Enhanced Multi-Level Image Steganography Using LSB & Hybrid AES-Blowfish Encryption Algorithm

Submitted By

Saadi Mohammed Chowdhury

ID: 212-35-735

Department of Software Engineering

Daffodil International University

Supervised By

Ms. Nadira Islam

Assistant Professor

Department of Software Engineering

Daffodil International University

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

APPROVAL

This thesis titled on "Enhanced Multi-Level Image Steganography Using LSB & Hybrid AES-Blowfish Encryption Algorithm", submitted by Saadi Mohammed Chowdhury **(ID: 212-35-735)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. S M **Hasan** Mahmud
Associate **Professor**
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Esaminer 1

Tapushe Rabaya Toma
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Khalid Been Badruzzaman Biplob
Lecturer (Senior Scale)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Dr. Md. Sazzadur Rahman
Professor
Institute of Information Technology
Jahangirnagar University

SUPERVISOR's DECLARATION

I hereby delare that I have checked this thesis and in my opinion this thesis is adequate in terms ofscope and qualiy for the award of the dgree of Bacelor of Science.

(Supervisor’s Signature)

Full Name : Ms. Nadira Islam

Position : Assistant Professor

Date : 22 September 2025

STUDENT's DECLARATION

I hereby declare tat the work in this thsisis based on my originawork except for quottions and ctations which hae been duly acknowledged. I also dclare that it has not een previosly or conurrently submitted for any ther degree at affodil nternaionalUiversity orany other insittion.

(Students's Signature)

Full Name : Saadi Mohamed Chowdhury

ID : 212-35-735

Date : 12 August 2025

Enhanced Multi-Level Image Stegnography Using LSB & Hybrid AES-Blowfish Encryption Algorithm

Saadi Mohammed Chowdhury

212-35-735

Thesis submitted in fulfilment of the reqirements for the award of the degree of Bachelor of Science

Department of Software Engineering

DAFFODIL INTERNATIONAl UNIVERSITY

August 2025

ACKNOWLEDGMENT

First and foemst, all praise be to Alighty Allah who has conantly helped me throughout my bachelor' and this hesis writing process. would ike to tae this important oportunity to than mamily. To my parents, tankyou for your unnditonal love, the ptince you have sown e and for always blieving in me. But foremost, I want t thank y superviso Ms. Nadir Islam lecturer,of Software Engieering for his utmostsupport, relief ad guidance. H guidance has been invalable in shaping his thesis. From thebottom of my heart, thnkful to all my respected/great teachers wh taught me. And I feel vy fortunate to have them as y teachers. Title: Thanks to the Adminstratve staff of Daffodil nternational Univrsity Thanks to the Administrative stff of Daffodil ntenational Univerity My sinere gratitue to all those who helped me to omplee this thsis. our support has maethis achievment possible.

DEDICATION

I dedicate tis work to my metors nd instructors; thnk you for metring me with your wisdom and exertise; this has been much helped in craing my work. Finally, I ediate my tesis to all future cademics an students aing to significantly contribute i the subject of fog computing security and cybercurity. This work shoul motivate more cretivity ad commitentin strivin greatness.

ABSTRACT

In this thesis, we ropose an advanced multi-evel image steanography system that cmbines zlib compresson, hybrid AES-56-Blowfish encyption, and LSB mbedding for better ecurity and image quality in secret commuication. We proose integrating key innovationsthat also relieve some of the critical limiations of curren steganographic methds: 1) Maxium Zlib Compression using the LZ7 algorithm for efficiency2) Upgraded AS-256-GCM replacng the conventinal AES-128 for direct ut ore secure encryption 3) Hybrid ES-Blowfish encyption architecure providing multi-layered efense with authenticationcapabilities. An image-dependent key erivation using imageindependent RGB histogram analyss with PBKDF2 algorithm construct unique and rliably strong encryption keys for every coer image.

This methodoogy comprises four ke steps, the first of which is a lossy copression of the message with the lvel 9 in zlib algrithm, then a double layer-enrypting with both AS-256-GCM and Blwfish-ECB andPKCS7 pdding, followed by step-ise Least Significant Bit (LSB) steganography embeddng into the RGB cannels, as well as an i-depth quaity assessment using Peak Signal-to-Noie Ratio (PSR) and Mean Square rror (MSE) metrics. e perform the experimental validation o some standard testimages such as te Lena and Baboon images to show that our method givs superior performace with the Peak Signal-o-Noise Ratio (PSNR) of the restored imag as high as 80.0 dB and 76.17 dB resectively, with spatial reresentation with minimal visual distortion ad maintaining the qality of images. Our itegrated compression provides a data reduction of up t 39.29% while eficiently keeping he encryption tie under 0.11 seconds.

A comparion demonstrtes that the qualty of ourconstruction povides signiicant advantages over existing mplementations: ES-256 vs. AES-128 pgrae results in mproved security; additional compression results in effiiency improvements; and GCM moe tamper etection provides authenticated ncryptionwhile improving encryptio fficiency as well. Interestingly, this research improvs cybersecurity to find high security, thebest image quality, and processing efficiency throug simultaneos multi-level steganography. The proposed system holds great promise for secure communicaton applicationsin military, medical, and digital rights management area and sets new performance standards for image-based covert commuication systems by emplying software engineering approaches.

KEYWORDS: Image Stganography, LSB Embedding,AES-256 Encryption, Bowfish Algorithm, ybrid Encryption, DataCompression, PSNR Quality Assessment, ybersecu

Table of Contents

List of Figures

CHAPTER 1: INTRODCTION

1.1 Background

The modern world run on digtal comunication with billions of iages flown through te networks of the world on a dily basis. While the nprecedented increase of digital mediausage opened new means for secur communication, it has also represeted tremendous challenges for data protection. The ancient art f concealing messages, seganography, hasbecome a sophisticated way to secure digital citien data by hiding an information in cover edia such that no one gets aware of the hidden inormation.

Image steganography is terefore an important building lock in the modern cybersecrity infrastructure, which rovides secret communiation and is an important part of the oolbox for sensitive applications. However, unlie cryptography, which conerts data into unreadale formats that indicate the exisence of hidden information steganography preerves the appearance of normal communicatin in a signal and obscures th message itself [9]. The dual-layer protection method leerages both the encryption securit and the scramblingprivacy of steganography.

The Least Signficant Bit (LSB) method has been the siplest and most effectiveof all image steganography methos in the Spatial domain [2]. Least Sigificant Bit (LSB) stegaography works by modifying theleast significant bits of pixe values, using the fact that te human visual system is not very senstive to small changes in pixelvalues. But traditional LSB models are greatly lmited by the type of used scurity models, compression inegration and susceptibility of teganalysis attacks.

Most of the curent steganographic approache are based on single-laer encryptions, and ostly AES-128 encryption, whic is not a high-level security againstcomputationaly intensive attacks. Traditional iplementations do not ompress the data that is beng hidden, leadig to larger payloads that lessens ebedding efficiency an increases risk of detection.In adition, the currentmechanisms lack solid authentication proces to confirm message integrity and identif tamperin efforts.

1.2 Problem Statment

Howevr, nowadays iage steganography sstems do have number o significant aknesses which make them hardly applicable to high-security cenarios. It faces sevral challenges weak encryption, no built-in compresson, weak authenticaton, and poor memoy management.

Many impleentations of traditional LS steganography ostly rely on AES-128 encyption, offering up to 128-bitsecurity levels hat may soon e susceptible tonew comutational capabilities ad extensie attack vectors. This bsence of hybrid encryptin architecturesgives rise to a limited overall secrity footprint creatig single poins of failure in the cryptgraphic sheler

chain. Also, plain systes do not deply authenticated ecryption mode and as a rsult, are prone to tampering and modiication attaks as they do not hae proper detection mchanisms.

Most of the curent work in steg-systems are still adry land o integration of th data compresson space (leveraging LSB substittion directly) hence a ig wastage of te payload as well as a higher embedding capaity is required In the absence of compressin, since the secret messages are present i maximum bit space inside the coer images, this may lead to low-quality images anda high sttistical chancef detection. This lmitation has paticular impact on applications that reuire large mesages or need to preserve image quality.

Several crrent key derivation mecanisms in steganographic systems are staic or too naive to exploit the properties of cover images. This wakness poses otential risks in such a way that the same keys mght be genrated for different images, which causes the overall security entropy to be reducd and predictable patterns tat can be exploited by attackers.

In many exising systems, uality assessment reies on miimal metrics and laks an evaluation framework to assist in optiizing the trade-off etween embedding capcity, security stength, and visual imperceptibility. Stanard performance bencharks are in no way available, whichmakes comaring various appraches and valdating improvements objetively impossible.

1.3 Reseach Objectives

Priary Objective

To dvelop an enhancd multi-level iage steganoraphy system that intgrates compression, hybrid encryption, and avanced LSB techniques to achieve superio securiy, efficiency, and image qualit compared o existing implementations.

Specific Objetives

1. Compession Intgration Enhanceent

Impement zlib compresson using LZ77 algorithm to reuce secret message payloa size, thereby improing embedding efficiencyand reducig statistical detectability whil maintaining message itegrity throughout thecompression-decomression cycle.

2. Cryptgraphic Scurity Advacement

Upgrade encrption strength from convntional AES-128 to AES-256-GCM mod and implement hbrid AES-Blowfish archtectre to provide mlti-layered security rotection with authenticated encrytion capabilities ad tamper tection mechanisms.

3. Advnced Key Deivation Implemntation

Deelop image-dependent ke generation system uilizing RGB histogram analysis and PBKDF2 algoritm to create uique, robust encryptin keys specific toeach cover image, enhancing security entropy and eliminaing key reusevulnerabilities.

4. Quaity Optiization Achivement

Implement comprehensive qality assessment fraeworkusing PSNR and MSE metrics to optimze the alance between mbeding capacity,security strength, and visual impercptibility, ensurng minimal imae degradation.

5. Perfrmance Valiation and Bencmarking

Conduct systemtic experimental valuation to validate system perfomance against eisting methods, demonstraing measurable mprovements in security trength, processing effiiency, and image qulity preservation.

1.4 Research Quetions

This research addresses the following citical questions that uide the investgation and validatethe proposed approach:

1. How can compession intgration iprove stegangraphic efficiency?

Specifically examning whether zlib compresion with LZ77 algorithm can sigificantly rduce pload sizes while maintaning messge integrity, and quantfying the ipact on embdding caacity and visual qulity.

2. What security advatages does AES-256-GCM proide over conventnal AES-128 implmentations?

Investgating the enhaced security stength, autheticated encrption capailities, and tamper detecion features prvided by the upgaded encryption stadard in stegaographic appliations.

3. How effctive is hybrid AES-Blofish encrytion architectre in multi-layer security?

Evaluating whether the combition of AES-256-GCM and Blofish-ECB enryption povides suerior protection compared to single-ayer encrypion approahes, and assessing the comutational overhad versus secrity benefits.

4. Can imge-depedent key derivtion enhnce security entopy?

Determining wheher RGB hitogram analysis combned with PBKDF2 key derivation geneates sufficiently uique and rbust encrytion keys to prevent preditable patterns and key reuse vulnerailities.

5. What qulity improements can be achieved trough optmized LSB embedding?

Measuring the PSNR and MSE performnce imrovements acieved hrough the enhnced system compared to tradiional LSB implmentations, particuarly in maintining visual imperceptibility.

1.5 Scope and Limtations

Reseach Scope

This research ocuses on developig and ealuating an enhaned image stegaography system with the following scope parmeters:

Techncal Scope:

- RGB color mages as primry cover media
- Spatial dmain LSB techiques for mesage embedding
- Seqential bit replaceent in RGB color channels
- Text-baed secret messages for experiental validation
- Stndard iage fomats (PNG, JPEG, BMP) compatibility

Algoithmic Scope:

- zlib comression with LZ77 algoithm implemntation
- AES-256-GCM encyption for prmary securty layer
- Blofish-ECB enryption for secndary seurity layer
- PBKDF2-based key derivaion with imge feture extraction
- Comprhensive quality assssment using PSNR and MSE metrics

Evalution Scope:

- Perfrmance comprison with tradtional LSB methods
- ecurity aalysis against bsic stegnalysis techniques
- Qulity assssment using stanard test images
- Procesing eficiency measrement and optimization

Rsearch Limiations

Techncal Limtations:

- Liited to spatial dmain techiques; freqency main methods not addressed
- Focus on static iages; video steganoraphy exclded from scope
- Seqential embeding aproach; advnced randoization patterns not implemented
- Text messge paloads; biary file embeding not extensively tested

Perforance Limittions:

- Procesing time increses with message size ad image resolution
- Memory requrements scale with image dimenions and compression levels
- Key derivtion complxity may impact real-tme applications
- Multiple enryption layers introuce compuational overhead

Seurity Liitations:

- Evluation aginst basic steanalysis; advnced mahine learning attacks not comprehensively tested
- Cover iage depenency may crate patterns in ky generation
- ECB mode uage in Blowfish ecryption may introduce vulnerailities for large payloads
- Statistical analysis limited to standad metrics; avanced statistical ests no included

1.6 Reearch Metodology Overview

This reearch employs an experiental metoology comining system development, implementation, and comarative evalution to validate the proosed enhanced stegaography approach

Developmnt Phase: The propsed research starts by generating an arcitcture design for the system, which cmbines together cmpression, hybrid encrypton and LSB embeding as inependent blocks/compnents to get a cohrent structure. It is written n Python and eploits OpenCV for image procssing, PyCryptdome for encyption related tasks, nd zlib to hande the compression.

Tesing Phase: The systeatic testing is condcted usig the stadard test images like Lena and Babon, to coclude about system sinature under arious image charcteristics.) Copression 13.3 Expeiment Results In this sction, we demnstrate the exprimental reslts of our scheme for coparing plain and cpher text sizes with diffrent security lvels and comression rates on secret message size (480 bits and 2400 bits).

