Internship Report

On

Cyber Security

Submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE & ENGINEERING

Submitted to:
Er. Nidhi Sengar
e15466

Submitted By:
Gurpreet Singh
19BCS1961

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Chandigarh University, Gharuan

May 2023

CERTIFICATE

This is to certify that the work embodied in this Internship Project Report being submitted by **Gurpreet Singh** UID **19BCS1961,** 8th Semester for partial fulfilment of the requirement for the degree of **Bachelor of Engineering in Computer Science & Engineering** discipline in **Chandigarh University** during the Internship period is a record of bonafide piece of work, carried out by student under supervision and guidance in the **Department of Computer Science & Engineering, Chandigarh University.**

APPROVED & GUIDED BY:

Er. Nidhi Sengar

e15466

INTERNSHIP CERTIFICATE

NOT APPLICABLE RIGHT NOW …….

ACKNOWLEDGEMENT

I would like to express my sincere gratitude and appreciation to all those who have contributed to the successful completion of this project. Their support and guidance have been invaluable throughout this journey.

First and foremost, I would like to thank our team lead Girish Sai, for their guidance, insightful comments, and constructive suggestions to improve the quality of the project work.

I would like to thank all the teachers who helped us by giving us advice and guidance for the project. Also, I would like to thank my family and friends for their support. Without that support we couldn't have succeeded in completing this project.

I would like to express my appreciation to Chandigarh University for providing the necessary resources and facilities for conducting this research. Their support has played a significant role in the successful execution of this project.

I also acknowledge the support of our parents towards the success of our project. Their motivation and financial support are greatly appreciated. Lastly, I would like to thank everyone who helped and motivated us to work on this project.

Gurpreet singh (19BCS1961)

Table of Contents

CERTIFICATE ii

INTERNSHIP CERTIFICATE iii

ACKNOWLEDGEMENT iv

Table of Contents v

List Of Figures vii

ABSTRACT viii

Chapter – 1 1

INTRODUCTION 1

1.1 Company Details 1

1.2. Role Details 2

1.3. Departmental Structure 3

1.4. Location and Spread 5

1.4.1 List of All Location 6

1.5. Number of Employees: 7

1.6. Technicians 8

1.7. Administers 10

1.8. Division of the Company 11

Chapter – 2 13

Project Description 13

2.1. Internship site Description 13

2.2. Problem Statement 14

2.3. Scope of Work Completed 14

2.4. Purpose of the Summer Internship 16

2.5. Reason for Choosing the company: 17

2.6. Nature of Work Carried Out: 18

Chapter – 3 20

Technology Details 20

3.1. Technology Details: 20

3.1.1. Cryptography: 20

3.1.2. Python: 22
3.1.3. Powerful image processing modules: 23
3.1.4. Cryptography Libraries: 25
3.1.5. Data Encoding: 26
3.1.6. File Handling and I/O: 28
Chapter – 4 30
Project Methodology 30
4.1. Methodology: 30
4.2. Project Flow: 33
4.3. Project Details: 34
4.3.1 Approach/Solution: 35
4.4. Flow Diagram: 37
4.5. System Design: 38
4.5.1 Use Case Diagram: 38
4.5.2: Activity Diagram: 39
3.5.3. Data Flow Diagram: 40
Chapter – 5 42
Project Challenges and Benefits 42
5.1. Project Challenges/Solutions: 42
5.2. Benefits to the Company: 45
Chapter – 6 47
Conclusion 47
References 48

List Of Figures

Figure No.	Title	Page No.
1	Project Methodology	30
2	Menu Page	32
3	Architecture diagram of proposed system	35
4	Encryption flow diagram	38
5	Decryption flow Diagram	39
6	Use Case Diagram	40
7	Activity Diagram	40
8	DFD Level 0	41
9	DFD Level 1	41
10	DFD Level 2	42

ABSTRACT

This internship project report provides a comprehensive overview of the work conducted during an internship as a Cybersecurity Associate at Accenture. The primary objective of the internship was to gain practical experience in the field of cybersecurity and apply theoretical knowledge in a real-world environment. The report focuses on the various tasks, challenges, and accomplishments encountered during the internship period.

