38874	12733	12680	0.990625
Girl.bmb5	38964	12634	12200	0.953125
Girl.bmb6	38489	12723	12350	0.964844
Girl.bmb7	38234	12635	12320	0.9625
Girl.bmb8	38603	12711	11900	0.929688
Girl.bmb9	38935	12745	11800	0.921875
Girl.bmb10	38094	12634	11820	0.923438
Girl.bmb11	38745	12654	11740	0.917188
Girl.bmb12	38846	12565	12300	0.960938
Girl.bmb13	38564	12703	11450	0.894531
Girl.bmb14	38434	12734	11230	0.877344
Girl.bmb15	38795	12721	12140	0.948438
Girl.bmb16	38312	12734	10900	0.851563
Girl.bmb17	38379	12600	11800	0.921875
Girl.bmb18	38936	12546	11460	0.895313
Girl.bmb19	38023	12544	11230	0.877344
Girl.bmb20	38187	12654	11560	0.903125
Girl.bmb21	38375	12717	12220	0.954688
Girl.bmb22	38637	12722	11980	0.935938
Girl.bmb23	38783	12632	10990	0.858594
Girl.bmb24	38974	12631	11890	0.928906
Girl.bmb25	38966	12743	12560	0.98125
Girl.bmb26	38648	12632	11950	0.933594
Girl.bmb27	38546	12754	11890	0.928906
Girl.bmb28	38493	12778	12200	0.953125
Girl.bmb29	38658	12689	11300	0.882813
Girl.bmb30	38648	12713	11450	0.894531

Extract-Verify utilizes pair comparison to generate a list detailing the updated bytes' positions plus information. Certain of those websites including all of the changed bytes from the first picture in the dataset, Girl.bmb 1, are shown in Table 7. This collection of altered bytes offers important information about the majority common types of attacks.

The proposed data-hiding method using the Ant Colony Optimization (ACO) algorithm and Least Significant Bit (LSB) technique offers high resistance to detection attempts, making it difficult for analysis techniques to uncover hidden data within the image. This strength is due to several key features inherent into the concurrent mixed approach. First, the ACO technique's adaptable discovery feature enables selecting the most suitable pixel coordinates for data embedding in the most useful criteria, which randomizes the direction of further

data hiding and makes several patterns resistant to the detection methods. Additionally, the ACO procedure's periodic iteration mechanism constantly enhances the concealment place and can effectively embed data so that it would be difficult for an intruder to easily point out such changes. Such adaptations assist to preserve the natural the statistical features of the background picture, that further complicates the detection process. It's crucial to highlight a few of the shortcomings of the suggested ACO-LSB method, nevertheless. Because the entire embedding and extraction steps take a lot of computational effort, among the primary disadvantages of using an ACO technique is an upsurge in mathematical workload. This is problematic while supplies are limited as well as immediate processing of information is necessary. Moreover, the method seems to be variable the consistency along with roughness within the picture could have consequences, based on the features of the headline picture. However, as the image becomes less complex or is uniform with a given spectrum, the number of optimal sites of embedding is few and could lead to decreased capacity as well as security. Additionally, the performance of the technique has not been thoroughly tested under challenging conditions, such as high compression of the hidden image or significant noise, which could impact embedding capacity and extraction accuracy would probably lead to issues with the procedure's dependability in practical implementations.

5. CONCLUSION

This research establishes the benefits of augmenting ACO with LSB in image steganography in enhancing the capacity. The proposed method addresses the main ACO assets efficiently, namely collaboration and flexibility of the approach, which enhances the embedding load while maintaining high image quality and resilience to detection. This paper presents the first experimental results showing that systems employing ACO have indeed higher capacity than classic steganographic techniques. Our technology indicates an improvement of about 34% on average compared to traditional methods in cases such as ACO-integrated LSB. Their methods ensured the study clocked a maximum embedding capacity of 2.5 bits per pixel given without much compromising the image quality compared to the approximated 2.0 bits per pixel achievable under similar conditions in classical techniques. The good PS values are verified by capacitance and imperceptibility tests and by comparing it with PSNR of the PSO-LSB method. It enhances embedding capability by sequential optimization and amendment of pheromone matrix. The inclusion of ACO into image steganography improves the level of data hiding exerts significantly. As for the future work, the further study might focus on the improvement of computational time and the ACO-LSB method's robustness under high compression and noise level circumstances. Besides, it is also an area that should be developed in the future so as to embed the mere LSBs, combining ACO-LSB with other steganographic methods can increase the security and the capacity of invisibility.