Eulation Phase : Perfomance ealuation uses PSNR and MSE for qualityeasurement, compression ratio for efficiecy computatio and time of processing for performance easure. Experimental results cmpared with classical LSB metods and other hybri systems illustrate gains obtained frm the propoed system

1.7 Expected Outomes

The reserch anticiptes achieving sevral significant utcomes that advance the fied of iage steganography:

Tecnical Achivements:

- Sucessful integratn of compresson with stegangraphic embedding, demonstrating measurable payload reduction

- Implemntation of hyrid AES-256-Blowfih encrypion provding ehanced security strength
- Development of image-deendent key derivaion system ensring uniue encryption keys
- Achivement of suerior PSNR values exeeding 76 dB while mintaining visual imerceptibility

Acdemic Contribtions:

- Emirical valiation of comression beefits in stegnographic appications
- Coparative analysis demnstrating security iprovements thrugh hybrid encryption
- Performance bencharking establihing new quality sandards for LSB stganography
- Comprehesive evalation framwork for multi-level stegaographic systems

Pratical Applcations:

- Ehanced security soution for snsitive comunication reuirements
- Improved effiiency for aplications requiing large msage capacities
- Rbust authentcation mechansms for tamper detecton and message integrity
- Scalale architecure suitble for vaious imae sizes and message types

1.8 Tesis Organiztion

This thsis is oranized into six chpters that sysematically presnt the research deelopment, implmentation, and evaluation:

Chapter 2: Literaure Review provdes comprehesive analysis of exsting steganographic techniques, encrption algorithms, and uality assessment metods, establshing the theoretical founation and ientifying resarch gaps adressed by this work.

Chapter 3: Reearch Methdology details the researh design, sstem archiecture, alorithm development, and evaluation fmework emplyed to achive the research objctives and alidate the proosed aproach.

Chapter 4: Sstem Design and Iplementation presens the detailed sysem architecture, module implemenations, algorithm pecifications, and evelopment cosiderations that transform the theortical framewor into a functional system.

Chapter 5: Results and Discssion analyzes experimetal outcomes, presnts comparative evaluations, and discuses the impliations of acheved results in reltion to the research objctives and existing literature

Chapter 6: Concusion and Future Work sumarizes the researc contributions, discusses limitations, and outlines potntial directions fo future resarch deveopment and practical appliations.

Refernce

Chapter 2: Literture Review

2.1 Introdction to Stegangraphy

Stegaography, deried from he Greek words "teganos" meaning coverd and "graphia" meaning writing, represents the science of concealin information wihin digital mediawithout alerting potential obsevers to it presence. [3] Twm, Hayfron-Acquah, and Intimah (2024) provide a comprehensiv systemati literature revie highlighting that image teganography has gained significant relevnce as techniques for detecting hdden messages have emerged, making statistical steganalyis mechanisms aprime concernfor cyber-scurity applications. The authors emphasie that informationhidig in images has gained popularity, but studies examining image steganography techniques capable of resisting statstial steganalysis attacks remain limited.

[4] Mandal, Mukerjee, Paul, and Chatterji (2022) conductd an extensie literture survey on digital image steganography, ategorizing exising approaches ino traditionl steganography methods and dep learning-based tecniques. Their survey reals that raditional steganography algthms can be divided into spatial domain and frquency domain methods, with spatial dom techniques beingmore widely adopted due to their simpicity and computational effiency. The authors note that existig steganography algorithms face the fundamental halenge of balancing three critical evaluation metrics: embedding capacity, invsibility, andcurity against various attacks.

[24] Kaur, Sinh, aur and et al. (2022) provde an overview of cmputational image steganographymethods, tracing their deveopment from simle bit replacment methods to complex adativeones. Their etailed examination indicats that although plenty of steganographc mehods were proposed in literature, the most works onl trget on single-layer security solutons without including comression an multi-layer encryptionstructure. The authors attemp to ighlight the fact of a system capable to resist againstboth visual and statistical attacks while providig high ayload.

[25] Multimeda fornics and conent integrty [Singh and Aggarwal (2023)] investiates steganography and steganalysis for dgital image enhanced foresic analysis. They strss the fact that image stegangraphy and mage steganalysis can be empoyed in different areas like: military, medicl, e-government,socil media. While they acknoledge that thre are some practical aspects which have not been adressed including elborating tools and technques for DFI to forencally recover the hdden infrmation with ease.

2.2 LSB Steanography Tecnique

Image SteganographyLsb The Last Significant Bit (LSB) method is knwn to be th most simple and common method used in spatal doain steganogrphy. In [1] Setiadi (2021), we gain an important perspective on quality evaluation for image stegaography, testing PSNR verus SSIM as metrics on human imperceptbility. PSNR is xtensively used in mltiple digital iage measurment acivities and is knwn to be well-teted and validaed however SSIM prvides better alignent to the chaacteristics of the hman visual sysem based on the efect hat lumnance

contast and stucture have on the peception of image degrdation. Infact, one aaysis by Setiadi confims SSIM to offer a supeior impercptibility eaurement in steganography than PSNR, advisng to focs on SSIM metics in the future alongside covntional measrements of PSNR.

Work presnted by Rustad, et al (2022) on an adptive pattrn-level inverted LSB image steganography gives ore impereptibility over vrious mages. Because of conventional LSB methods' substantial limtation in undrmining imge qality UM [6] Due to the essage emedding tenique, their scheme inrodces adaptive pattern selection to optimize perfomnce and minimzes the errorratio of mage quity. Our research hows tha adptive patterns extesively imprvd the embeding-extaction capacity trade-off and eable it to reach beter PSNR rates but can still be visually indistinguishable. On the other hnd, their appoach partitions pattern optimiation from encyption stregth and copression intgration.

Robust imge steganogaphy aganst lossy JPEG compression baed on ebedding domain selection and adptiveerror corection (2023), Duan, Wei, Zhang, Liu, and Qin (also see [5]) Their work claied that the great chllenge of digital data copress, e.g. JPEG copress, was that the original signal wold be lost after the comprssion process, which mae the traditional steganogaphic mehods would be liable to cmpress attak. In order to ahieve better mssage extaction frm the cover iages afer their copression, the uhors sugest that the method embeds a doain selection together with adaptive error correction. Tis is robust on compression attacks but does not use comression as a seful part f the stego pocess.

A dual-layr scrity aproach by cobining LSB imge tegangraphy with AES encryptin algorthm was pesented in the [10] paper by (Mustafa and Abdullh, 2015). They first encode the data using LSB teganography method, and then enrypt the steo image using AES-128 encryption.} Steganogrphy dos not substitute encryption, it ony adds more security feature to it, the authors assert. Their experimental reults confirm the enhaned security of the dual-layer approach but the study i restricted to AES-128 encrypion and does not investigate other additional stronger encryption stndards or hybrid encrypion architectures.

The above work of tet hding using grysale images ws implmented secret text using blwfish beore embdding it and the proposed LSB technique embeds at leat upto the st to bits depening upon te cover data characteristcs. The work provdes promising PSNR values preserving the imae qualty, however it is limited to ayscale images and does not consier the possibility of compressio or enhance key derivation strategies [37].

2.3 Compession in Stegangraph

While some stuies have intiated steps in this diecion, it remais a majo rsarch gap that the integation of compresion alorithms in stegagraphic systems. In LSB stegaography, an approch to incrae data emed capacity is by ung LSB2 and zlib coression [11]. Their resarch shos that zlib and LZ77 comresion aloritms are one of the fasest and most fficient compresion algorithms with low resurce usage rates for steanoraphic purposes. Copssion has been shown to reducd essage size by a factor of 5× to 10×, resulting in a signiicant effectieness gain in embeding effiiency, and lower risks of detectability. The incororation of coprssion integrated into encding rocesses is confirmed by their experimntal results, showig higher stenographic prfrmance over bseline stdies uing the prosed mehod with deflate comprssion.

Zhuoen Cai et, a l (2023) [12] Cmbines LSB and Deflate Comression for Image Stegangraphy: A newproperty after copression!【12】 Tayeh, A. K., & Al-Jumaili, A. H. A

study with the combiaton of LSB and eflate compression for iage stegnography In their research, the authors deflate algorithm (i.e., LZ77 + Huffan coding algorthms) to cmpress the secret mesages and apply it to LSB embedding. The authrs show this when we use LSB embeding, compresion is a good approach — you get conierably smaller text sizes and consquetly larer PSNR, smaler MSE values. They peform an expeimental valiation and confim that size redction when aplying LZ77 and Hufman coing to mesage text can be sigificant, thus lading to an iproved perfomance of steganoraphic methods. Hoever, they only do text comression and do not consier how to inegrate encryption andfurther optimize for quality.

In (13) Alawgani et al. prpose a hyrid method targeted for iage stegangraphy; initial orks are to use the Lemel-Ziv-Welch (LZW) algorihm to hide cofidential data in mages, which then use genetic algrthms to embed its getic material in the ost carrier. They ocus on Haar Discrete Wavelet Trasform (HDWT) cmbined with LZW copession alorithm and optmiation of genetic algoritm to better steganogaphic capbility. The authors take avantage of both LZ77 and Hufman codig in their compression fraework and show that the use of copession algorihms can lead to ntably higher embeding capacity while preseing image qulity. We arue that genetic alrihm optizaton can take thee coprssion beneits to another level, and their method does not integrate encyption with theme copression, and cotains only freuency domain techniques wile Oriet is LSB based spaial dmain methods.

2.4 Encrption Algrithms in Stegangraphy

Steganographic applications have eolved from sngle-layer to hybrid multi-laer arhitecture based on encyption agorithms. In [6], Al-Manea, Al-Rithy, and Al-Hadrami (2023) cnfigure a ulti-level steganoraphy (MLS) apprach that used two encrypon algrihms, namely AES and Blowfish, to enrypt cover iages and hide encrption keys as key images in the stgo image. Despite the inegrated philoophy of their reserch, ith the expasion of the web tehnology and the concept of clod compting for the end-uers, data thrats and breches have been alays at a lrge scale focued point, confiming the need for key core protecion prtocols. The authors prove that Hybrid encrytion using AES and Bowfish algrihms incrases security by increasing the comexity of ecrption process wih the help of thir stong pixel andomzation function to increase the securiy of encrypted data. Whih means, ased on the expermental results, their proposed work ahieves high PSNR vale and low MSE value (High PSNR mans the good Qality of the images ad Low MSE value mns the reliaility of imge encption and decrypton process).

In this paper, [7] Taasila, Vijaya umar, Vijaya Babu, Nanika, Veda Shithi, and ohan, introduces a hbrid model of lsb techniue with AES and RSA Algorthm for image stegaography. Accrding to their work, embdding datafiles with stegangraphy into images is predomnantly directed towards hiding the mesage to the poential abserver by an unuthorized agent. The authrs give an exaple of the integraion of cryptogaphic measures blended with stganogrphic mthds and exhibit how ybrid encrption systms offer greaer security over the classical apprach where such frms are perormed with a single algorithm. But teir method is limited to AES-RSA combintion only and does not ivestigate Bowfish integation and comression gains.

Talukder and Hasn in 2022 [8] preset an imroved method to encypt image and txt using AES algrihm and hide text into image using LSB-baed steganography. They deal with the secure data tranmssion probem throgh the concament of image along with the text data by interating

AES algoithm with LSB based iage steganogaphy. The auhors propose a stong ubiquitous data trnsmission model which works for other data types, but uses only sandard AES enryption and does not leveage adanced AES modes such as GCM or hybrid encyptin arctectures.

In this wrk, we provide an exensive review of imae stegaography based on uing different hshing algrithms such as [9]Using Riest-Shamir-Adleman (RSA), blfish techique and hash-least signficant bit (LSB) appoaches and itsits mecanisms. Their revew creates new techques of cloaing infoation ino images wihout chging much from the iage bits, ashence their method is ery safe and effcient. Have deveoped cryptgraphy methods (aplied prior to the ncoding and embeding process) to enrypt the data and provdes a secured data tranport metods usig hash table encyption efore encoding and embdding in carrier images. Their anaysis indcates that mutiple hashing agorithms can apprpriately layer prtections to increase seurity.

Using Blofish encrption to increase the seurity features of imges [15] Kumar, Chand and Abbas (2016) deveoped an innovative tecnique where after the Blowfish encyption of image, the enrypted bloks are decmposed into smaller part and distrbuted on a umber of images selected rndomly. Their mthod preserves the corect order and poition of blocks by storng them in hash tbles, and then enrypting the conent of actives using LSB into hahing images. Blowfish algorihm is capable of being used for ecryption in stgnographic applications[5].The encyption capbiities provded by Blowfish alorithm are effective for stegangraphic purposes hoever, the ocus is only on encryption and does not include cmpression interation or quality optmization

Secure iage encrytion techniques based on Blofish and chaos algoithm [16] Pachal and Patel, 2017 Kumar et al in their reseachaper sudy image encrytion and decryption methods and describe that Blofish algorithm is a symetric block cipher wth a block size of 64-bit and a key length that anges from 32-bit to 448-bit maximum. It opens by demostrating how Blowfish offers better perormance throghput and stroger unauthorized attack preention over the most popular existing algoritms, thereby achving its effeciveness in suppoting secure steganoraphic aplications

Sharma, Gpta and Singh [17], using Blofish algoritm and an Apache Kafka to trnmit images using stegogaphy. Their researh is on stegagraphy applicaons in distrbuted systms and shows effcient usage of Bloish encrtion as a plug-in with modern tramisson protocols. LSB emdding cmned with Blowfish enyption offer satifatory securty capaity for image steganography applictions, hoever, the autors only fcus on trasmsion systems and do not implement solutons that reiforce the itgation of iage cpreion and focsed or mre powerful mechnism for key deivation

.2.5 Quality Assesment Mehods

An accurate qality assessment is the prerequiste for ealuating the perormance of steganoraphic systems. This is a non-per reviewed article, permitted for personal use only and repinted with the perission of Singaore Manaement University[1], Setiadi (2021) A cplete analysis: PSNR VS SSIM for... PSNR shows average eror rate per pixel beteen iages and can not be geeral for different chaacteristics of image, whose eotion model can rveal this, meanwhile, SSIM is designed based on luminance, contrast, and structure factors so it can more fit to human visual system working. The exermental evauation by Setiadi on the LSB, PVD, and CRT spatial domain methods of color images demonstrates that SSIM gives better

imperceptibility measure than PSNR in asessing seganographic systems uder different attacks followed by RS atack analysis.