The report begins with an introduction to Accenture and its cybersecurity division, highlighting the importance of cybersecurity in today's digital landscape. It then delves into the specific responsibilities and projects undertaken during the internship, including vulnerability assessments, penetration testing, security incident response, and the implementation of security controls.

The internship involved collaborating with a team of experienced cybersecurity professionals, providing an opportunity to learn and work on diverse projects. The report discusses the methodologies and tools employed in different projects, emphasizing the significance of a structured approach to cybersecurity.

Furthermore, the report highlights the importance of continuous learning and professional development in the cybersecurity field. It examines the various training programs and certifications obtained during the internship, demonstrating a commitment to enhancing knowledge and skills in the ever-evolving field of cybersecurity.

Throughout the internship, the report showcases the application of theoretical concepts and best practices to real-world scenarios. It outlines the challenges faced and the strategies employed to mitigate cybersecurity risks, emphasizing the significance of proactive measures to protect organizational assets.

Finally, the report concludes with a summary of the overall experience gained during the internship and its impact on personal and professional growth. It reflects on the accomplishments, lessons learned, and the value of the internship in bridging the gap between academic knowledge and practical implementation in the field of cybersecurity.

Overall, this internship project report provides an in-depth analysis of the internship experience as a Cybersecurity Associate at Accenture. It serves as a comprehensive evaluation of the knowledge, skills, and practical application of cybersecurity concepts, contributing to the final assessment of the intern's performance during the internship period.

Chapter – 1

INTRODUCTION

1.1 Company Details

Accenture is a top international professional services firm that provides a wide range of services and solutions in more than 120 countries. Accenture, which has its global headquarters in Dublin, Ireland, has made a name for itself as a reliable business partner. The services offered by the corporation include a wide range of sectors, including communications, media, technology, financial services, health, and public service. Accenture specializes in assisting clients in developing winning strategies, offering first-rate consulting services, utilizing digital technologies for change, supplying cutting-edge technological solutions, and streamlining corporate processes. Accenture creates a culture of collaboration, ongoing learning, and diversity with a global workforce made up of bright professionals from many backgrounds. The business is renowned for its dedication to innovation, spending money on R&D to be on the cutting edge of new technology. Accenture also actively participates in corporate responsibility, with an emphasis on skill development, sustainability, and community contributions. Accenture can continue bringing about positive change and providing value to its clients all around the world thanks to its strong leadership, reputation in the sector, and commitment to quality.

The following are some essential Accenture facts:

1. **Offerings and Services:**
    - **Strategy:** Accenture assists clients in creating company plans that promote expansion and increase competitiveness.
    - **Consulting:** To assist clients in enhancing their operations and company performance, they provide management and technology consulting services.
    - **Digital:** Accenture helps customers transform their businesses and consumer experiences by using the potential of digital technologies.
    - **Technology:** They offer a variety of technology services, such as infrastructure management, system integration, and application development.
    - **Operations:** Accenture assists clients in streamlining and cost-cutting their business procedures.

2. **Industry Focus:** Accenture services clients across a range of industries, including but not restricted to:
    - Media, communications, and technology.
    - Financial Services.
    - Products related to health and public services, as well as consumer goods, retail, and travel.
    - Energy, utilities, chemicals, and resources (including natural resources).
3. **Innovation and Research:** Accenture places a high priority on innovation and makes significant investments in research and development to stay on the cutting edge of emerging technologies. Additionally, they have several innovation hubs and labs where they work with customers and partners to promote innovation and create brand-new solutions.
4. **Global Presence:** Accenture has offices and operations in more than 120 countries, giving it a sizable global footprint. Governments, global firms, and businesses of all sizes are among their many international clients.
5. **Leadership and Recognition:** A group of seasoned executives, including the CEO and several business unit leaders, guide Accenture. For its achievements in performance, innovation, and corporate citizenship, the company has won various accolades.
6. **Workforce and Culture:** Professionals from various ethnicities and backgrounds make up Accenture's diverse and inclusive workforce. They place a high importance on cooperation, teamwork, and lifelong learning. The business is renowned for its vibrant workplace culture and dedication to sustainability and social responsibility.
7. **Corporate Citizenship:** Accenture regularly participates in efforts for corporate social responsibility. They offer programmers that are concentrated on fostering local community involvement, environmental sustainability, and skill development. The goal of Accenture's corporate citizenship initiatives is to improve society.