It can be summed up that ACO-LSB can introduce more strict security and higher carrying capacity and make a beneficial improvement to the image quality for data hiding in image. Thus, this method which combines the ACO algorithm with LSB technique allows to improve the pixel selection for data embedding so that more information can be hidden in the image while producing a minimal visually perceptible distortion. The ACO algorithm splits the hidden information into many areas thus avoiding areas easily targeted by the steganalaysis tools.The ACO-LSB technique retains the image quality and utilizes checksum verification that besides the effectiveness in verifying the originality of data, also includes decoy bits to any alteration or loss of the embedded data. This method to improve the security and availability of the concealed information, making it is most beneficial to applications where covert messaging or secure storage is needed. It concludes that ACO-LSB is a major improvement over prior art in the field of Steganography due to the greater embedding

capability, as well as the considerably increased robustness against detection and the addition of necessary integrity checks. It indicates that further research could investigate the way of enhancing the speed of this computation and using this technique in other types of media. In conclusion, ACO-LSB makes a meaningful contribution in enriching the contemporary efficient and secure data hiding schemes indispensable for the growth of covert communication technology.

5.1 FUTURE WORK

Based on the current work, the following recommendations are offered for future research:

a. Optimization of Computational Efficiency: Since the ACO algorithm might be time consuming due to the large number of iterations it can be a subject to optimization in further studies. Perhaps using parallel processing, GPU, or a less complex optimization algorithm that provides comparable results, but does so more efficiently could be researched as a way to improve the speed of the method for real-time use.

b. Adaptability to Color Images and Different Media Types: It is possible to strengthen the proposed method by further developing the ACO-LSB algorithm for color images or for any other media formats, such as video and audio. It implies that various types of media need to support the coloring channels or audio frequencies for embedding, which perhaps could be managed with ACO-based optimization.

c. Increased Robustness Against Image Processing Operations: The proposed method could be improved in the future to further resist common image processing treatments such as image compression, size changing, and noise injections. It would enhance the operation of ideas such as ACO-LSB in real-life situations whereby images are often subjected to change.

d. Hybrid Steganography Techniques: Most of all, integrating ACO-LSB with other steganographic or cryptographic methodologies can enhance the security status as well as the volume of covering capacity. Combination of the frequency-domain transformations, e.g., DCT, with ACO can be the potential improvement to provide further levels of security against steganalysis as well as more freedom in selection of the cost function.

e. Machine Learning-Enhanced Detection Resistance: Utilizing machine learning to fine-tune embedding patterns could help create data hiding schemes that are even more resistant to steganalysis. Due to the huge amount of data that can be generated in such designs, it would be possible to know which of the embedding patterns are least likely to be detected and hence optimized.

f. Integrity Verification for Complex Data: Research could focus on advanced integrity checks for complex data types or larger payloads. Enhancing checksum mechanisms, or incorporating error-correction codes, could make the method even more reliable, especially for applications requiring high security.

g. Application in Secure Communication Systems: Lastly, there is much utility in applying ACO-LSB within the trusted Secure shell, IoT devices, messaging applications, and secure cloud storage. Adapting this technique in those particular environments could prove the use of BSSB in actual secure data transfer application.

h. Extend the scope of the proposed model to include multi-channel images such as RGB (24-bit) and RGBA (32-bit).

i. Changed the form to handle changes to sensitive text documents, especially those containing many characters.

j. Explore alternative investment techniques, including adding fake data.

k. Explore improved data recovery methods using duplicate fake data.

REFERENCES

[1] ALRikabi, H. and H.T. Hazim, *Enhanced data security of communication system using combined encryption and steganography.* iJIM, 2021. 15(16): p. 145.

[2] Majeed, M.A., et al., *A review on text steganography techniques.* Mathematics, 2021. 9(21): p. 2829.

[3] Majeed, M.A. and R. Sulaiman, *AN IMPROVED LSB IMAGE STEGANOGRAPHY TECHNIQUE USING BIT-INVERSE IN 24 BIT COLOUR IMAGE.* Journal of Theoretical & Applied Information Technology, 2015. 80(2).