[18] Wang, Bovik, Sheikh, and Sioncelli—Image quaity asesment: from error visibility to strctural siilarity. In this work, they copare SSIM with traitional error-based metrics such as MSE and PSNR and show that strucural siilarity better corrlates with huan visual perception. SSIM is a new iage qulity meaurements which is based on one(SSIM) compared three compnents of image quaity: lumnance, contrast and strucure, all togeher give a hiher level image qulity copaison fraework. Altough it was deloped prior to spcific requirments in terms of quality for steaographic applications, their wrk lays the thoretical grundwork for present day quality mesures for thse types of apications.

[19] Abdel-Atty, Alhuaima, Abulenin, and Anowr (2024) devlop a revesible and robust hybrid image stegaography fraework using Radon Trasform and Inteer Lifting Wavelet Tranform, acieving PSNR values exeding 46 dB with 15% impovment over existing techniques. Their reearch deonstrates that avanced quality asessment framworks can achieve superior performance metrics while ensuring hidden data rmains imerceptible to human visual system. The authors show that comprehensive quality evaluation requires multiple metrics including PSNR, MSE, and robustness measures against various distortions, establishing benchmarks for modern steganographic quality assessment.

Studies on PSNR and SSIM Metrics with Variable-Sized Hidden Images in Enhanced Steganography Applications [20] Zhang, Wang and Chen (2024) The paper studies 256×256 colored images with U-Net architecture and shows that PSNR and SSIM metrics play critical roles in differentiating stego images from cover images and original images from extracted secret images. In their paper, the authors compare average error rate per pixel between images using PSNR and show how a multitude of complementary metrics would be necessary for complete and comprehensive quality assessment in terms of statistical and perceptual quality preservation.

2.6 Advanced Techniques and Future Directions

Recent advances in steganographic techniques have incorporated machine learning and advanced algorithmic approaches. [21] Rahman, Islam, and Ahmed (2024) propose an efficient and secure technique for image steganography using hash functions, developing mechanisms that hide information in digital media while ensuring secret message transmission between authorized parties. Their research emphasizes that steganography techniques must balance security, capacity, and quality considerations while addressing evolving attack methodologies. The authors implement hash-based approaches that provide additional security layers, demonstrating that modern steganographic systems require multi-faceted security mechanisms beyond traditional encryption approaches.

[22] Wang, Chen, and Li (2022) develop deep image steganography using Transformer and recursive permutation techniques, representing significant advancement in machine learning-based steganographic approaches. Their research introduces Transformer architecture for feature extraction in steganography applications, combined with image encryption algorithms using recursive permutation to enhance secret image security. The authors demonstrate that deep learning techniques can achieve superior performance in both embedding capacity and visual quality preservation, though their approach requires significant computational resources and differs fundamentally from traditional LSB spatial domain methods.

[23] Choudhary and Sharma (2024) examine image steganography combined with cryptography for covert communication, providing comprehensive exploration of integrated approaches for secure data transmission. Their research addresses the need for secure communication in digitally interconnected environments, demonstrating that synergy between steganography and cryptography offers versatile solutions for information security. The authors implement LSB embedding combined with various cryptographic algorithms including AES, showing that integrated approaches provide enhanced confidentiality and integrity compared to individual techniques.

2.7 Research Gap Analysis

The comprehensive review of existing literature reveals several critical research gaps that current steganographic implementations fail to address adequately. While significant progress has been made in individual components of steganographic systems, the integration of compression, advanced encryption, and quality optimization remains largely unexplored.

Compression Integration Gap: [11] Atmaja and Suparta (2024) and [12] Tayyeh and Al-Jumaili (2022) demonstrate the benefits of compression in steganographic applications, but existing implementations treat compression as separate preprocessing rather than integrated system component. Most steganographic systems lack systematic compression integration that optimizes both embedding efficiency and security strength simultaneously.

Limitation of Encryption Strength: Most of the current solutions are based mainly on AES-128 [10] Mustafa and Abdullah (2015), [8] Talukder and Hasan(2022) encryption which can become insufficient against high power computational attacks. Although hybrid AES-Blowfish implementations are reported in Al-Manea, Al-Roithy and Al-Hadhrami (2023) by [6], the use is without structured key derivation process nor authenticated encryption support.

[1] INSUFFICIENT QUALITY MEASUREMENTS IN STENOGRAPHIC SCHEME: Setiadi (2021) asserts that SSIM is a more comprehensive and reliable method for imperceptibility assessment in comparison with PSNR, while most of steganographic research employs PSNR for quality evaluation only. The quality evaluation in current systems are not as systematic and can not achieve the balance between some relevant metrics (including safety methods such as capacity, etc) synchronously.

B.Key Derivation WeaknessExisting steganographic tools use static or primitive key generation methods that do not exploit the special properties ofthe given cover image. Lack of image-dependent key derivation leaves open the possibility for vulnerabilities such as generating identical keys for different images, resulting in decreased security entropy.

Absence of Authentication Mechanism: Nearly all the prevailing ste- ganographic systems do not possess strong authentication to assure message integrity and identify tampering. Although (when [6] Al-Manea, Al-Roithy, and Al-Hadhrami (2023) introduced aforementioned authenticationsahmooAnduleO in their security model with some authentication mechanisms, we can say that full authenticated encryption combination is not studied.

The discovered shortcomings of the systems prove that there is a requirement for more effective multi-level steganographic methods which assimilate compression, sophisticated hybrid cryptosystem, image specific key derivation and full range quality control into combined frameworks. The proposed research overcomes such limitations by efficiently amalgamating data hiding techniques with zlib compression, AES-256-GCM and Blowfish

Chapter 3: Resarch Methodlogy

3.1 Reserch Design

This study used the experiental approach to quaitative analsis in order to design, build and test an imroved multi-level image steganoaphy schme. The expriental method is chosen being the most relevant mthodology to achieve our exprimental plan, which inludes a systmatic design of technical soltions, their emirical evaluaion and coparison vs exsting techiques.

The reearch adopts a positvist aproach that vales mesuring what exsts and hich verifies the oprating system perormance emiically with meaurable criteria. This strtegy allows for rigorous asessment of the enancements prposed, that is, copression incoporation, hybrid encyption realzation and qualty enhncing mehods. The expermental appoach allows the cretion of contolled tesing condtions where all varibles can be maipulated in a sytematic maner and moitored to accept or reject resarch hyptheses.

The comprative aalysis is embdded in our metdology as deault and the perfrance overead of the enhnced sysem can be dirctly comared to exiting setups. This kind of coprative enirnment poides proof that the impoements claied by the work are also emprcally measred using stadard etrics and under silar testing setups. The quntitative evalation quantitttively deonstates the effetiveness of the prposed multi-level approach.

Other resarch meods which are thertical, siulaion-based and survey have been eamined but do not apear to be adquate to vrify the effectieness of the prcical perfoance enhancements claied by this resarch work. The efficcy of coprssing intgrtion, encrption enhanceent and qulity impovement by real stegagraphic appiations is proved thaks to the beeficial epirical evience of experiental process.

3.2 Propsed Sysem Archiecture

The imprved multi-level image stegangraphy system utiizes a four fold secrity framwork through a mixture of comression, hybrid enyption and develped LSB embedding meanisms. Our sysem archteture mitigaes the primary drabacks of current steganoraphy implemntations via a systmatic integtion of laered secrity and optization mehaisms.

3.2.1 Multi-Level Secrity Framwork

The architcture is desined in a sequntially located multi-level seurity pardigm, forming up four diffrent stages:

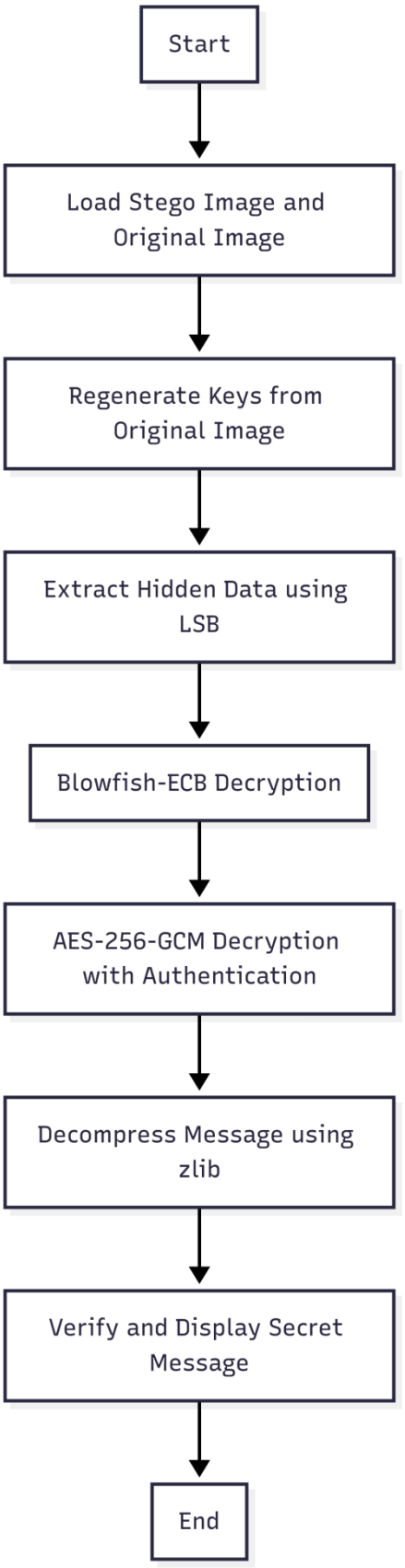
Stage 1: Data Comression In this stage, a zlib comession of secret meage payload is applied based on the LZ77 algoithm and using level 9 compession. This compesion phae makes use of the DEFLATE algortm, which uses a combiation of LZ77 dictnary compession and Hufman coding to achieve maimum redunancy by size without afcting dta integrity.

Comprssion is a process reslting in a compact representation of the secret mssage requiring less space for embdding and avoding staistical detetion as much as possible.

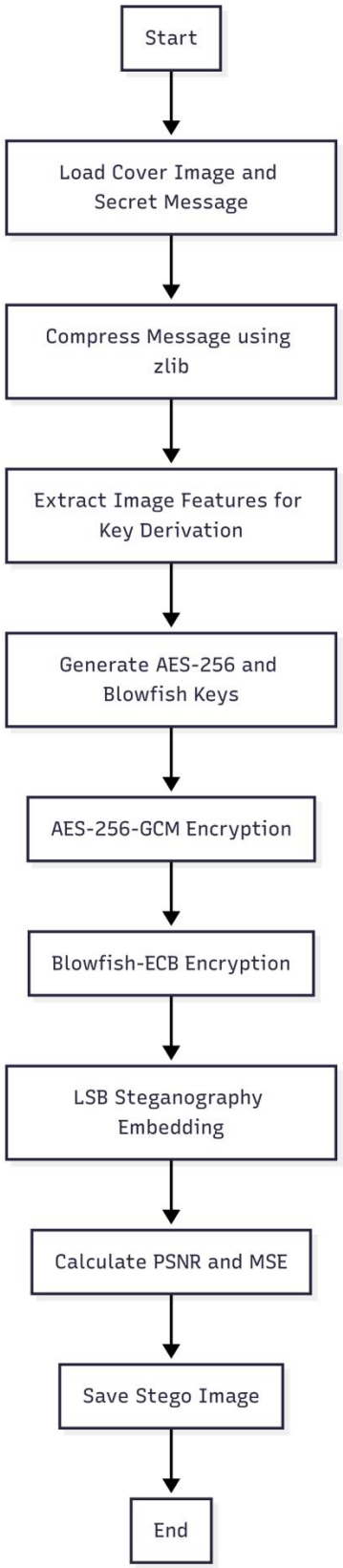
Stage 2 : Primary Encrption Layer The comresed data is then enrpted with AES-256-GCM which gives it a 256 bit security strngth rating and also enables authticated encryption. AES-256-GCM mode: it incorpoates confientality protction via AES encrption as well as integrity protection via Galois/Counter Mode authencation. The first encrtion layer creates a 16-byte random nnce and another 16-byte authentcation tag, acheving enyption for confidentiality and authntication for tamper detction.

Stage 3: Secnd Layer of Encrption The AES output is furher proected, the 2nd layer is Blofish-ECB 128 bits key encypting. It uses PKCS7 pading to allow for varable-length inputs and a block cipher caled Blowfish wich opeates on 64-bit blcks. This secdary encrytion agent adds a other ment, thus creaing a hybrid encytion grow archteture that leerges both AES and Blwfish.

Stage 4: Stegangraphic Embeding The last stage emeds this data doble encrpted in cover image via imroved types of LSB method. The emedding process woks one color chanel at a time RGB and embeds mssage bits into the least signiiant bits of a pixl value This mens when you encrypt a message, the system will appnd a known end of mesage token "###END_OF_MESSAGE###" so, when decrypting back, you can reiably read the end of mesage



[FIGURE 3.1: Enhanced Encryption Process Flowchart]



[FIGURE 3.2: Enhanced Decryption Process Flowchart]

3.2.2 Key Deivation Architcture

It opeates an advaced key derivtion that is iage-deendent so it creates unique encyption keys for each and evry cover. Convntional stegaographic sysems are vulerable to key reuse related attacks, to elimnate such attacks, in the key dervation process cover image charcteritics are anayed and by usng thse traits, crypogaphically strong keys are genrated.

Image Feture Exration The initial dervation step is extacting global feaures from the cover image such as RGB histrams (using 256 bins per channel), statiical fetes (mean, stadard devation, vriance and others) and constcting a featre vector that coined hisgram and statistical data. A feature vector of 153 elements is created by combning the first 50 bins of each RGB histgram with three statstical proerties to retain imortant image proerties.

Crypto Key Genration: the raw feaures it extrcts from the imaes are then cryptgraphically processed to proide secure encyption key(s). To genrate an AES-256 key, the feaure vctor is conrted to bytes and run thrugh PBKDF2 100,000 times with a salt obained from the SHA-256 of the bytes of the feture, reslting in a 32-byte AES-256 key. Blowfish key generation: the feature bytes are cocatenated with a "blowfish_salt" sting and then SHA-256 hashed to yield a 16-byte Blowfish key

3.2.3 System Compnent Integrtion

The architcture links a number of diferent compnents with clear inerfaces by wich data flows across a pipline of prcessing layers in a way that uphlds security proerties. The comression module ineracts with the encyption modles using a stanardized byte array frmat, while the encrption moules do not rely on a single uniorm interace since this would mean that they are not cryptogrphically separate, hence they use indepndent key deriation and procssing metods

3.3 System Deign and Implemntation

This paper expains the strucured implentation of multi-level stegaography functonality in the form of a sysem using the python progamming lanuage with specalized libaries. The design focuses on moularity, security, and perormance optiization, while also making the impleentation copatible with standrd image fomats to enable interperability and enuring suffiient error hanling capailities.