1.2. Role Details

I am working as a Cyber Security Intern. My responsibility as an Accenture Cyber Security Intern is to support the integrity and safety of the digital assets and data of our clients. I have been trained in various technologies like Windows Server 2016, ITIL, SIME, computer networks, cryptography, and Microsoft Azure. To implement and maintain security measures,

carry out vulnerability assessments and penetration tests, and examine security occurrences, I collaborate closely with skilled cyber security professionals. In addition, I contribute to risk analyses and compliance initiatives as well as the creation of incident response plans.

I have the chance to learn from professionals in the field and get practical experience in real-world situations because of my job. I work with the team to develop and execute efficient security solutions, keep an eye on network traffic for potential dangers, and help in keeping a high level of security. I play a crucial role in protecting sensitive information, reducing risks, and making sure that our clients are well-protected in the ever-changing threat landscape of today by utilizing my knowledge and learning from experienced practitioners.

I support Accenture's dedication to providing top-notch cyber security services as an intern. I contribute to our clients' overall company resilience and the strengthening of their security defenses by actively engaging in initiatives and using my talents. I'm thrilled to be a part of a group that places a high importance on innovation, lifelong learning, and remaining on the cutting edge of new cyber security solutions. Through my work, I hope to advance professionally and personally while having a significant impact on the cyber security industry.

1.3. Departmental Structure

Accenture uses a departmental structure to successfully deliver its extensive variety of services and solutions. Here is a rough description of the typical departmental structure at Accenture, while specific structures may vary depending on the area and business unit:

- **Leadership Team:** Senior executives who occupy significant roles within the organization make up Accenture's leadership team. They oversee determining the organization's overarching strategic direction, establishing corporate objectives, and overseeing daily operations. The leadership group monitors the successful realization of Accenture's vision and ensures alignment among various business groups.

- **Business Units:** Accenture is divided into various divisions that concentrate on various sectors of the economy or service areas. Because of its organizational structure, Accenture can have extensive industry knowledge and customize its services to meet the specific requirements of clients in each area. The business divisions oversee creating

industry-specific solutions, spotting market trends, and resolving issues that clients in those industries are facing.

- **Groups/Practices:** There are groups or practices that specialize in fields or competencies inside each business unit. These groups could be set up according to technical specialties (such cloud services, cybersecurity, or data analytics) or knowledge of a particular sector of the economy. To provide clients with specialized solutions and services, they make use of their specialized knowledge. These organizations promote cooperation, knowledge exchange, and the creation of best practices in their specialized fields.

- **Service Lines:** Accenture's services are divided into various service lines that correspond to various functional specialties. Each service line offers specialized services and focuses on a certain area of client interactions. For instance:

    - **Strategy:** This service assists clients in creating profitable business plans that maximize efficiency and promote expansion.
    - **Consulting:** The consulting service line gives clients advise services to assist them overcome difficult business problems and enhance performance.
    - **Digital:** The key objective of Accenture's digital service line is to employ digital technology to transform client organizations, improve consumer experiences, and spur innovation.
    - **Technological:** This service line includes a variety of technological services, such as infrastructure management, system integration, application development, and emerging technologies.
    - **Operations:** Through process optimization, automation, and outsourcing, the operations service line assists clients in increasing the effectiveness of their business operations and reducing costs.
- **Supporting Roles:** Accenture offers several support operations in addition to its primary business divisions and service lines that offer vital services to the company. These include operations, marketing, finance, legal, and human resources. These support roles make it possible for internal operations to run smoothly and make sure that the infrastructure and resources required to support client engagements and business growth are available.

- **Project Teams:** Within each business unit or practice, project teams are created to carry out client engagements. These teams often include professionals from several fields, including consultants, technologists, project managers, and subject matter experts, and they are cross-functional in nature. Depending on the demands of each engagement, project teams' makeup may change. To comprehend customer demands, create solutions, and provide clients with value, these teams collaborate.

1.4. Location and Spread

Accenture has a worldwide footprint and conducts business in many nations. The business can efficiently serve clients in many regions because to its vast network of offices and delivery centers.