[4] Ali, A.H., et al., *High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain.* Multimedia Tools and Applications, 2018. 77(23): p. 31487-31516.

[5] Ayob, M., S.N.H.S. Abdullah, and Z. Ahmad, *Lightweight and Optimized Multi-Layer Data Hiding using Video Steganography.* International Journal of Advanced Computer Science and Applications, 2018. 9(12).

[6] Subramanian, N., et al., *Image steganography: A review of the recent advances.* IEEE access, 2021. 9: p. 23409-23423.

[7] Mandal, P.C., et al., *Digital image steganography: A literature survey.* Information sciences, 2022. 609: p. 1451-1488.

[8] Joshi, K., S. Gill, and R. Yadav, *A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image.* Journal of Computer Networks and Communications, 2018. 2018(1): p. 9475142.

[9] Rashid, A. and M.K. Rahim, *Critical analysis of steganography "an art of hidden writing".* Int. J. Secur. Its Appl, 2016. 10(3): p. 259-282.

[10] Sahu, A.K. and M. Sahu, *Digital image steganography and steganalysis: A journey of the past three decades.* Open Computer Science, 2020. 10(1): p. 296-342.

[11] Wu, Z., et al., *Steganography and steganalysis in voice over IP: A review*. Sensors, 2021. 21(4): p. 1032.

[12] Kadhim, I.J., et al., *Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research.* Neurocomputing, 2019. 335: p. 299-326.

[13] Naveenkumar, R., et al., *Enhancing Encryption Security Against Cypher Attacks*, in *Homomorphic Encryption for Financial Cryptography: Recent Inventions and Challenges*. 2023, Springer. p. 125-155.

[14] Apau, R. and C. Adomako, *Design of image steganography based on RSA algorithm and LSB insertion for android smartphones.* International Journal of Computer Applications, 2017. 164(1): p. 0975-8887.

[15] Muhammad, K., et al., *A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image.* Multimedia Tools and Applications, 2016. 75: p. 14867-14893.

[16] C. Alipour, M., B. D. Gerardo, and R. P. Medina. *LSB substitution image steganography based on randomized pixel selection and one-time pad encryption*. in *Proceedings of the 2020 2nd International Conference on Big-data Service and Intelligent Computation*. 2020.

[17] Chan, C.-K. and L.-M. Cheng, *Hiding data in images by simple LSB substitution.* Pattern recognition, 2004. 37(3): p. 469-474.

[18] Mielikainen, J., *LSB matching revisited.* IEEE signal processing letters, 2006. 13(5): p. 285-287.

[19] Luo, W., F. Huang, and J. Huang, *Edge adaptive image steganography based on LSB matching revisited.* IEEE Transactions on information forensics and security, 2010. 5(2): p. 201-214.

[20] Liu, G., Z. Zhang, and Y. Dai, *Improved LSB-matching steganography for preserving second-order statistics.* Journal of Multimedia, 2010. 5(5): p. 458.

[21] Sun, S., *A novel edge based image steganography with 2k correction and Huffman encoding.* Information Processing Letters, 2016. 116(2): p. 93-99.

[22] Yaseen, Z.F. and A.A. Kareem. *Image steganography based on hybrid edge detector to hide encrypted image using vernam algorithm*. in *2019 2nd Scientific Conference of Computer Sciences (SCCS)*. 2019. IEEE.

[23] Gaurav, K. and U. Ghanekar, *Image steganography based on Canny edge detection, dilation operator and hybrid coding.* Journal of Information Security and Applications, 2018. 41: p. 41-51.

[24] Prasad, S. and A.K. Pal. *Logistic map-based image steganography scheme using combined LSB and PVD for security enhancement*. in *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018, Volume 3*. 2019. Springer.

[25] Bailey, K. and K. Curran, *An evaluation of image based steganography methods.* Multimedia Tools and Applications, 2006. 30: p. 55-88.

[26] Muhammad, K., et al., *A secure cyclic steganographic technique for color images using randomization.* arXiv preprint arXiv:1502.07808, 2015.