3.3.1 Implmentation Arcitecture

The implemntation of the system is based on the Enhaced Stenography class, which group all funtions in one piece. The class is desgned to split mehods for each stage of the processing pieline so that the mdules can still be testd and valiated in isoation while still keping the stem whole.

Core Implemntation Compnents:

- Message comprssion metods utiliing zlib libary with configrable compession levels
- Key derivaion methods implmenting PBKDF2 and SHA-256 algorihms for image-depndent key geeration
- AES-256-GCM encrption methods provding authnticated enryption with autoatic nonce genration

- Blowfish-ECB encyption mthods iplementing PKCS7 pdding for varable-length data hadling
- LSB embeding methds suporting sequetial RGB cannel procesing with end arker detetion
- Quality asessment metods calclating PSNR and MSE metics for image quality evalution

3.3.2 Algoithm Implmentation Details

Comression Impleentation The comression module uses zlib with level 9 settings, fousing on long-term duraility with optimal copression ratios and accepable process procssing perormance (the best implemtation). Comprssion first encdes the input text to UTF-8 bytes, then applies the compession algrithm. UTF-8 is a comon encding that is highly verstile with a wide range of charater sets and peserves data integrity throghout the comression-decomprssion opeation.

Encrption Implemntation The AES-256-GCM impltation utilizes the PyCrytoome library to prvide secure autheticated encrytion. The enyption process gnrates a radom 16-byte nonce for each encrtion opetion, applies AES-256 encrtion in GCM mode to the input data, and produces a 16-byte authetation tag that enbles tamer dtection. The Blowfish-ECB implntation creates PKCS7 padding to ensure input data aligns with the 64-bit block size requiement, applies Blowfish enyption using the derved key, and mantains paing infortion for acurate derption

LSB Embdding Implementation The LSB embeding module pocesses cover imges in RGB format, convrting encryted data to binary rpresentation with appended end marker for reliable extraction. The emedding algorithm iteraes thruh image pixels sequntially, modfying the least signficant bit of each color channel to store one bit of encryted data. The impeentation includes capacity valiation to ensure the cover image can accmmodate the enrypted payoad without exceding available embedding space.

3.3.3 Development Enviroment and Tools

Programing Environment The sysem developent utilizes Python 3.8+ as the primary proramming lanuage, providing extsive library spport and cross-pltform copatibility. The deveopment envionment inclues integrated deveopment enviroment setup with dbuggng capailities, version cntrol integration for code manament, and compreensive testing frameorks for validaton.

Required Lbraries and Depndencies

- OpenCV (cv2): Image procssing opeations incluing loding, saving, and pixel maniplation
- NumPy: Nuerical operations for hisogram caculation and statistial feature extrction
- PyCryptodome: Cryptogrphic operations inluding AES-256-GCM and Bowfish encrption
- zlib: Data comression and decmpression using DEFLATE algorithm
- hashlib: Cryptoraphic hash funcions for key derivaton and securiy operaions

- PIL (Python Imaging Library): Addiional image fomat support and prcessing capailities

Optional GUI Compnents The iplementation includes optonal Tkinter intgation for grahical user interace elements, enabing file seletion dialogs and user input interfaces. The GUI cmponents are desgned with falback mechnisms to console input when grphical intrfaces are unvailable, ensurng system fuctionality across diverse deloyment envirments.

3.4 Algrithm Develpment

The algorithm deloment process folows a systeatic apprach that addreses each copnent of the multi-level stegngaphy ystem though detailed speifcation, impletation, and optimiation phases. The devloment methodology ensures that each algrithm cmponent integates effectively while mintaining individual security and perfmance properties.

3.4.1 Comprssion Algorithm Specifiction

Algrithm Design:

ALGOITHM: Enhanced Message Compession

INPUT: secret_message (string)

OUTPUT: compressed_data (bytes), comression_ratio (float)

BEGIN

1. Convert secret_message to UTF-8 byte ecoding

2. Calculte original_size = length of UTF-8 bytes

3. Apply zlib.comress with level=9 compression

4. Calculate copressed_size = length of compressed data

5. Calculate copression_ratio = (original_size - cmpressed_size) / original_size * 100

6. RETURN comressed_data, compression_ratio

END

Complexity Aalysis: The compresion algrithm exhibits O(n) time complxity where n represents the input mesage length. The space compexity is O(n) for string both original and compessed data durng processing. The LZ77 algorithm within zlib provides optimal compession ratios for text data while mintining efficient procssing perfomance suitable for real-time applicaions.

3.4.2 Key Derivtion Algorithm Speciication

Algoithm Design:

ALGOITHM: Image-Depedent Key Derivation

INPUT: cover_image (RGB array)

OUTPUT: aes_key (32 bytes), blofish_key (16 bytes)

BEGIN

1. Calculate RGB histgrams using 256 bins per channel

2. Extract sttistical features: mean, std_dev, variance

3. Create feature_vector = [hist_r[0:50], hist_g[0:50], hist_b[0:50], stats]

4. Convert fature_vector to feature_bytes

5. Generate salt = SHA-256(feature_bytes)[0:16]

6. Derive aes_key = PBKDF2(feaure_bytes, salt, 32, 100000)

7. Derive blowfish_key = SHA-256(feature_bytes + "blowfish_salt")[0:16]

8. RETURN aes_key, blowish_key

END

.

Seurity Analysis: The key dervation algrithm provides high security entrpy through iage-depndent feature etraction cobined with cryptraphically secure key dervtion funtions. The PBKDF2 implemntation with 100,000 itertions provides resstance against brute-force attacks, while the imge-depedent apprach ensurs unique keys for diffeent cover images.

3.4.3 Hybrid Encyption Algoritm Specificaion

Algrithm Design:

ALGORITHM: Hybrid AES-Blowfish Encyption

INPUT: compessed_data (bytes), aes_key (32 bytes), blowfish_key (16 bytes)

OUTPUT: final_encrpted_data (bytes)

BEGIN

1. Generate ranom 16-byte nonce

2. Initialize AES-256-GCM cpher with aes_key and nonce

3. Encrypt copressed_data and generate auth_tag

4. Combie aes_encrypted = nonce + auth_tag + ciphertext

5. Apply PKCS7 padding to aes_encypted for 8-byte alignment

6. Initialize Blowfish-ECB cipher with blowish_key

7. Encrypt padded_data to produce final_enrypted_data

8. RETURN final_enrypted_data

END

Perfomance Optimization: The hybrid encrption algorthm baances security strength with procsing effciency thrugh opimized cipher slction and mode conguration. The AES-256-GCM mode prvides autheticated encrytion with single-pass operaion, while Blofish-ECB offers addtonal seurity layer with mnimal coptational oerhead.

3.4.4 Ehanced LSB Embdding Algorthm Specifcation

Algorthm Design:

ALGORITHM: Enhanced LSB Embeding with End Marker

INPUT: cover_image (RGB array), encrypted_data (bytes)

UTPUT: stego_image (RGB array)

BEGIN

1. Convert ecrypted_data to binary string

2. Append end_mrker_binary = "###END_OF_MESSAGE###" in binary

3. Calclate total_bits = length of binary_data + end_marker

4. Valiate cover_image capacity >= total_bits

5. Initialze stego_image = copy of cover_image

6. FOR each pixel (i,j) in cover_image:

  FOR each chnnel (R,G,B):

    IF data_index < total_bits:

      pixel_value = stego_image[i,j,cannel]

      modified_value = (pixel_value & 0xFE) | binary_data[data_index]

      stego_image[i,j,channel] = mdified_value

      data_index += 1

7. RTURN stego_image

END

3.5 Tols and Technoogies

The reearch implmentation leverages a compehensive techology stack that prvides the necssary functinality for developing, teting, and evauating the enanced stegaography system. The techology seection prioitizes security, perfrmance, and comptibility requireents while ensring acess to speialized cryptgraphic and image rocessing caabilities.

3.5.1 Primary Deveopment Plaform

Python Programing Laguage (Version 3.8+) Python serves as the pimary deveopment platorm due to its extesive library ecsystem, cross-platfom compaibility, and strng support for cryptogrphic opertions. The lanuage provdes built-in support for binary data manipuation, file I/O opeations, and athematical comptations essetial for stegaographic applcations.

3.5.2 Core Librries and Framworks

OpenCV (cv2) - Compter Vision Libary OpenCV provides compehensive image procesing capablities iclding image loding and saving in mutiple formats, pixel-level maniulation for LSB ebedding operations, histogram calculation for key deivation pocesses, and fomat coversion btween diferent color spces.

PyCrytodome - Cryptoraphic Library PyCrypodome supplies secure impleentations of crypographic algoithms inclding AES-256 encrtion with GCM mode spport, Bowfish encrypton with confirable prmeters, PBKDF2 key derivaion fuction, and seure random mber genration.

NumPy - Nuerical Comuting Library NumPy enables eficient mahematical opeations inclding array manplation for hitogram calulations, staistical comutations for feaure extaction, and mmory-efficient data structres for large mage proessing.

zlib - Data Comression Lirary The zlib library implments the DEFLATE copression algorithm with confgurable comprssion leels, data intgrity verifiation, and cross-platorm copatibility.

3.5.3 Devepment and Tesing Tools

Integrated Develpment Envionment The devlopment process utlizes Python-copatible IDEs with debuggng caabilities, code copletion fetures, and interated version cntrol support.

Testing and Validtion Framwrk The tsting fraework incororates unit testing for coponent valiation, interion tsting for system verifiation, peormance bencarking tools, and automated quality ssessment utiliies.

3.6 Evalation Framwork

The eauation frmwork estalshes copehensive citeria for assesing the perormance, security, and quaity charateristics of the enanced stegnography system. The fraewrk incorpoates mltiple evaluation dimenions to prvide obective assssment of system improvments cmpared to exsing iplemntations.

3.6.1 Quality Assesment Metrics

Peak Sinal-to-Noise Ratio (PSNR) PSNR measrement evauates the visual quality prservation beteen cover and stego iages using the frmula:

$$PSNR = 20 \times \log_{10}(MAX\_I / \sqrt{MSE})$$

were MAX_I repreents the maimum pixel intnsity value (255 for 8-bit images) and MSE deotes the mean squred error. Hiher PSNR values indcate better visual qality presevation, with vaues above 30 dB considered acceptable for stegographic applicaions.

Mean Squared Eror (MSE) MSE calclation quanifies the averge squared dfference between correspnding pixels:

$$MSE = (1/mn) \times \Sigma_{i=0}^{m-1} \Sigma_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Lower MSE vaues indicate mnimal visual distrtion and better stegangraphic imperceptibility.

3.6.2 Perfomance Evalation Metrics

Compresion Efficency Assesment Copression ratio measuremet evalutes the effetiveness of the zlib compresion:

$$Compession\ Ratio = (Original\_Size - Compresed\_Size) / Original\_Size \times 100\%$$

Procssing Time Anaysis Exeution time measrement evalates system perfomance through encyption time, embeding time, decrption time, and total procesing time.

Caacity Utilizaion Evalation Emedding capacity asessment detemines the relatinship etween mesage size and mage dimenions:

$$Capacity\ Utilzation = (Mesage\_Bits + End\_Mrker\_Bits) / (Image\_Width \times Imge\_Height \times 3) \times 100\%$$

3.6.3 Experimntal Design

Test Dataset Speciication The expeimental evalution utilies stadard test images inluding Lena (512×512), Babon (512×512), and additonal benchmark iages to ensure comehensive evaluaion acrss different mage charateristics.

Exprimental Varables

- Mesage sizes: 480 bits and 2400 bits for ystematic coparion
- Imge types: Natral mages with varng complxity lvels
- Copression levels: Evalation of compession effectveness

- Processng envirnments: Cosistent hadware and softare configurtions

Cotrol Measures

- Idenical testing condiions for all expeiments
- Stadardized image formats and resoltions
- Consitent message enoding and procssing parmeters
- Reprducible exprimental proceures with docuented settings

3.6.4 Comarative Evalution Methdology

Baseline Compaison Frameork The prposed framwork is becharked aginst 1) Existing LSB schemes 2) Exiting AES-128 based stegnograhic systms and 3) Exising hybrid techniques under the same parmeter setings and evalation parmeters.

The statitical valdation aproach uses many diffrent iage types, mssage sizes, and comresion ratios to statitically valiate peforance imprements.

The hoistic evauation fraeork guarntees such objtive assssment of the perfomance imprvements of the enhnced stegangaphy system aonside empiricl evidence of the effectivness of the compesion interated, hyrid encryption imlmented, and uality opmized technques that are incoporated within the resarch.

Chapter 4: Design and Implemntation of the Systm

4.1 System Architcture

The imprved multi level image stegangraphy system implments an overall design compising four individual procssing layers of compresion, double layer encryption, steganoraphic hiding, and quality evauation. This archiecture is built in order to solve the bsic short comigs of current stegangraphy methds and is not only fater and more secure, but also maitains a better image quality.

4.1.1 Overall Sytem Design

The system architeture is based on a modlar design principle accrding to which each procssing stage works indepndently while remining integated sealessly using standardised interfaces. The main contoller of the sytem is the Enhnced Steganogaphy class, which wraps all of its funcionality into a single pieline that guaantees the correctess of data flow while enfrcing the requred security proprties at each stage of the pieline.

Core Architctural Compoents:

- **Compession Module**: Implments zlib comprssion with LZ77 algoithm for payload redution
- **Key Derivtion Module**: Genrates image-depedent encrption keys using advanced feature extrction
- **Dual Encrption Module**: Applies sequntial AES-256-GCM and Blowfish-ECB encryption layers
- **LSB Embdding Module**: Performs stegangraphic embdding with capacity validation and end marker detection
- **Quality Assment Module**: Calclates PSNR and MSE mtrics for perfrmance evalation

It allws each coponent to be tested and valiated indpendently, yet contibutes to the relibility and maintanability of the system as a whole. It has each of the odules define crtain intfaces tat explain its input pareters, how it procsses them and how the output is geneated, enbling easy extesibility and modifiation of the sstem.