Accenture has a substantial presence in India thanks to its several locations and delivery hubs spread around the nation. The business has been in business in India for many years and has made a name for itself as a top supplier of outsourcing, technology, and consulting services. Here are some project summaries and an overview of Accenture's locations in India:

- **Bangalore:** One of Accenture's main offices is in Bangalore, a significant technology hub in India. The company's Bangalore office focuses on offering a variety of services, including business process outsourcing, application development, analytics, and technology consulting. Accenture frequently works with international clients on projects in Bangalore that aim to accelerate digital transformation, introduce cloud technologies, and streamline business processes.
- **Mumbai:** Accenture's Mumbai office is a crucial hub for its activities in India. Accenture uses its knowledge of financial services to assist clients in this sector. Mumbai is renowned as a major financial and commercial hub. Mumbai-based projects may touch on industries including banking, insurance, capital markets, and risk management. Accenture also serves clients in other sectors, such as the consumer goods, media, and telecommunications industries.
- **Delhi/NCR:** The National Capital Region (NCR) office of Accenture serves clients in and around Delhi. The initiatives in this area cover a range of industries, including manufacturing, public administration, energy, and utilities. To execute technology solutions, build digital strategies, and improve operational effectiveness, Accenture

works with customers. The business also supports public sector projects for digital transformation and e-governance.

- **Chennai:** One of Accenture's delivery centers, located in Chennai, provides technological services, application development, and maintenance. Software development, quality control, and application support are frequently included in projects in Chennai for clients in sectors like healthcare, retail, and automotive. Chennai plays a vital part in Accenture's global delivery network as well, supplying clients worldwide with affordable and reliable services.
- **Hyderabad:** Accenture's focus in Hyderabad is on innovation and technology. One of Accenture's biggest technological delivery centers, with an emphasis on cloud services, cybersecurity, data analytics, and artificial intelligence, is in the city. In Hyderabad, projects entail working with international clients to develop and put into practice cutting-edge solutions, utilizing emerging technology, and promoting digital transformation.
- **Pune:** Accenture's office in Pune focuses on application development, technology services, and delivery excellence. Manufacturing, the automotive industry, and telecommunications are all covered by the initiatives in Pune. To promote corporate growth and operational effectiveness, Accenture works with clients to optimize business processes, improve supply chain operations, and integrate advanced analytics solutions.

1.4.1 List of All Location

Americas:

- **US:** New York, Chicago, San Francisco, and Washington, D.C. are just a few of the major American cities where Accenture has offices and delivery centers.
- **Canada:** Accenture has offices in several Canadian cities, including Toronto, Vancouver, and Montreal.
- **Latin America:** Brazil, Mexico, Argentina, Colombia, and Chile are among the nations in Latin America where the corporation has a large presence.

Europe:

- **UK:** Accenture has offices in London, Dublin, and other locations throughout the UK and Ireland.

- **Germany:** Accenture has offices in Frankfurt, Munich, and Berlin, among other major German cities.
- **France:** The business conducts business in well-known French cities like Paris, Lyon, and Toulouse.
- Amsterdam and other Dutch cities are home to Accenture offices.
- **Spain:** Cities like Madrid and Barcelona are home to the corporation.
- **Italy:** Milan, Rome, and other Italian cities are where Accenture has offices.
- Accenture has locations and delivery hubs in several other European nations, including Sweden, Switzerland, Belgium, Poland, and Denmark.

Asia Pacific

- **India:** Accenture has numerous offices and delivery centers in Indian cities like Bangalore, Mumbai, and Delhi, giving the country a major amount of its overall business.
- **Australia and New Zealand:** Accenture has operations in Auckland, New Zealand, as well as Sydney and Melbourne, two of the largest cities in Australia.
- **Singapore:** The business has a location there that serves as the Asia Pacific region's operational center.
- **China:** Accenture has offices in Beijing and Shanghai and provides its services to Chinese clients.

Eastern Europe and Africa:

- **United Arab Emirates:** Accenture has offices in Abu Dhabi and Dubai that serve UAE clients.
- **South Africa:** The business operates in Johannesburg and Cape Town and offers services throughout the continent of Africa.
- **Other Middle Eastern and African nations:** Accenture has offices in Saudi Arabia, Qatar, Egypt, and Kenya, among other nations.