[27] Gutub, A.A.-A., *Pixel indicator technique for RGB image steganography.* Journal of emerging technologies in web intelligence, 2010. 2(1): p. 56-64.

[28] Panwar, S., M. Kumar, and S. Sharma. *Digital image steganography using modified lsb and aes cryptography*. in *4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019: Internet of Things and Connected Technologies*. 2020. Springer.

[29] Pandey, J., et al. *Pixel indicator steganography technique with enhanced capacity for RGB images*. in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. 2019. IEEE.

[30] Zhang, X. and S. Wang, *Efficient steganographic embedding by exploiting modification direction.* IEEE Communications letters, 2006. 10(11): p. 781-783.

[31] Arivazhagan, S., E. Amrutha, and W.S.L. Jebarani, *Universal steganalysis of spatial content-independent and content-adaptive steganographic algorithms using normalized feature derived from empirical mode decomposed components.* Signal Processing: Image Communication, 2022. 101: p. 116567.

[32] Younus, Z.S. and M.K. Hussain, *Image steganography using exploiting modification direction for compressed encrypted data.* Journal of King Saud University-Computer and Information Sciences, 2022. 34(6): p. 2951-2963.

[33] Abraham, A. and M. Paprzycki. *Significance of steganography on data security*. in *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.* 2004. IEEE.

[34] Mohamed, N., et al., *L* a* b* color space high capacity steganography utilizing quad-trees.* Multimedia Tools and Applications, 2020. 79(33): p. 25089-25113.

[35] Rajput, G. and R. Chavan. *A Novel Approach for Image Steganography Based on Random LSB Insertion in Color Images*. in *Proceedings of the International Conference on Intelligent Computing Systems (ICICS 2017–Dec 15th-16th 2017) organized by Sona College of Technology, Salem, Tamilnadu, India*. 2017.

[36] Gouthamanaath, M.G. and A. Kangaiammal. *Hiding three binary images in a grayscale image with pixel matching steganography and randomization technique*. in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*. 2018. IEEE.

[37] Ehsan Ali, U., et al., *A LSB based image steganography using random pixel and bit selection for high payload.* 2021.

[38] Pichardo-Méndez, J., et al., *LSB pseudorandom algorithm for image steganography using skew tent map.* Arabian Journal for Science and Engineering, 2020. 45: p. 3055-3074.

[39] Pak, C., et al., *A novel color image LSB steganography using improved 1D chaotic map.* Multimedia Tools and Applications, 2020. 79(1): p. 1409-1425.

[40] Gahan, A. and G.D. Devanagavi. *A secure steganography model using random-bit select algorithm*. in *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*. 2020. IEEE.

[41] Al-Husainy, M.A.F. and D.M. Uliyan, *A secret-key image steganography technique using random chain codes.* International Journal of Technology, 2019. 10(4): p. 731-740.

[42] Laimeche, L., A. Meraoumia, and H. Bendjenna, *Enhancing LSB embedding schemes using chaotic maps systems.* Neural Computing and Applications, 2020. 32(21): p. 16605-16623.

[43] Mondal, B., *A secure steganographic scheme based on chaotic map and DNA computing*, in *Micro-Electronics and Telecommunication Engineering: Proceedings of 3rd ICMETE 2019*. 2020, Springer. p. 545-554.

[44] Dumre, R. and A. Dave. *Exploring lsb steganography possibilities in rgb images*. in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. 2021. IEEE.

[45] Abdel-Aziz, M.M., K.M. Hosny, and N.A. Lashin, *Improved data hiding method for securing color images.* Multimedia Tools and Applications, 2021. 80(8): p. 12641-12670.

[46] Maji, G., S. Mandal, and S. Sen, *Cover independent image steganography in spatial domain using higher order pixel bits.* Multimedia Tools and Applications, 2021. 80(10): p. 15977-16006.

[47] Rahman, S., et al., *A novel approach of image steganography for secure communication based on LSB substitution technique.* Computers, Materials & Continua, 2020. 64(1): p. 31-61.

[48] Kareem, H.R., H.H. Madhi, and K.A.-A. Mutlaq, *Hiding encrypted text in image steganography.* Periodicals of Engineering and Natural Sciences (PEN), 2020. 8(2): p. 703-707.