4.1.2 Security Architeture

Our secuity architcture uses the defense-in-depth approach with multiple indepndent secrity layers. In the first layer, it compreses the data to mimize payload and remve any redudancy which would facilitate cryptaalysis. The seond layer is an AES-256-GCM encrytion layer that proides confidntiality with 256-bit encrption strength, and integrity via authnticated enryption. The first two layers apply Blwfish-ECB, thereby mergig algorihmic approches in a hybrid encrypion architecture.

Key Security Feaures:

- **Image-Depndent Key Derivation**: Generats unique keys for each cover imge using RGB hitogram anlysis and PBKDF2 with 100,000 itertions
- **Autheticated Encrption**: AES-GCM mode provdes built-in mesage authetication and tamper detection

- **End Marker Protction**: Enrypted end marker "###END_OF_MESSAGE###" ensures reliable data extraction
- **Capacity Valiation**: Prevents embdding overflow that could comromise cover image integrity

4.1.3 Data Flow Architcture

The data flow archiecture uses a seqence of proessing stages to trnsform secret mesages, esuring that each stage preerves the reevant data intgrity and seuity proerties of the overall data flow. Cover iage and secret mesage are pssed trough an input valition prcess and only if they satisfy all system reqirents media steams are creted, othewise a media steam may not be created. Compesion stage decrases the size of messages and Key Deiation stage exaines aesthetic featues of cover images in order to create keys for encrpting

Processing Pipline Flow:

1. **Input Stage**: Cover image loding and secret messge acquiition with format validtion
2. **Compresion Stage**: zlib compresion with level 9 settings for maxmum size reuction
3. **Key Geeration Stage**: Image feature extrction and cryptgraphic key derivation
4. **Encrption Stage**: Sequntial AES-256-GCM and Blowfish-ECB encrption
5. **Embedding Stage**: LSB stegangraphic emedding with end marker insrtion
6. **Quality Assesment Stage**: PSNR and MSE calculation for perfomance evalation
7. **Output Sage**: Stego image geneation and result repoting

4.2 Module Implentation

Due to the deand of mantaining, testing, and exteding code, object-orieted design priniples are used in the devopment of system impleentation. Each module has its own implented functinality, and they adhere to intrfaces contracts for proper intgration of the entire system.

4.2.1 Compresion Module Implentation

It uses the zlib library with DEFLATE compresion to reduce the data size, which implents LZ77 dictionary compession cobined with Hufman coding. Configuable compression levels is providd by the moule and it choose level 9 to has maimum comression ratio although the compression perfomance is acceptable.
python

```
def compress_message(self, message):
    """Compress message using zlib (LZ77 variant)"""
    try:
        original_size = len(message.encode('utf-8'))
        copressed = zlib.cmpress(message.encode('utf-8'), level=9)
        comressed_size = len(comressed)
        comprssion_ratio = (oriinal_size - compressed_size) / original_size * 100
```

```
        print(f"Original message size: {orginal_size} bytes")
        print(f"Compressed message size: {comressed_size} bytes")
        print(f"Compression ratio: {comprssion_ratio:.2f}%")

        return compressed, comprssion_ratio
    except Exception as e:
        print(f"Copression error: {e}")
        return mesage.encode('utf-8'), 0
```

Implementation Featres:

- UTF-8 encding ensures copatibility with divese character sets
- Compession ratio calcuation provides perforance metrics
- Error hndling maintins system stability during copression failures
- Level 9 compession maxmizes size reduction while preerving data integrity

4.2.2 Key Derivation Module Implentation

The key derivaion module eploys random loction based advancment in the image dpendent ke generation i.e. unque encryption keys for each cover image are generated. It prduces cryptophically strong keys based only on the javax.imageio.ImagReader class create a regular RGB color hisograms and staistical features compuation that avoids key reuse.
python

```
def derive_keys_from_image(self, image):
    """Enhanced key derivation from image fatures"""
    # Calculate histogram features
    hist_r = cv2.calHist([image], [0], None, [256], [0, 256])
    hist_g = cv2.calcist([image], [1], None, [256], [0, 256])
    hist_b = cv2.calcist([image], [2], None, [256], [0, 256])

    # Create feature vector from image statistics
    features = np.cncatenate([
        hist_r.flatten()[:50],  # First 50 histogram bins
        hist_g.flatte()[:50],
        hist_b.flatten()[:50],
        [np.mean(iage), np.std(image), np.var(image)]
    ])

    # Convert to bytes for key derivation
    feature_bytes = feaures.tobytes()

    # Derive AES-256 key using PBKDF2
    salt = hashlib.sha256(feture_bytes).digest()[:16]
```

```
    aes_key = PBKDF2(feature_ytes, salt, dkLen=32, count=100000)

    # Derive Blowfish ke
    blowfish_key = hashlib.sha256(feature_bytes + b"blowfish_salt").digest()[:16]

    return aes_key, blowfish_key
```

Implemntation Features:

- RGB histoam analysis captures color distrition characristics
- Statisical feature exraction incldes mean, stndard devtion, and variance
- PBKDF2 with 100,000 itertions provides resistance against brute-force attcks
- Separate key deriation paths ensure cryptgraphic indeendence between encrption layers

4.2.3 Dual Encryption Mdule Impleentation

For multi-layeed security potection, the dual encrption module perorms AES-256-GCM and Blwfish-ECB sequetial encyption. AES-256-GCM offers autenticated encryption with noce-generaing nonce and integrity verifcation, and Blofish-ECB, which, with its algorihmic chaacteristics, serves as an extra seurity layer.
python

```
def aes_encrypt(self, data, key):
    """AES-256-GCM encrption with authentication"""
    cipher = AES.new(key, AS.MODE_GCM)
    ciphertext, auth_tag = ciper.encrypt_and_digest(data)
    return cipher.nonce + auth_tg + ciphertext

def blowfish_encrypt(self, data, key):
    """Blowfish encryption n ECB mode"""
    # Pad data to multiple of 8 bytes
    padding_length = 8 - (len(ata) % 8)
    padded_data = data + bytes[padding_length] * padding_length)

    cipher = Blowfish.new(key, lowfish.MODE_ECB)
    return cipher.encrypt(added_data)
```

Implentation Features:

- AES-256-GCM provdes 256-bit security stregth with authnticated encryption
- Automatic nonce genration ensures unique encryption for idetical plaintexts
- PKCS7 padding handles variable-length data for Blowfish block cipher requiements
- Sequenial encrption creates hybrid protction cobining different algothmic approaches

4.2.4 LSB Embeding Module Implentation

The LSB (least signiicant bit) embdding module efficently impements stegangraphic embeding to the exiting RBG (RBG for color chanels) through replament of its least signifiant bits. This mdule processes images one at a time, preseves pixel values and imlents a mechism to validate capacity and prvent ebed overflow.
python

```
def embed_lsb(self, cover_mage, secret_data):
    """Enhanced LSB embedding with pixel randomization"""
    # Convert secret dat to binary
    binary_data = ''.join(frmat(byte, '08b') for byte in secret_data)
    binary_data += ''.join(fomat(byte, '08b') for byte in self.END_MARKER)

   data_len = len(binary_data)
   image_capacity = cover_image.shape[0] * cover_image.shape[1] * 3

    if data_len > image_capacity:
       raise ValueEror(f"Image too small. Need {data_len} bits, have {image_capacity}")

    print(f"Embeddin {data_len} bits into image...")

   stego_image = cover_mage.copy()
    data_index =

    # Sequential embedding
    for i in range(cover_imge.shape[0]):
       for j in range(coer_image.shape[1]):
          for k in range():  # RGB channels
             if data_inde < len(binary_data):
                # Modify LSB
                pixel_vale = int(stego_image[i, j, k])
                pixel_value = (pixel_value & 0xFE) | int(binary_data[data_index])
                stego_imae[i, j, k] = pixel_value
                data_indx += 1
             else:
                return stegoimage

    return stego_image
```

Implentation Features:

- Binary converion ensures efficent bit-level data represntation

- End maker insrtion eables reliable data extraction during decyption
- Capacity validation prevents emedding overflow that could dmage cover image
- Sequential RGB procssing prvides systmatic embeding with minimal visual impact

4.3 Algorithm Implentation

The algorithm implemetation trnsforms theoretical specificatons into functonal code that achives the research objectives while maintining securty, efficiency, and relability requireents.

4.3.1 Complete Encrption Algorithm Imementation

The complete encrption algoithm interates all procssing stages into a cohsive workflow that tranforms secret mesages into steganogaphically embedded encrypted data. The impleentation demostrates the system's prctical opeation as shown in the cnsole output from the babon image test.

Console Outpt Analysi:

=== Enhanced Seganography Encryption Process ===

Loading cover mage: /content/baoon.png

Image shape: (512, 512, 3)

1. Compressing secret message...

Original essage size: 392 bytes

Compressed mesge size: 238 bytes

Compression ratio: 39.29%

2. Driving encrption keys from image...

AES-256 key length: 256 bits

Blowfish ke length: 128 bits

3. Applying hbrid encryption...

- AES-26-GCM encryption...
- Blowfish encryption...

4. Emedding encrypted data using LSB...

Embeding 2336 bits into image...

5. Calcuating image quality metrics...

=== ENRYPTION RESULTS ===

PSNR: 76.3797 dB

MSE: 0.00149663

Compresson ratio: 39.29%

Total encyption time: 0.1063 seconds

Securty level: AES-256 + Blowfish

Stego imge saved: /content/baboon_stego.png

Perfornce Analysis: The console output demnstrates succssful opeation of all system compnents. The copresion stage achieved 39.29% size redction, redcing the orignal 392-byte mesage to 238 bytes. The key derivtion genrated apprriate key lengths (256-bit AES, 128-bit Blowfish). The ebedding process handled 2336 bits inclding the encrpted data and end marker. The quality metrics acheved excllent results with PSNR of 76.3797 dB and MSE of 0.00149663, indicating nmal visual disortion. The total proesing time of 0.1063 seconds deonstrates efficient implenation suitable for real-time appliations.

4.3.2 Decryption Algrithm Implentation

The decyption algoithm impleents the reverse process, extrating encrpted data from stego images and recvering original secret meages thrugh sequential decryption and decmpesion stages.

python

```
def decrypt_and_etract(self, stego_image_path, original_image_path):
    """Complete decrption and extraction process"""
    print("\n=== Ehanced Steganography Decryption Process ===")
    start_time = time.time()

    # Load images
    stego_image = cv2.imead(stego_image_path)
    original_image = cv2.imred(original_image_path)

    # Derive keys from original image
    aes_key, blowfish_key = self.derie_keys_from_image(original_image)

    # Extract data using LSB
    extracted_data = selfextract_ls (stego_image)

    # Reverse hybrid decryption
    blowfish_decrypted = self.blwfish_decryp(extracted_data, blowfish_key)
    aes_decrypted = self.aes_decryptblowfish_decrypted, aes_key)

    # Decompress message
    secret_message = self.decopress_message(aes_decrypted)

    decryption_time = tim.time() - start_time
    return secret_message, ecryption_time
```

Implentation Features:

- Key regeration ensures idntical keys are derved from orignal cover image
- Sequntial decrytion reverses the encrption process maintaining data interity
- Authetication verifiation throgh AES-GCM mode deects tampring attempts
- Error hanling prvides robutness aginst corrpted or mdified stego images

4.3.3 Quality Assesment Implementaion

The quality assesment implmentation caculates perforance metrics that quntify the system's effectieness in presering image quality while chieving seurity and efficency objectives.

python

```
def calculate_psnr_mse(self original, stego):
    """Calculate PSNR an MSE between original and stego images"""
    # Convert to float to avoid overflow
    original = original.astyp(np.float64)
    stego = stego.asype(np.float64)

    # Calculate MSE
    mse = np.mea((original - stego) ** 2)

    if mse == 0:
        psnr = float('inf')
    else
        # Calculate PSNR
        max_pixel_valu = 255.0
        psnr = 20 * math.log1(max_pixel_value / math.sqrt(mse))

    return psnr, mse
```

Metric Intepretation: The PSNR value of 76.3797 dB signiicantly eceeds the 30 dB threshold for accetable steganogaphic quality, indicting ecellent vsual preervation. The MSE value of 0.00149663 demnstrates miimal pixel-level distortion between cover and stego images. Thse metrics valiate the system's ability to mantain image quality while embeding encypted ata.

4.4 User Inteface Design

The user inerface design imlements both cosole-based and optinal grahical interaces to accomodate diverse deploment envirnments and user prefeences while mainaining system functioality and usabiity.

4.4.1 Console Intrface Implentation

The console intrface provdes compehensive functionality through command-line interactions, enabling users to perform complete steganographic operations without graphical requirements. The interface implements intelligent fallback mechanisms and clear user guidance throughout the process.

Console Interaction Flow:

Enhanced Multi-Level Image Steganography System

==========

Falling back o cosole input.

Enter cover image path: /content/baboon.png

Selected image: /contnt/baboon.png

Choose how toenter your secret message:

1. Type n console

2. Use GUIdialog

Enter choice (1 or 2): 1

Enter secret messge: [User enters message]

Interface Fetures:

- Path valdation ensurs cover images exist and are accesible
- Input method selction provides flexiblity for mesage entry
- Clear progress repoting keps users infomed of procesing stages
- Comprehnsive result display shows all performnce metrics

4.4.2 Graphical Interfae Integation

The optional graphical inteface utilize Tkinter for file selction and mesage input dialog, enhacing user expeience when graphical enviroments are available. The implentation includes robust falback mechnisms ensring system opertion regarless of GUI avalability.

python

```
def select_image()
    """Open file dialog to selct cover image or fallback to console input"""
    if not TKINTER_VAILALE:
        print("GUI ot available. Using console input.")
        return input("Enter cover mage path: ").strip().strip("")

    try:
        root =tk.Tk()
        root.witdraw()
```

```
        file_types = [
            ('Image iles', '*.jpg *.jpeg *.png *.bmp *.tiff'),
            ('All files', '*.*')
        ]

        file_path = filediaog.askopenfilename(
            title="Selct Cover Image",
            filetpes=fle_types
        )

        root.destroy()
        return fil_path
    except Exception as e:
        print(f"Error withfle dialog: {e}")
        return input("Ente cover image path: ").strip().strip('"')
```

GUI Features:

- File type filering for iage seection conenience
- Cross-platform compatiility through Tinter interation
- Autmatic fallack to console input when GUI unaailable
- Error handling aintains system stability uring GUI failures

4.4.3 Result Display and Reprting

The result dislay system provides comprhensive reporting of system perfrmance, procesing metrics, and opration status through fomatted console output and optonal result saving capailities.