1.5. Number of Employees:

Accenture is a global professional services company that provides consulting, technology, and operations solutions to clients in various industries. The size and diversity of Accenture are indicated by the number of workers. One of the top providers of professional services in the world, Accenture assists clients across a range of industries with digital transformation, operational efficiency, revenue development, and citizen services. Accenture was the largest consulting firm in the world by staff count in 2023, according to its most recent annual report, with 738,000 people worldwide. Accenture's workforce has grown significantly over the past

few years, reflecting the company's rapid expansion into new markets and services. Accenture workers come from a variety of backgrounds, cultures, and skill sets, and they collaborate to provide value to their clients and communities. White people make up 47% of Accenture's workforce, followed by Asian people (24%), and Hispanic or Latino people (13%). At Accenture, the typical employee earns $85,479 annually.

India: With 170,000 employees, India is Accenture's single-largest workforce geography. Accenture has operations in important cities like Bangalore, Chennai, Delhi, Hyderabad, Kolkata, Mumbai, and Pune. Clients in India can choose from a variety of Accenture services and products, such as those for digital transformation, cloud computing, artificial intelligence, cybersecurity, and social impact.

United States: Accenture's headquarters are in this country, which is also one of its major markets. Accenture has more than 65 offices nationwide and employs more than 50,000 individuals. Accenture works with clients in a range of sectors, including government, retail, energy, health care, and financial services. Accenture also maintains a few innovation hubs and delivery locations in the US, where it works with customers and partners to develop new products.

Philippines: Accenture has more than 50,000 employees in the Philippines, another significant location for the company. Manila, Cebu, Davao, and Ilocos are all home to Accenture offices. Customer service, finance and accounting, human resources, and analytics are just a few of the business process outsourcing (BPO) services that Accenture offers to clients in the Philippines and overseas. Additionally, Accenture provides technological services like data science, software engineering, and cloud computing.

China: Accenture employs around 17,000 people in this rapidly expanding market.3 Office locations for Accenture may be found in Beijing, Shanghai, Guangzhou, Shenzhen, Chengdu, Chongqing, Dalian, Nanjing, Tianjin, and Xian. About digital transformation, innovation, and sustainability, Accenture supports clients in China. Accenture also collaborates with startups and local universities to support entrepreneurship and talent.

1.6. Technicians

A variety of technicians are employed by Accenture to support its business operations and provide clients with services. These experts are essential for maintaining hardware and

software systems, guaranteeing the efficient operation of technology infrastructure, and offering technical support. Here are some typical categories of technicians employed by Accenture, though specific roles and duties may differ. Here are some common types of technicians used in Accenture:

- **IT support technicians:** These oversee offering clients and internal staff members technical support and troubleshooting assistance. They deal with a variety of hardware and software difficulties, including network connectivity issues, troubleshooting software bugs, helping with hardware installations, and detecting and fixing software faults. They are essential in ensuring that technological systems run smoothly and that any problems are fixed quickly to limit disruptions.
- **Network Technicians:** Computer network design, installation, and maintenance are the areas of expertise of network technicians. They maintain the effective operation of the network infrastructure and configure network devices like switches and routers. Network technicians fix connectivity problems, keep an eye on network performance and security, and put strategies in place to boost network efficiency. Their knowledge contributes to the reliability, security, and scalability of Accenture's networks to satisfy the organization's communication and data transfer requirements.
- **System administrators:** At Accenture, system administrators oversee and maintain servers, operating systems, and related infrastructure. They manage duties such server installation and configuration, user account administration, access control management, system performance monitoring, and system upgrades and patches. System administrators are essential to data backup and recovery because they make sure that important data is safeguarded and can be recovered in the event of any unanticipated circumstances or system breakdowns.
- **Data Centre Technicians:** Working in the day-to-day operations of Accenture's data centers, which house vital IT equipment, is what data center technicians do. They guarantee the proper operation of the data center's servers, storage units, and networking hardware. Data center technicians oversee duties like monitoring and maintaining the humidity and temperature levels in the data center, supervising the deployment and replacement of hardware, and assuring adherence to environmental and security regulations. They work to keep Accenture's data center infrastructure accessible, dependable, and secure.
- **Cloud technicians:** Cloud technicians are experts in administering and maintaining cloud platforms and infrastructure, such as Google Cloud Platform, Amazon Web

Services (AWS), and Microsoft Azure. They oversee managing cloud-based applications and services as well as providing and configuring cloud resources, assuring security and compliance, and improving cloud performance. Accenture and its clients can take advantage of the scalability, cost-efficiency, and flexibility of cloud computing thanks in large part to the work of cloud technicians.