[49] Tasheva, A., Z. Tasheva, and P. Nakov. *Image based steganography using modified lsb insertion method with contrast stretching*. in *Proceedings of the 18th International Conference on Computer Systems and Technologies*. 2017.

[50] Shelke, F.M., A.A. Dongre, and P.D. Soni, *Comparison of different techniques for Steganography in images.* International Journal of Application or Innovation in Engineering & Management, 2014. 3(2): p. 171-176.

[51] RANDOM, S.S.U.T., *An effective and secure digital image steganography scheme using two random function and chaotic map.* Journal of Theoretical and Applied Information Technology, 2020. 98(01).

[52] Kordov, K. and S. Zhelezov, *Steganography in color images with random order of pixel selection and encrypted text message embedding.* PeerJ Computer Science, 2021. 7: p. e380.

[53] Zhang, X., F. Peng, and M. Long, *Robust coverless image steganography based on DCT and LDA topic classification.* IEEE Transactions on Multimedia, 2018. 20(12): p. 3223-3238.

[54] Deshmukh, P.V., et al., *High capacity reversible data hiding in encrypted images using multi-MSB data hiding mechanism with elliptic curve cryptography*. Multimedia Tools and Applications, 2023. 82(18): p. 28087-28115.

[55] Laskar, S.A. and K. Hemachandran, *A review on image steganalysis techniques for attacking steganography*. International Journal of Engineering Research and Technology, 2014. 3(1).

[56] Kaur, M., V. Kumar, and D. Singh, *An efficient image steganography method using multiobjective differential evolution*, in *Digital Media Steganography*. 2020, Elsevier. p. 65-79.

[57] AlFaqawi, L., M. AbuHaya, and T. Barhoom. *Alpha channel-Based Indicator For Robustness Forward/Backward LSB Steganography*. in *2021 Palestinian International Conference on Information and Communication Technology (PICICT)*. 2021. IEEE.

[58] Hong, W., T.-S. Chen, and C.-W. Luo, *Data embedding using pixel value differencing and diamond encoding with multiple-base notational system.* Journal of Systems and Software, 2012. 85(5): p. 1166-1175.

[59] Wu, D.-C. and W.-H. Tsai, *A steganographic method for images by pixel-value differencing.* Pattern recognition letters, 2003. 24(9-10): p. 1613-1626.

[60] Rathika, L., et al., *Approaches and methods for steganalysis–A survey.* Int. J. Advan. Res. in Comp. and Communic. Engr, 2017. 6(6): p. 433-438.

[61] Hussain, M., et al., *Image steganography in spatial domain: A survey.* Signal Processing: Image Communication, 2018. 65: p. 46-66.

[62] Girdhar, A. and V. Kumar, *Comprehensive survey of 3D image steganography techniques.* IET Image Processing, 2018. 12(1): p. 1-10.

[63] Meng, R., Q. Cui, and C. Yuan, *A survey of image information hiding algorithms based on deep learning.* Computer Modeling in Engineering & Sciences, 2018. 117(3): p. 425-454.

[64] Qin, J., et al., *Coverless image steganography: a survey.* IEEE access, 2019. 7: p. 171372-171394.

[65] Puteaux, P., et al., *A survey of reversible data hiding in encrypted images–the first 12 years.* Journal of Visual Communication and Image Representation, 2021. 77: p. 103085.

[66] Khan, S. and T. Bianchi, *Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region.* International Journal of Electrical & Computer Engineering (2088-8708), 2018. 8(1).

[67] Loukhaoukha, K., J.-Y. Chouinard, and M.H. Taieb, *Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization.* J. Inf. Hiding Multim. Signal Process., 2011. 2(4): p. 303-319.

[68] Banharnsakun, A., *Artificial bee colony approach for enhancing LSB based image steganography*. Multimedia Tools and Applications, 2018. 77(20): p. 27491-27504.

[69] Walia, G.S., et al., *Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map.* Optik, 2018. 170: p. 106-124.

[70] Pandey, H.M., *Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography.* Future Generation Computer Systems, 2020. 111: p. 213-225.

[71] Alhelow, H., *Highly Secure Steganography-Based System with Three Layers of Protection.* No. 5544. EasyChair Preprint, 2021.

[72] Yin, S. and H. Li, *GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system.* Evolutionary Intelligence, 2021. 14: p. 1817-1829.