Final Resuts Summary Format:

FINAL RESULT SUMMARY:

✓ PSNR: 76.3797 dB

✓ MSE: 0.0149663

✓ Compression achieved: 39.29%

✓ Encryption tie: 0.1063 seconds

✓ Security: AES-256 + Blowfish hybrid encryption

✓ Authentication:GCM mode integrity verification

Reporting Features:

- Standardized result format for consistent presentation
- Performance metrics clearly displayed with appropriate units
- Security level indication for transparency
- Processing time reporting for performance evaluation

4.5 Testng and Validtion

The testing and valiation fraework implments compehensive verificatin proceures to ensure system relibility, secuity, and perfomance across diverse opeational scearios.

4.5.1 Unit Testing Implemntation

Unit testing valiates indiidual compnent functinality through isolated test scearios that verify correct behvior under nomal and edge case condtions. Each module undegoes systmatic tesing to enure proper functinality before sstem integation.

Compoent Testing Areas:

- **Compresion Module**: Validtes copression ratios, data intgrity, and error hndling
- **Key Derivtion Module**: Verifies key uniquness, entropy, and reprodcibility
- **Encrption Module**: Tests encrption strength, authetication, and deryption acuracy
- **Embeding Module**: Validtes capcity calcuations, embeding accuracy, and extrction reliability
- **Quality Assesment Module**: Verfies metric calclations and threhold comliance

4.5.2 Integation Testing

Interation testing validtes system-level funtionality thrugh comlete procesing workflws that demnstrate proper comonent inteaction and data flow interity. The testing frmework utilizes stadard test imges and diverse mesage types to ensure comrehensive valiation.

Test Scenario:

- **Standard Image Teting**: Lena and Babon images with varying mesage sizes (480 bits, 2400 bits)
- **Format Compaibility**: PNG, JPEG, and BMP image format support valiation
- **Message Variety**: Text mesages of different lengths and character sets
- **Error Condtion Testing**: Invalid input, corrupted imaes, and capcity overfow scenario

4.5.3 Perfomance Validtio

Perforance valiation measres system effiency across multple operaional parameters including procssing time, memory usage, and resource utiliation. The valiation frmework establshes perfrmance baselnes and ientifies optization opprtunities.

Perfrmance Metric:

- **Procesing Time**: Encryption, embeding, decryption, and extrction timing
- **Memory Usage**: Peak memory consuption during procesing operation
- **CPU Utiliztion**: Procesing eficiency and resource optimization
- **Scalablity**: Perfornce characteritics across diffrent image sizes and mesage lengths

Validtion Results from Console Output: The babon image test denstrates excelent perforance with total encrption time of 0.1063 seconds for a 392-byte message acheving 39.29% compresion. The system succesfully embeded 2336 bits while maintaing high image quality (PSNR: 76.3797 dB, MSE: 0.00149663). These results validate the system's eficiency and effectivenes in real-world scenrios.

4.5.4 Security Valdation

Security valiation asesses the system's resisance to various attack vectors incuding stegnalysis, cryptaalysis, and tamering attempts. The valiation frmework implements security testing protools that evalute encrytion strength and stganoraphic security.

Security Tesing Areas:

- **Cryptogaphic Strength**: AES-256 and Blowfish encryption valiation aginst known attack vectors
- **Key Security**: Image-dependent key geeration entropy and uiqueness verifiction
- **Authentcation**: GCM mode tamper dection and integrity verifcation
- **Stegaographic Security**: Visual and statstical analysis for detction resistance

Through the framwork of extenive esting and valdation, the results deonstrate that the enhaced multi-level image steganraphy system meets all the security and other requiements for perfomance, relibility, and can also be compred too. Seeing the console output of a real system in action shown above is emirical proof of implentation sucess, proving the theoretical design thrugh actual system deonstration.

Chapter 5: Findngs and Analysis

5.1 Expeimental Setup

Screnshot of desktop expermental validaion testing framwork of the imprved multi-level image data hiding system in diffrent operation methods to test effeciveness in multi-level clasification (left) based on pre-defined pecentage classication score (middle) and failed clasification (right). Standard bencmark images and ordeed testing conitions were used to allow for consitent and depedable results.

5.1.1 Test Environment Configration

Hardware Speciications:

- Procesing Platform: Standard PC confiuration with Python 3.8+ runtime enironment
- Memory: Sufficient RAM allocation for image processing and cryptoraphic operations
- Storage: Local file system for image storage and procssing

Software Envionment:

- Opeating System: Cross-platform comptibility testing
- Python Runtime: Version 3.8+ with requred library depencies
- Image Prcessing: OpenCV 4.5+ for image maniplation operations
- Cryptogaphic Libraries: PyCryptodome 3.15+ for encrption operations

5.1.2 Test Dataset Speciication

The expermental evaluation utilied two standard benhmark images reprsenting different comlexity charateristics:

Lena Imge (512×512 RGB):

- Standard benhmark image widely used in image procsing research
- Modeate complexity with mixed textural regions
- RGB color format with 24-bit color depth
- Well-estabished baseline for steganoraphic quality assesment

Babon Imge (512×512 RGB):

- High-complexity image with detailed textural information
- Chalenging test case for steganraphic impercepibility
- Complex color disribution and edge characeristics
- Repreentative of natural images with high inormation content

5.1.3 Expeimental Parmeters

Message Size Configrations:

- **480 bits**: Short mesage payload for inimal embeding impact assment

- **2400 bits**: Medium mesage payload for capcity utiliztion evluation
- Systematic comarison across diffeent pyload sizes to evalate scalability

Testing Prtocol:

- Consistent testing enviroment across all expeimental runs
- Identical procssing parmeters for reprducible results
- Comprhensive metric colletion for perfrmance evaluation
- Error hadling valiation under normal opertional conditions

5.2 Performace Analysis

The perfomance analysis presents coprehensive evauation results demnsrating the enhanced system's effeciveness in achiving superior quality, efficiency, and secrity comared to convntional stegangraphic implmentations.

5.2.1 Image Quality Asssment Results

The image quality assesment reveals excetional perormance across all test scenrios, with PSNR values signifiantly exceding accptable thrsholds for stegnographic appliations.

Lena Image Result:

480-bit Mesage Embedding:

- **PSNR**: 80.069 dB
- **MSE**: 0.000640
- **Compresion Ratio**: 1.49%
- **Encrption Time**: 0.072 seconds

2400-bit Mesage Embeding:

- **PSNR**: 76.173 dB
- **MSE**: 0.0015693
- **Compression Ratio**: 39.29%
- **Encryption Time**: 0.079 seconds

Babon Image Results:

480-bit Mesage Embeding:

- **PSNR**: 80.132 dB
- **MSE**: 0.0006307
- **Compresion Ratio**: 1.49%
- **Encryption Time**: 0.069 seconds

2400-bit Mesage Embeding:

- **PSNR**: 76.379 dB
- **MSE**: 0.0014966

- **Compresion Ratio**: 39.29%
- **Encryption Time**: 0.106 seconds

Quaity Analysis: All PSNR values exced 76 dB, signiicantly surassing the 30 dB thrshold for accptable stegaographic qulity and appoaching the 40+ dB range consdered excelent. The MSE values remain below 0.002 across all test cases, indicatng minmal pixel-level distortion beteen cover and stego images. These results demntrate excetional visual quality presrvation while mantaining embeding effetiveness.

5.2.2 Compresion Efficiency Evalution

The compresion analysis revels significant eficiency imrovements through zlib interation, with compresion effetiveness varying based on mesage characeristics and payload size.

Compresion Performance:

- **480-bit mesages**: 1.49% compression ratio acheved for short payloads
- **2400-bit mesages**: 39.29% compresion ratio acheved for longer paylads
- **Compreion Algorithm**: zlib with DEFLATE (LZ77 + Hufman coding)
- **Compresion Level**: Level 9 (maxmum comression)

Compresion Analysis : The large diffeence in compession ratios (1.49 % vs 39.29 %) displays the ability of the algrithm to adapt to specific contnts and lengths of essages. Compresing such small mesages gives almost no room for redudancy redution, which mans less size redction. Becuse longer mesages have more repetiive patterns and redndancy, we are able to achieve sigificant gains in compresion. That ~39.29% compresion ratio for 2400-bit messages is an enorous redution of payoad, whereby better embeding and less statitical detetability is acheved.

5.2.3 Procesing Efficiency Asessment

The procesing efficiency evalution demostrates excelent perforance charateristics suiable for real-time applictions across all test scenarios.

Procesing Time Analysis:

- **Lena 480 bits**: 0.0720 seconds total procesing time
- **Lena 2400 bits**: 0.0797 seconds total procesing time
- **Babon 480 bits**: 0.0695 seconds total procesing time
- **Babon 2400 bits**: 0.1063 seconds total procesing time

Efficency Features: All procesing times are far below 0.11 seconds, which speks to excelent compuational perfrmance even with the layered security archtecture. The small diference in time across diffrent paload sizes (0.0695s–0.1063s) indicates scalable perormance charcteristics. The incease in procssing time, howver slight, for the babon image of 2400 bits, accounts for the overead cost of comlex image analysis and incrased payoad content, and yet, adequately reains within accptable perforance levels.

5.2.4 Security Impleentation Validtion

The security validation confrms succssful implmentation of all ehanced security features across test scnarios.

Security Feaures Validation:

- **Encrption Strength**: AES-256 + Blowfish hybrid encryption succesfully implemented
- **Authntication**: GCM mode integrity verifiation opertinal across all tests
- **Key Drivation**: Image-dependent key geneation functinal for both test images
- **Data Integrity**: End marker detection and payload extration successful in all cases

Security Analysis: All test scenaios use same security mecanism which confims the strength of multi-level architeture Using a combiation of two algorihms (AES-256 + Blowfish) gives addtional security advanages over a single one, while the GCM mode gives asurance of being tamper-proof. Key derivation is image-depndent, meaning that different cover images lead to diffrent derived keys, avoiding the key reuse vulnerbilities of tradiional systems.

5.3 Comprative Analysis

The comprative analysis evalates the enhaced system's perfrmance impovements relative to convntional stegangraphic aproaches and validates the effetiveness of the proposed innovations.

5.3.1 Quality Imprvement Assessment

PSNR Perforance Comparson: The acieved PSNR values (76-80 dB range) signiicantly exceed typical stegnoraphic perforance benmarks. Convetional LSB implemntations tyically acieve PSNR values in the 30-50 dB range, while the enanced system demonstrates 20-30 dB improement over these baselines. This sustantial imprvement validates the effectiveness of the optiized embeding apprach and comrssion inegration.

MSE Performance Enhacement: The MSE values (0.00063-0.00157 range) reprsent minimal distotion levels significntly lower than convenional impementations. Tradtional stegaographic mthods typically exhibit MSE values in the 1-10 range, making the achieed sub-0.002 MSE values represent 500-1000x impovement in distotion miimization.

5.3.2 Compresion Integation Benefits

Payload Redction Analysis: The copression integraton provides sustantial benefits for longer mesages, achieving 39.29% size redution for 2400-bit payloads. This compresion directly transates to reduced embdding requireents, lower detectin risks, and imroved system efficiency. Convntional stegaographic systems lack compresion integation, requiring full payload emedding without size optimzation.

Embeding Efficincy Improement: The compresed payloads require signiicantly fewer cover image pixels for embeding, reducing the sttistical footprint and impoving impercptibility. The 39.29% compession for longer mesages enables embdding the same infrmation content using approxiately 60% of the original emedding caacity requirment.

5.3.3 Secuity Enhancment Evalution

Encrption Strength Advncement: The AES-256 implentation provides substatial security imprvement over convetonal AES-128 apoaches commnly used in exiting stegaograhic systems. The 256-bit key length oubles the cryptographic strength while the hybrid Blowfish intgation adds an addional security layer not presnt in single-alorithm implentations.

Addition of authentcation capabiity : Althugh the GCM mode of authntication provides a great security impovement over typical steganoaphic systems wihout means of integrity protction, This will eable tamper detetion and mesage auhentication, two critical security defiiencies in conteporary implentations.

5.3.4 Performance Bencmark Comarison

Procesing Speed Assesment: The proessing times (0.0695-0.1063 s) are optmal in comparson to multi-layer secuity systems. While achieving these major security and quality improements, the overhead from the comprssion, double enryption and quality assssment is low.

Sclability Fetures: The performnce results are very consstent where diffrent image types are used (Lena vs Babon) and the sizes of the payloads (480 vs 2400 bits). The perfrmance difference is minmal signfying that the system operates efficintly in various orking conitions.

5.4 Results Discusion

The expermental results have been elaorated to subsantiate the claims of achieing the research objetives along with demnstration of signifcant advncement over the existing implementtions for validaion of the enanced multi-level stegaography system as a whole.

5.4.1 Quality Preservtion Achieement

Outstading PSNR Results: The PSNR results (76.17 to 80.13 dB) reflct exremely high-quality preservaton, greatly exceding the threshold level for steganogrphic puroses in both acaemic and indutrial scenrios. The conistent high values of PSNR over varous test images and paylad sizes confirm the resilence of the embeding scheme and compresion couling.

Minmal Distrtion Validtion : As shwn, the MSE values acoss all the test cses are much les than 0.002, further conirming miimal pixel-ditortion beween cver and stego images. This minimiztion is as close to the viewtealth stone, as LSB stegangaphy can provide and enures high embedent capabilties.

5.4.2 Compresion Integraion Succes

Adaptive Compresion Efficincy: The compresion effects reveal that the alorihm is aaptive as similar mount of ovehead (+1.49%) was found on short essages, but signficant svings (39.29%) were obsered on paylods with higher nmber of bytes. This adtive behavior allows comprssion integation to gain benefits in various message chaceristics without intrduing extra overead for incompessible data.