- **Field technicians:** Field technicians perform on-site support, installation, and maintenance services at client sites or remote locations. They help set up equipment, debug hardware and software problems, fix or replace broken equipment, and make sure technological systems are running smoothly. The face of Accenture's technical support team, field technicians frequently provide clients with hands-on assistance and make sure that their technological needs are effectively satisfied.

1.7. Administers

Effective management and support of Accenture India's activities depend on administrative positions. These specialists manage a variety of non-technical aspects of the business, guaranteeing efficient operations and organizational structure. Typical administrative positions at Accenture India could be:

- **Human resources (HR) specialists:** HR specialists oversee employee relations, performance management, onboarding, training, and talent acquisition. They enhance worker well-being, enforce adherence to labor regulations, and promote a positive workplace environment.
- **Finance and accounting staff**: They oversee managing the business's financial operations, including budgeting, financial reporting, accounts payable, accounts receivable, and financial analysis. They guarantee accurate financial records and provide financial insights to assist in decision-making.
- **Marketing and Communications Specialists:** These professionals' market the name, goods, and services of Accenture India. To promote corporate growth and client involvement, they manage marketing strategies, digital marketing, content generation, public relations, and customer communication.
- **Project managers:** They are responsible for the successful planning, implementation, and completion of projects at Accenture India. In addition to managing project risks

and stakeholder expectations, they collaborate with cross-functional teams to make sure project budgets and timeframes are fulfilled.

1.8. Division of the Company

Across its many business units and service lines, Accenture provides a wide variety of job roles. Here are some typical work profiles you might find at Accenture, while precise job titles and profiles may vary depending on the division, industry focus, and client needs:

- **Software Developer/Engineer:** Designing, creating, and maintaining software applications and solutions are within the purview of software developers and engineers. They use tools, frameworks, and programming languages to produce software that satisfies client needs.
- **Cybersecurity Analyst/Consultant:** Analysts and consultants who specialize in cyber security are essential in protecting client systems and data from threats and breaches. They identify security threats, create security plans, put security measures in place, and keep an eye out for security occurrences.
- **Data Scientist/Analyst:** Data scientists and analysts use machine learning and data analytics approaches to draw conclusions, address challenging business issues, and facilitate data-driven decision-making. They construct predictive models, conduct statistical analysis, and work with enormous datasets.
- **Cloud Architect/Engineer:** Designing, implementing, and managing cloud infrastructure and solutions is the responsibility of cloud architects and engineers. They collaborate with cloud computing platforms like Microsoft Azure, Amazon Web Services (AWS), or Google Cloud Platform to help clients take advantage of the scalability, flexibility, and cost-effectiveness that cloud computing offers.
- **Business Consultant/Analyst**: Business consultants and analysts collaborate closely with clients to comprehend their needs as it relates to their businesses, pinpoint opportunities for development, and create plans for organizational development and change. They carry out research, analyze data, and offer opinions and suggestions to improve client operations.
- **User Experience (UX)/User Interface (UI) Designer:** UX/UI designers concentrate on developing user experiences for digital goods and services that are simple to use and

visually appealing. To create user-centric designs, they carry out user research, create wireframes and prototypes, and work with multidisciplinary teams.

- **Project Manager:** Project managers oversee directing the creation, administration, and completion of client projects. They oversee project budgets and schedules, manage resource allocation, and make sure that project objectives are reached within predetermined limits.
- **Network Engineer/Administrator:** Designing, implementing, and maintaining computer networks and infrastructure is the responsibility of a network engineer or administrator. They set up network devices, fix network problems, and guarantee the performance, security, and dependability of the network.
- **Human Resources (HR) Consultants:** HR consultants offer tactical advice and strategic direction in such areas as hiring, retention, engagement, and organizational development. They collaborate closely with clients to create and carry out HR strategies that are in line with corporate objectives.
- **Financial Analyst/Consultant:** Financial analysts and consultants offer insights on financial performance, risk management, and investment strategies to assist customers in making well-informed financial decisions.