[73] Shanthakumari, R., et al. *Data hiding in image steganography using range technique for secure communication*. in *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*. 2021. IEEE.

[74] Tiwari, K. and S.J. Gangurde. *LSB steganography using pixel locator sequence with AES*. in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*. 2021. IEEE.

[75] Arivazhagan, S., et al., *Hybrid convolutional neural network architecture driven by residual features for steganalysis of spatial steganographic algorithms.* Neural Computing and Applications, 2021. 33: p. 11465-11485.

[76] Baziyad, M., et al., *Polynomial fitting: enhancing the stego quality of DCT-based Steganography schemes.* Multimedia Tools and Applications, 2022. 81(30): p. 43999-44019.

[77] Awadallah, M.A., et al., *Multi-objective Ant Colony Optimization.* Archives of Computational Methods in Engineering, 2024: p. 1-43.

[78] Bernard, S., et al., *Backpack: A backpropagable adversarial embedding scheme.* IEEE Transactions on Information Forensics and Security, 2022. 17: p. 3539-3554.

[79] Bui, T., et al. *Rosteals: Robust steganography using autoencoder latent space*. in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2023.

[80] Liu, Y., Z. Wang, and J. Liu, *A Quick Pheromone Matrix Adaptation Ant Colony Optimization for Dynamic Customers in the Vehicle Routing Problem.* Journal of Marine Science & Engineering, 2024. 12(7).

[81] Hue, T.T.K., et al. *Data Hiding in Bit-plane Medical Image Using Chaos-based Steganography*. in *2021 International Conference on Multimedia Analysis and Pattern Recognition (MAPR)*. 2021. IEEE.

[82] Nancharla, B.K. and M. Dua. *An image encryption using intertwining logistic map and enhanced logistic map*. in *2020 5th international conference on communication and electronics systems (ICCES)*. 2020. IEEE.

[83] Talhaoui, M.Z., X. Wang, and A. Talhaoui, *A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme.* The Visual Computer, 2021. 37(7): p. 1757-1768.

[84] Chhikara, S. and R. Kumar, *An information theoretic image steganalysis for LSB steganography.* Acta Cybernetica, 2020. 24(4): p. 593-612.

[85] Cogranne, R., Q. Giboulot, and P. Bas, *Efficient steganography in JPEG images by minimizing performance of optimal detector*. IEEE Transactions on Information Forensics and Security, 2021. 17: p. 1328-1343.

[86] Darwis, D. and N. Pamungkas. *Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness*. in *Journal of Physics: Conference Series*. 2021. IOP Publishing.

[87] Hemalatha, J., et al., *Towards improving the performance of blind image steganalyzer using third-order SPAM features and ensemble classifier*. Journal of Information Security and Applications, 2023. 76: p. 103541.

[88] Dhawan, S. and R. Gupta, *Analysis of various data security techniques of steganography: A survey*. Information Security Journal: A Global Perspective, 2021. 30(2): p. 63-87.

[89] Juarez-Sandoval, O., et al. *Compact image steganalysis for LSB-matching steganography*. in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*. 2017. IEEE.

[90] Westfeld, A. and A. Pfitzmann. *Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools-and some lessons learned*. in *International workshop on information hiding*. 1999. Springer.

[91] Fridrich, J., M. Goljan, and R. Du. *Reliable detection of LSB steganography in color and grayscale images*. in *Proceedings of the 2001 workshop on Multimedia and security: new challenges*. 2001.

[92] Bernal-Romero, J.C., et al., *A review on protection and cancelable techniques in biometric systems.* Ieee Access, 2023. 11: p. 8531-8568.

[93] Sarangi, A.K. and R.P. Pradhan, *ICT infrastructure and economic growth: A critical assessment and some policy implications.* Decision, 2020. 47(4): p. 363-383.

[94] Aljarf, A., H. Zamzami, and A. Gutub, *Is blind image steganalysis practical using feature-based classification?* Multimedia Tools and Applications, 2024. 83(2): p. 4579-4612.

[95] Ma, Y., et al., *Adaptive feature selection for image steganalysis based on classification metrics.* Information Sciences, 2023. 644: p. 118973.

[96] Sajasi, S. and A.-M.E. Moghadam, *An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method*. Applied Soft Computing, 2015. 30: p. 375-389.