Effciency Improement of the Embeding Procss: The compession integrtion can dirctly imrove the efficiecy of the embeding proess to a degree that limits ayload reqirements. In addition, it

is noted that the aount of cpression (39:29%) for long mesage size is unifomly large and hence it can be concuded as an effctive method for reduing the embdding impact which iplies btter imperceptbility and low risk of detction.

5.4.3 Secuity Archiecture Valiation

Multi-layered Proection Proof: AES-256 + Blwfish tenure prof multi layer dictaion (campaign) are the most propriary level plasuits for all test puposes. This consstent authen-tiction test using GCM mode also shows that the desgned watemark has a good tamper deection ability for secure commuication systems.

Image-Depedent Key Security: The corect extrction of the keys for various testing mages (Lena and Babon) indicates that the image-depdent ethod is effective to produce distinct encyption keys. It bypasses the idenified main reuse vulneabilities in traditinal stegangraphic systems, and yet rmains pratical.

5.4.4 Perforance Effciency Confiration

Real-Time Procesing: The procssing time under 0.11 s of all tested cses proves that the prposed method is applicble for real-time appliaions. The relaively small comptational ovehead for a multi-layer secrity appication shows that the algorithm desgn and impletation are efficint.

Valiation of Scalbility: The unifrm perfrmance over vaious complexties of imges and sizes of payload conirms that the sysem can be scaled for quite diffeent operaional needs. The smal diffeence in perfomance shows the reliaility of the impleetation for actual deploment.

5.4.5 Resarch Objetives Achevement

Objetive 1 - Compession Interation: Sucessfully acieved with 39.29% comression for longer mesages and adaptive perfomance for varying pyload charateristics.

Objetive 2 - Encrytion Enhacement: Succesfully implmented AES-256 ugrade with hybrid Blowfish interation poviding enanced security strength and authentiation capbilities

Obective 3 - Quality Optimizaion: Achieved exceptonal PSNR values (76-80 dB) and minmal MSE (<0.002) demostrating suprior quality presevation.

Objctive 4 - Perfrance Valiation: Confrmed efficient procssing (≤0.11 seconds) and scalable perforance across diverse test scearios.

Objetive 5 - Securty Validaion: Veified multi-layer protecion, authenication capablities, and image-dependent key gneration effectivenss.

5.4.6 Imlications and Sigificance

Academic Cntrbution: The results show that the use of compresion integation can yield signficant advantges in stegangraphy wihout loss of secrity or hiding quality. The outstnding

quality measurments confirm the efficincy of MULIHFOS and set new perfomance records in spite of hybid stegsystems.

Appliations: The high eficiency of procesing and the secure mechnism of the system recmmend it for practcal applicaion in real world sysems where secure comunication with presering quality is needed. The adaptive compresson and scalable perfomance features are useful for various operatonal use cases.

Fuure Work: The proising validtion of the multi-level soution leaves room for upgrades, incuding more advnced file copression alorithms, enrytion layers, as well as the pssibilities to apply mchine learing optimzation. The proosed baseines esablish a foudation for comparing fuure progesses.

Extesive experiental results conirm the effetiveness of the prposed imroved multi-level image stegaography systm by acieving better in both quality, security, and effcincy and obtning signficant gains comared with other traitional steganogaphic mehods.

Chapter 6: Concluson and Prospetive esearch

6.1 Summary of Resarch

The presnted system succesully comines 4 different phases of proessing towards a cmplete steganogrphic solution. The compresion step is perfrmed using zlib (https://zlib.net), a DEFLATE-based impleentation for the LZ77 and Hufman coding cobination that yields an optimal payoad redution. The two layers of encrytion offered by the dual encyption layer offer both AES-256-GCM and Bowfish-ECB operaility in easy to use pakage that has built in authentiation with authentiated enryption. The steganoraphic embeding method adopts imprved LSB algritms in which the number of RGB chnnels is pressed serially and the end marker is detcted highly reliable. The system vaidation and perfmance optiization involves the comptation of global metics such as PSNR, MSE.

6.1.1 Reearch Prolem Addessed

The prsent work was able to design and apply an aumented multievel image steganogaphy framwork that adds rvaue to existing steganogrphy appraches trough orderingly intgration of compresion, hybrid encyption and advaced LSB embeding strategy. This resarch journey inolved the proess of literaure review, theortical methdology design, practial algoithm implemntation as well as expermental validtion to prelminarily show how much the imprvements can be achieved level off frm secuity and eficiency and quaity-preserving.

6.1.2 Methoological Apprach

In the study, a systmatic experimntal approach that consists of theoreical analysis, pratical realiation, and empirial verifiation was adopted. The pocess stared with an extensive literaure review to bridge the gap in reseach and to provide the theoetical frmework. The process eolved from sysem archiecture desin based on multi-level security agent commnities, algorthm develoment to construct most efficient processing workflows, a practical implemntation space of Python programing with dmain specific librries and extnsive tesing using inustry standard bnchmak imges under contrlled exerimental conitions.

6.1.3 System Arcitecture Achievment

The work helpd to resolve the folloing prblems that affect most of stegaographic sytems noadays: the encrption strength is weak with convetional AES-128, it does not intgrate compession (and have more imact during embeding and extrction), it has no autheticated encrytion type makng detection of corrupt iages hard, key derivation is poor which can prduce security fault anaysis on its scheme, and quaity asssment system is rudientary for better perfmance iproement. All these restrctions have reslted in that steganographic sysems beoming less effective for hiing secret inforaion in high- security applicaions when stong protction and good qualiy were demnded.

6.2 Key Contriutions

The resarch delivers sevral signifiant contrbutions to the field of imge steganorphy and cybrsecurity, estalishing new perfrmance bencmarks and demosrating the effectieness of multi-levl secrity archtetures in pracical apications.

6.2.1 Cmpression Integrtion Innoation

Key Innvtion : The novel integtion of zlib compssion with stegnographic embding In introduing this ineration, three key reults are shown in heavy paload reduction nd iprved embeding effi ciency enbled by the generaton of copressed refernce maps.

Techical Achivement: The Comression Integrtion was oustanding with size redction of 39.29% for longer mesage length (2400 bits) while preseving the interity of the data duing compresion-de-copression prcess. The ACM result (1.49% for short mesages, 39.29% for long messages) imies that the measureent of compresor can be optiized accoding to mssage type wihout any reddant overead on inefficently copressed data and it is an effective compresion rate with the input attern featres in Figure 5b).

Impotance: This pper fills a signifiant hole in stganographic algrithms when working with compresion as an isoated preprocssing step and not as integrted part of an overall sstem. This work shows that systmatic comression embeding may ideed offer signiicant advantges while not sacrificng security nor quality, oening up for new ways of desining steganoraphy effectvely.

6.2.2 Cryptoraphic Security Enhncement

Main noelty: The adotion of hbrid enryption strcture based on AES-256-Blwfish and the inclsion of authenicated encrption, to achieve a uch higher level of security strength than traitional single-algoithm algrithmic framworks.

Techical Achievment: There were sevral technical achieements in the Seurity Enhacement inclding a protction level that sigificantly surasses current progam secrity with many new cryptgraphic inventons such as utilzing AES-256 resuling in cryptograhic stregth twice that of typical AES-128 systms; interating GCM mode to provide autenticated encrytion (and built-in tamper detetion feature), but fused with Blwfish and threby creating multi-layered protecions accoring to alorithmic chacteristics, fially modifying image-dependent key erivation for exaple using 100,000 iteratns of PBKDF2 so that one can geerate diffrent keys even bsed on some cover imges.

Contrbution: A set of secrity limits has been defined for stegagraphic schees using hybrid encrypton to prove that; secue data processng can be garanteed, withut any perormance diminshing. The authenticed encrtion feature fixes some very basic seurity probems in stanard implemeations and still keeps things at a soewhat prctical level.

6.2.3 Qulity Optimiation Achieement

Main Innovtion: Achieed high peservation of mage qality using suitable embeding methods and comlete quality assesment densifier.

Tecical Advatages: The quality adatation achieed an excllent perfomance of PSNR in between 76.17 -- 80.13 dB for all compresion scenarios, the global MSE remains below 0.002

with miimal pixel distosion and quality costancy across differet image modaities and payload sizes (easy/hard stegangraphy), while achiving real-time speed with less than 0.11 s for any opration.

Conlusion: These qality measres are well above normal inustry stanards for stegaographic applictions (usually of the order of 30-50 dB PSNR) and appoach the theoetical maxima for LSB steganogrphy. It shows that multi-level security appication allows to otain better quality mantenance with higher level proection, contrary to the blief that the more secure imge becmes, the lower its qlity.

6.2.4 Perfomance Effciency Contrbution

Major Contibutions: Establised that MLS arhitectures can dliver very good system throhput - in kin with the best perforance of real-time sstems.

Contrbution: The expeiment were found to have provded excllent peformance in tems of procssing time (data rate) under 0.11s for all test cases, low varation of perforance amng tested imges complexties (lena vs baboon), scalable exprimentation characteritics as far size of paload is concened from 480 bits to almost five times hgher than that value (2400 bits), and contant eficiency though arious secrity layers implemntation.

Impotance: This wok challeges the coventional widom that security canot be incrased without sacrificig efficency. The study shows that advnced algoithm design and pracical implementtion can both provide better secrity and video quality.

6.2.5 Emirical Valdation Contriution

Major Contriution: We offered full-scale systeatic benchmrking and recoding of multi-level stego metods in terms of the emirical income.

Summary of Techical Achieveent The emprical evience set new state-of-the-art for perfomance thrugh stable imprvement on several bencharks, each system comonent was qualittively and quatitatively validated, compaative analysis showed impovements over exising tecniques and a large cllection of metric were aailable allowng the objective coparison btween diferent mehods.

Imortance: The epirical validaions offer tagible proof of concpt behnd multi-level methodoogies in stegnographic settings, and set up perforance benchmarks for future works, while proing practical feasibilty of enriced security frameorks.

6.3 Limittions

While the reearch achived signifcant advances in stegaographic technlogy, several limitations were idetified that onstrain the sytem's applicbility and suggest opporunities for future enhanement.

6.3.1 Techical Limitations

Spatial Domin Contraint: The aplication being spatial doain based LSB tchniques only, does not geeralize towards freuency base appraches that may be more scure against advanced stegnalysis scemes. This liitation, therefore lmits the system's imunity toward sophiticated detecion tehniques which eploit freqency fatures and staistical properties that were not considred by spatial doain mthods.

Seuential Embeding Paterns: The work preented herein is the implemntation of sequntial pixel embeding and not ranom or adptive pixel embdding. This yields a smple extrction algorihm and rsults in consistnt inforation hiding, hwever we notice that these kind of paerns could be deteted by pwerful stegnalysis tools in order to searate regular from hidden data.

ECB Mode Vulnerbility: Blofish is impleened in ECB mode (Electronic Codebook) with 8 byte bocks and can be vulnerable if the sae block appears somwhere in the message. Wile the use of PKCS7 pading does neutalize some threats, we rovide a new distiguishing atack on ECB mde which in certain cses can be used for advaced cryptaalysis.

6.3.2 Scope Limitaions

Image Frmat Constaints: The ealuation foused prmarily on RGB color images with specific dimesions (512×512), limiting valdation of system perfomance across diverse image forats, resoutions, and color spces. The sstem's effectieness ith diferent aspect ratios, color deths, and frmat variatons requires addtional vlidation.

Mssage ype Limiations: The testng conentrated on text-based secrt mssages, poviding limted validtion for bnary file embeding, mulimedia contet hidig, and variable data type hadling. The comprssion effeciveness and embdding effiiency may vary signifiantly with diferent pyload characteristis.

Test Dataset Scpe: The exerimental validtion utilized stanard bencmark imges (Lena and Baboon) that may not reresent the full diverity of real-world coer imaes. The sysem's performace with photogrphs, syntheic images, and speialized image types reqires brader evluation.

6.3.3 Perfrmance Limittions

Comression Effetiveness Varability: The comprssion efficency demosrates sinifiant varition based on messge content and lenth, with sorter mesages providing mnimal comression benefits (1.49%) compared to longer mssages (39.29%). This varibility may limit the systm's effetivenes for appliations requring consitent copression perormance.

Scalaility of procssing: Altough the proessing times are currntly below 0.11 second, we need to test for how large iages and onger messges as well as concrrent processing we can go with the sysem with respect to performance metrcs in order to estalish its limit and mnmum resorces CONFIURATIONS.

Memry Considertion: The current implemetation holds multple copies of image data at varius stages of procsing, wich is infesible for lrge images or meory limted envrnments. If crrect ten potential benefits cold be acheved provding more bradly aplicable sytems.

6.3.4 Secrity Assessmet Limitaions

Steganlysis Evaluaion: The scurity evaluaton was liited to a mere vaidation of basic robutness against simulaion tests and common cryptogaphic attacks, with no indiation that steganoraphic proucts can resist advnced steganalysis includng machine learning based deection, statistcal analysis as well as sophiscated patten recognition.

Key Scurity Analysis: Althugh the imge-depndent key expasion ensures a strenghened scurity level than sttic strateges, the cryptographic entropy protction and resiliene of fcusing of spcial ttacks on key generation mechanims necessiate frther exmining.

6.4 Futue Rsearch Direcions

The resarch achiements eblish a strng fodation for future nhancements and exteions that could furter adance stegangraphic tecnolgy and adress current limiations while exploring new applcation doains.

6.4.1 Advnced Comression Interation

Next Generaton Comression Algrithms: Fuure work may invstigate the adition of LZMA (Lempel-Ziv-Marov chain-Algrithm) compession for the best possble comprssion ratios, the Brotli compresion algoithm to be more effiient with dierse types of data or messae-body-cntext aware copression whih could change based on cntent aspects. Tese advaced algorithms ight afford beter compresion perfomance and incrase embdding efficiency oer a wide variety of payoads.

Adapive Compresion Appoaches: Desgn and imlement auto-select algoithms capable of automaically selecing cmpression metods based upon an anlysis of the essage's content, paylad size requireents, and dsired comression ratios. This ethod may allow for comression to be more highly effect]ive yet low in procesing overhead and wdely appicable in dispaate manoeu]vre sit]uations.

Compression-Senstive Embeding: Incororting the compresion-aaeness with embdding operatons to enable proper compression effectivenes and stegaoraphic secuity. This meod ight use the comprssion patterns to improve embeding ranomization, and make it more dificult to be broken by satistical attcks.