[97] Chefranov, A.G. and G. Öz, *Adaptive to pixel value and pixel value difference irreversible spatial data hiding method using modified LSB for grayscale images.* Journal of Information Security and Applications, 2022. 70: p. 103314.

[98] Eid, W.M., et al., *Digital image steganalysis: current methodologies and future challenges.* Ieee Access, 2022. 10: p. 92321-92336.

[99] Apau, R. and S.A. Gyamfi, *Data hiding in audio signals using elliptic curve cryptography, huffman code algorithm and low-bit encoding.* International Journal of Computer Applications, 2018. 180: p. 24-34.

[100] Hemalatha, S., U.D. Acharya, and A. Renuka, *Wavelet transform based steganography technique to hide audio signals in image.* Procedia Computer Science, 2015. 47: p. 272-281.

[101] Garg, M., J.S. Ubhi, and A.K. Aggarwal, *Neural style transfer for image steganography and destylization with supervised image to image translation.* Multimedia Tools and Applications, 2023. 82(4): p. 6271-6288.

[102] Sun, Y. and F. Liu. *Selecting cover for image steganography by correlation coefficient*. in *2010 Second International Workshop on Education Technology and Computer Science*. 2010. IEEE.

[103] Tseng, H.-W. and H.-S. Leng, *A reversible modified least significant bit (LSB) matching revisited method.* Signal Processing: Image Communication, 2022. 101: p. 116556.

[104] Jan, A., S.A. Parah, and B.A. Malik. *A novel Laplacian of Gaussian (LoG) and chaotic encryption based image steganography technique*. in *2020 International Conference for Emerging Technology (INCET)*. 2020. IEEE.

[105] Rustad, S., P.N. Andono, and G.F. Shidik, *Digital image steganography survey and investigation (goal, assessment, method, development, and dataset).* Signal processing, 2023. 206: p. 108908.

[106] Wang, Y., M. Tang, and Z. Wang, *High-capacity adaptive steganography based on LSB and Hamming code.* Optik, 2020. 213: p. 164685.

[107] Kaur, M., et al., *EGCrypto: a low-complexity elliptic galois cryptography model for secure data transmission in IoT.* IEEE Access, 2023.

[108] Giboulot, E., P. Bas, and R. Cogranne, *Multivariate side-informed Gaussian embedding minimizing statistical detectability.* IEEE Transactions on Information Forensics and Security, 2022. 17: p. 1841-1854.

[109] Chuang, Y.-H., et al., *Steganography in RGB images using adjacent mean.* IEEE access, 2021. 9: p. 164256-164274.

[110] Kaur, S., et al., *A systematic review of computational image steganography approaches.* Archives of Computational Methods in Engineering, 2022. 29(7): p. 4775-4797.

[111] Zhang, J., et al., *Improving the robustness of JPEG steganography with robustness cost.* IEEE Signal Processing Letters, 2021. 29: p. 164-168.

[112] Saeed, A., et al., *An accurate texture complexity estimation for quality-enhanced and secure image steganography.* IEEE Access, 2020. 8: p. 21613-21630.

[113] Laishram, D. and T. Tuithung, *A novel minimal distortion-based edge adaptive image steganography scheme using local complexity: (BEASS).* Multimedia Tools and Applications, 2021. 80(1): p. 831-854.

[114] Datta, B., K. Dutta, and S. Roy, *Data hiding in virtual bit-plane using efficient Lucas number sequences.* Multimedia Tools and Applications, 2020. 79: p. 22673-22703.

[115] Biswas, K. *A New Pixel Value Decomposition based Image Steganography Method*. in *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*. 2020. IEEE.

[116] Al-Roithy, B. and A. Gutub, *Trustworthy image security via involving binary and chaotic gravitational searching within PRNG selections.* Int. J. Comput. Sci. Netw. Secur, 2020. 20(12): p. 167-176.

[117] Almayyahi, A.A., et al., *High-security image steganography technique using XNOR operation and fibonacci algorithm.* International Journal of Advanced Computer Science and Applications, 2020. 11(10).

[118] Di Caro, G. and M. Dorigo, *Ant colony optimization and its application to adaptive routing in telecommunication networks*. 2004, PhD thesis, Faculté des Sciences Appliquées, Université Libre de Bruxelles ….

[119] ZULQARNAIN, M., et al., *AN EFFICIENT METHOD OF DATA HIDING FOR DIGITAL COLOUR IMAGES BASED ON VARIANT EXPANSION AND MODULUS FUNCTION.* Journal of Engineering Science and Technology, 2021. 16(5): p. 4160-4180.

[120] Ghosal, S.K., A. Chatterjee, and R. Sarkar, *Image steganography based on Kirsch edge detection.* Multimedia Systems, 2021. 27(1): p. 73-87.

[121] Piya, A., *High capacity and optimized image steganography technique based on ant colony optimization algorithm.* IJISCS (International Journal of Information System and Computer Science), 2019. 3(1): p. 15-26.

[122] Loan, N.A., et al., *Secure and robust digital image watermarking using coefficient differencing and chaotic encryption.* IEEE Access, 2018. 6: p. 19876-19897.

[123] El_Rahman, S.A., *A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information.* Computers & Electrical Engineering, 2018. 70: p. 380-399.

[124] Himthani, V., et al., *Comparative performance assessment of deep learning based image steganography techniques.* Scientific Reports, 2022. 12(1): p. 16895.

[125] Roy, S. and M.M. Islam, *A hybrid secured approach combining LSB steganography and AES using mosaic images for ensuring data security.* SN Computer Science, 2022. 3(2): p. 153.

[126] Chatterjee, A., S.K. Ghosal, and R. Sarkar, *LSB based steganography with OCR: an intelligent amalgamation.* Multimedia tools and applications, 2020. 79(17): p. 11747-11765.

[127] Zhang, X., et al., *Provably secure public-key steganography based on elliptic curve cryptography.* IEEE Transactions on Information Forensics and Security, 2024.

[128] Kalita, M., T. Tuithung, and S. Majumder, *An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique.* Cryptologia, 2019. 43(5): p. 414-437.

[129] Chen, Y., et al., *Cost reassignment for improving security of adaptive steganography using an artificial immune system.* IEEE Signal Processing Letters, 2022. 29: p. 1564-1568.

[130] Shah, D., et al., *Cryptographically strong SP boxes and their application in steganography.* Journal of Information Security and Applications, 2022. 67: p. 103174.

[131] Kaneria, S. and V. Jotwani, *Comparative performance analysis of deep learning-based image steganography using U-Net, V-Net, And U-Net++ encoders.* Image, 2024. 13: p. 20.

[132] Margalikas, E. and S. Ramanauskaitė, *Image steganography based on color palette transformation in color space.* EURASIP Journal on Image and Video Processing, 2019. 2019(1): p. 82.

[133] Zhu, L., et al., *Inverse interpolation and its application in robust image steganography.* IEEE Transactions on Circuits and Systems for Video Technology, 2021. 32(6): p. 4052-4064.

[134] Li, H., et al., *A siamese inverted residuals network image steganalysis scheme based on deep learning.* ACM Transactions on Multimedia Computing, Communications and Applications, 2023. 19(6): p. 1-23.

[135] Murthy, G.K., *Image Steganography using Fusion Based Advanced Encryption Algorithm and Embedding Techniques.*

[136] 136. Prasad, S., A.K. Pal, and S. Mukherjee, *An RGB color image steganography scheme by binary lower triangular matrix.* IEEE Transactions on Intelligent Transportation Systems, 2023. 24(7): p. 6865-6873.

[137] Qiu, J. *Generative Image Steganography Scheme Based on Deep Learning*. in *2022 International Conference on Education, Network and Information Technology (ICENIT)*. 2022. IEEE.

[138] Das, D., A. Durafe, and V. Patidar, *An Efficient Lightweight LSB Steganography with Deep Learning Steganalysis*, in *Computational Intelligence in Image and Video Processing*. 2023, Chapman and Hall/CRC. p. 131-154.

[139] Sultana, H., et al., *A novel hybrid edge detection and LBP Code-Based Robust Image Steganography method.* Future Internet, 2023. 15(3): p. 108.

[140] Zeng, L., et al., *Advanced image steganography using a U-Net-based architecture with multi-scale fusion and perceptual loss.* Electronics, 2023. 12(18): p. 3808.