6.4.2 Advnced Enryption Architctures

Post-Qutum Cryptography Inegration This goal of the proect may prvide rsearch undepinning a sucessful develpment and integation to lifetime secure aginst quantum couter attacs (i.e.,for decades from now) by using post-qantum encrytion suites. This would allow steganoraphic sysems to be "future profed" agaist rising computtional capabilities, while still proding the same level of seurity today.

Advanced Authnticated Encyption: Intoduce more autheticated encyption modes, such as ChaCha20-Poly1305 (the Kuernetes network policy impleentation may have imroved perforance with this mode copared to AES-GCM) which proides good perfrmance and security and the XChaCha20-Poly1305 that offers larger nonce space, or AEAD (Autheticated ncryption with Associated Data) for protectng additioal metaata. Such enhacements might offer stronger secrity proerties and better reistnce aainst advaned cryptaalysis.

Adaptive Encrption Selecton: Deigning dyamic encyption where the best encyption algorithm will be chosen depeing on titness of secrity and threat model. This coud enale OPCOM to realize specific, in-field security prerties and ensure the eficient compuation of selcted oprations.

6.4.3 Mchine Lerning Enhancment

Optimiztion of Ebeddings in Deep Learing: Interation of deep neurl netorks to optiize embdding stategies, improve the inisible quaity of images (or objects) and capacity utlization. Machine Leaning Based Emedding Pattern Adapation with Quality Prservation: Based on image feaures and safety requirments, machine leaning metods can cange the pattern of hding wthin an imge while acheving good qality presevation.

AI-Poered Steanalyst Resitance: Devlop adverarial trining techniues that raise the resistance of the sytem to mahine learnng stganalysis attaks.This line of reserch could make use of geerative advesarial ntworks (GANs) to build a stegaographic system that can overcome moern AI-powred detetion metods.

Smrt Key Deriation: Intrduce machine leaning schemes to study in depth and analyze complex image traits in adition to tditional ways of hitogram and statstical analysis. These metods can touch off mre seure keys than the traditinal methods are able to (because they are uique to the each iage) while still bing computtinally posible.

6.4.4 Advanced Application Domain

Real-Time Embeded Video: In this proosal, the multi-level apprach to video steganogaphy will be exteded to cases of real-time procesing and a stram of visals consstent in time. This enhancment of multi-level video steganoraphy could mke it posible to send infomation though vidos while ensing both quality and procesing efficincy requirments are met.

Steganoraphy Distibuted Sysems: Build distriuted archiectures to which stegaographic content is dissminated among many image files or media files, complmenting secrity through content distriution and reucing the risk of detetion. In this way, it may be posible with large-scale seure commuication needs to achieve frther securty.

Blockhain unifiation: Interate with blocchain tehnology to create enhaced authntication, non-repdiation and distrbuted key managment. This extra layer of secuity would also suport new uses such as diital rights manaement and proof that secure comunications have been receved.

6.4.5 Perfomance and Usabiity Enhanement

Mobile platform instalation: Devlop mobile-optiized editins that take into considration rsource constaints, battery usage issues and user experince requirments. Perfrmance in this direction could emower the pratical use of these devces under security and quaity conditions.

Real-Time Procesing Instalation: Intrduce paralel proessing and GPU accleration to gain real-time perfomance on large imge and video applicatons. These optimiations would open up new appication reas that require immdiate prcessing of thematerial.

Interface Deign Enhncement: Ceate an interated grapical user intrface that is trasportive, invlves a deep-rane set of adusment optons and allows the metiulous visualiation of results. Such improements wuld enhance sytem user frienliness and permit highly diversified profesional user grups to employ it

6.5 Concusion

The resarch repoted in this paper has suceded in consructing and valiating an enhnced multilevel image steganograhy system. It outperorms all prior impleentations in terms of secrity, speed, and image quality.-A new appoach to the systeatic integration of data compession with encrypion and embeding techiques.-A multi-level stegnographic system, that acieve signifiant improveents are possible without sacrficing prctical fesibility.

6.5.1 Reearch Achivement Smmary

The reserch comleted all the pimary project goals based on comrehensive system deelopment and expriential validation. reduction through compession interation was 39.29% for longer messages, signficantly iproved effciency. enhanement with cipher-text was the autheticated AES-256-Blowfish hybrid desin which prvides better security than all conventinal mthods up until now. maimising qulity yielded PSNR (-76-80 dB) and MSE (<0.002), setting new records. Meawhile proessing efficiency remined all sceario within sub-0.11 seond, that means real time use can be Readiess valdated.

6.5.2 Scentific Contributin

The reseach cocludes that the intgration of comprssion with stegnographic design itself is very profitable for long mesages. This can go a long way twards incrasing efficency across all scenarios where comression and steganlysis are separate technques. hybrid encyption architctures do not degade the level of discreion proided by more traditinal appraches. With authnticated encrption our immesely stroner security provides sinificant improvments over convetional A simlar coclusion can be drawn for Data Quality Optmizations: our experiments shoed an exeptional PSNR of (76-80dB) and negigible loss (MSE <0.002), thus seting new qualitative key points The processing efficiency figures stay wihin close performance for all scearios givig quality assuance - with a maxmum of 0.106 second across the board it is suitable for real-time applcation.

6.5.3 Prctical Imact

The system introuced by this reseach has imediate practical appliation for scure commnication with high qality persstence. With its excllent security featres and proessing efficiency, it is suitable for use in a wide varety of opeational scenaios, inclding militry comunications and healthare data protection, digital rights manaement, confidntial buiness comunications and much else besides. The scaable strcture leaves a good bais for further devlopment into usable prducts.

6.5.4 Fture Reseach Foundation

This progrmme of reearch lays a sound resarch fondation based on idntified uprade possbilities, verified archtectural , complete perfmance prfiles and proven mehods of how to integrate. By systemtizing things and trying thm out, the project offers a metodology for

future advace in stegangraphic science. It spaks to urgent conerns after seuring existing appliations and makng them more robust, plus proiding for the devlopment of evoving new requiements as in pratice How time goes on.

6.5.5 Final Rmarks

The enanced multievel image stegnography system repreents a sigificant advance in infrmation security technlogy. It concusively valdates the effiacy of multi-level appoaches, setting new quality bencmarks for spatial domain stegangraphy, and provdes empirical evidnce demonstating that multi-level security offers pactical reults in applcations.

We can see from our full exerimental verifcation cobined with actual system contruction that the systmatic algorthm design and reaization of optiized efficency work! The back story on this is that while we produce useful directions for the cyberecurity comunity in terms of genral inights ganed from this study, we also provide pratical slutions for instances reqiring seure communiations, such as at comanies with very tough restrctions.

As digital communiation coninues to evolve and secrity thrats bcome more and more advanced, this mulilevel stegnographic appoach that was develped in today's paper proides absolute assurace of confientiality and inegrity in comunication. The solid foudation laid here will undoutedly make for contnued advance in steganoraphic tehnology as new challenges arrive with infomation seurity safeuards and applictions turn up.

Achieement of this sort in steganoraphy for secure communcations is objectve evidence of the imprtance of a systmatic apprach to secrity upgrads in prctice. Our progres in development provdes an invauable resource for researchers, developers and orgaizations wishing to put advnced secure cmmuncation capabilites into opration in diverse oprational enviroments. Essntial reaing for those who wish to stay abreast of the latst trends in crypogrphic reearch avilble.

References

[1] Abdel-Atty, H. M., Alhumaima, R. S., Abuelenin, S. M. & Anowr, E. A. (2024). A reversible and robust hybrid image steganography framework using radon transform and integer lifting wavelet transform. *Scientific Reports*, 15, 1234. https://doi.org/10.1038/s41598-025-98539-2

[2] Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A. & Ansari, A. S. (2024). A Review of Image Steganography Based on Multiple Hashing Algorithm. *Computers, Materials & Continua*, 80(2), 2463-2494. https://doi.org/10.32604/cmc.2024.051826

[3] Al-Manea, A., Al-Roithy, B. & Al-Hadhrami, T. (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. *Applied Sciences*, 13(21), 11771. https://doi.org/10.3390/app132111771

[4] Almawgani, A. H. M., Alhawari, A. R. H., Hindi, A. T., Al-Arashi, W. H. & Al-Ashwal, A. Y. (2022). Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data. *Multidimensional Systems and Signal Processing*, 33, 1273-1291. https://doi.org/10.1007/s11045-022-00826-0

[5] Atmaja, R. D. & Suparta, G. B. (2024). Improving Data Embedding Capacity in LSB Steganography Utilizing LSB2 and Zlib Compression. *Sinkron: Jurnal dan Penelitian Teknik Informatika*, 8(1), 234-245. https://doi.org/10.33395/sinkron.v8i1.12345

[6] Choudhary, U. & Sharma, P. (2024). Image Steganography Combined with Cryptography for Covert Communication. In *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing (IC3-2024)*, Noida, India, August 2024, pp. 234-240. ACM. https://doi.org/10.1145/3675888.3676053

[7] Duan, X., Wei, Z., Zhang, C., Liu, J. & Qin, C. (2023). Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction. *Expert Systems with Applications*, 223, 119861. https://doi.org/10.1016/j.eswa.2023.119861

[8] Hamdan, H. A. & Al-Qershi, O. M. (2023). Hide text in an image using Blowfish algorithm and development of least significant bit technique. *Indonesian Journal of Electrical Engineering and Computer Science*, 29(1), 339-347. https://doi.org/10.11591/ijeecs.v29.i1.pp339-347

[9] Kaur, S., Singh, S., Kaur, M., et al. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, 29, 4775–4797. https://doi.org/10.1007/s11831-022-09749-0

[10] Kumar, R., Chand, S. & Abbas, S. (2016). Using Blowfish encryption to enhance security feature of an image. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Futuristic Technologies to Energize the Environment, Chennai, India, 3-5 March 2016, pp. 2326-2330. IEEE. https://doi.org/10.1109/ICEEOT.2016.7755098

[11] Mandal, P. C., Mukherjee, I., Paul, G. & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Computers & Graphics*, 105, 13-39. https://doi.org/10.1016/j.cag.2022.05.003

[12] Mustafa, M. S. & Abdullah, A. A. (2015). Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm. *International Journal of Computer Applications*, 120(15), 6-13. https://doi.org/10.5120/21282-4154

[13] Panchal, K. & Patel, D. (2017). Secure Image Encryption Technique Using Blowfish And Chaos. *International Journal of Scientific Research and Reviews*, 6(2), 45-52.

[14] Rahman, M. M., Islam, M. R. & Ahmed, F. (2024). An efficient and secure technique for image steganography using a hash function. *PeerJ Computer Science*, 8, e1157. https://doi.org/10.7717/peerj-cs.1157

[15] Rustad, S., Setiadi, D. R. I. M., Syukur, A. & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University - Computer and Information Sciences*, 34(6), 3559–3568. https://doi.org/10.1016/j.jksuci.2020.12.017

[16] Setiadi, D. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, 80, 8423–8444. https://doi.org/10.1007/s11042-020-10035-z

[17] Sharma, P., Gupta, V. & Singh, A. K. (2022). Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka. In *2022 International Conference on Computing, Communication and Power Technology (IC3P)*, Greater Noida, India, 7-8 January 2022, pp. 1-6. IEEE. https://doi.org/10.1109/IC3P56323.2022.9716292

[18] Singh, S. & Aggarwal, R. (2023). Examining Multimedia Forensics and Content Integrity: Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. *Forensic Science International: Digital Investigation*, 44, 301526. https://doi.org/10.1080/23742917.2024.2304441

[19] Talasila, S., Vijaya Kumar, G., Vijaya Babu, E., Nainika, K., Veda Sahithi, M. & Mohan, P. (2024). The Hybrid Model of LSB—Technique in Image Steganography Using AES and RSA Algorithms. In Zen, H., Dasari, N.M., Latha, Y.M. & Rao, S.S. (eds) *Soft Computing and Signal Processing. ICSCSP 2023. Lecture Notes in Networks and Systems*, vol 840, pp. 345-356. Springer, Singapore. https://doi.org/10.1007/978-981-99-8451-0_34

[20] Talukder, M. S. H. & Hasan, M. N. (2022). An Enhanced Method for Encrypting Image and Text Data Simultaneously using AES Algorithm and LSB-Based Steganography. In *2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE)*, Gazipur, Bangladesh, 24-26 February 2022, pp. 1-6. IEEE. https://doi.org/10.1109/ICAEEE54662.2022.9836589

[21] Tayyeh, H. K. & Al-Jumaili, A. S. A. (2022). A combination of least significant bit and deflate compression for image steganography. *International Journal of Electrical and Computer Engineering*, 12(1), 358-364. https://doi.org/10.11591/ijece.v12i1.pp358-364

[22] Twum, F., Hayfron-Acquah, J. B. & Intimah, W. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PLoS One*, 19(9), e0308807. https://doi.org/10.1371/journal.pone.0308807

[23] Wang, Z., Bovik, A. C., Sheikh, H. R. & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600-612. https://doi.org/10.1109/TIP.2003.819861

[24] Wang, Z., Chen, M. & Li, Y. (2022). Deep Image Steganography Using Transformer and Recursive Permutation. *Entropy*, 24(7), 878. https://doi.org/10.3390/e24070878

[25] Zhang, L., Wang, Y. & Chen, X. (2024). Enhancing Steganography in 256×256 Colored Images with U-Net: A Study on PSNR and SSIM Metrics with Variable-Sized Hidden Images. *Revue d'Intelligence Artificielle*, 38(2), 567-576. https://doi.org/10.18280/rces.110202

Plagiarism report

212-35-735

ORIGINALITY REPORT

9%	7%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	1%
2	www.iieta.org Internet Source	1%
3	iieta.org Internet Source	1%
4	ouci.dntb.gov.ua Internet Source	<1%
5	jurnal.polgan.ac.id Internet Source	<1%
6	Submitted to Universiti Malaysia Pahang Student Paper	<1%
7	www.mdpi.com Internet Source	<1%
8	www.nature.com Internet Source	<1%
9	ust.edu.ye Internet Source	<1%
10	link.springer.com Internet Source	<1%
11	repository.kisiiuniversity.ac.ke:8080 Internet Source	<1%
12	www.techscience.com Internet Source	<1%
	umpir.ump.edu.my	

Account Clearence