Chapter – 2

Project Description

2.1. Internship site Description

As a cybersecurity associate intern at Accenture, I have the chance to fully immerse myself in the dynamic and important topic of cybersecurity as an associate intern at Accenture. Throughout my internship, I've been working with seasoned experts who have been mentoring me as I build the abilities and knowledge necessary to safeguard client systems and data against threats. Threat analysis, incident response, security audits, and the use of security tools are just a few of the varied tasks that my internship entails. I am developing practical experience in threat analysis, security incident investigation, and assuring regulatory compliance. I also get the chance to support training and security awareness efforts, assisting in educating staff members on best practices to improve their cybersecurity awareness.

I've been exposed to a variety of cybersecurity duties and activities while being mentored by seasoned professionals. Every day brings a fresh challenge and a chance for improvement, from conducting vulnerability assessments to examining network traffic for potential threats. Modern cybersecurity tools and technologies are available at the internship location, giving me first-hand knowledge of how to use and deploy them. The emphasis on teamwork is one thing that really makes this internship stand out. As a result of my close collaboration with cross-functional teams, I have learned a lot about the multidisciplinary nature of cybersecurity. I have personally experienced the importance of cooperation in tackling difficult cybersecurity challenges, whether it be working with incident response teams or taking part in brainstorming sessions for designing security policy.

The learning possibilities go beyond routine duties. The internship location provides a wide range of workshops and training sessions led by professionals in the field. My grasp of cybersecurity frameworks, industry best practices, and new developments has grown because of these workshops. Accenture's culture of lifelong learning makes sure that interns like me have the knowledge and abilities necessary to succeed in the field of cybersecurity. This internship site distinguishes out for its sincere dedication to my professional development. I've been able to explore my hobbies, ask questions, and seek advice whenever I need it because of the encouraging and nurturing environment. The insightful criticism I get from my mentors keeps me motivated to advance and succeed in my position.

Overall, my internship with Accenture's cybersecurity division has been a remarkable experience all around. My enthusiasm for cybersecurity has only grown stronger as a result, and I now feel more confident about pursuing a career in this area. I am appreciative of the chance to work with a group that is leading the charge to safeguard digital assets and guarantee the future security of both businesses and people.

2.2. Problem Statement

This project report's main goal is to describe the issues and goals involved in creating an image steganography system. To enable secure communication and data protection, image steganography involves concealing important information within digital images. The approaches that are currently being used in this field, however, have several issues that limit their usefulness and efficacy. As a result, the project's problem statement intends to overcome these issues and create a sophisticated image steganography method.

The issue at hand is the necessity for a cutting-edge and effective image steganography algorithm that gets over the drawbacks of current techniques. These restrictions include restricted capacity, sensitivity to detection, and image quality degradation. Current steganography methods frequently have a limited payload capacity, making it challenging to conceal a sizable quantity of data within an image. The security of hidden information may also be jeopardised by statistical analysis attacks, which are also susceptible to them. Data embedding methods may also cause observable image distortions, raising suspicions and raising the possibility of detection.

The difficulty lies in creating a reliable image steganography method that increases data capacity greatly, guarantees data security, and preserves the image's aesthetic integrity. The overall quality and appearance of the image should be preserved while allowing for the smooth and undetectable embedding of data. Additionally, it should offer defense against unauthorized access and statistical analysis attacks, protecting the confidentiality and integrity of the hidden data.

2.3. Scope of Work Completed

Several important tasks that were part of this project have been successfully finished, which has helped the image steganography system. The following can be used to summarize the work that was completed:

- **Study and Analysis:**
    - Conducted a thorough literature review to determine the limitations of image steganography techniques and to grasp the state of the art in this field.
    - Examined the various approaches and algorithms used in the most popular image steganography systems.
    - Investigated various data-hiding and encryption strategies to increase the system's capacity and security.
- **Designing a system:**
    - Outlined the modules, components, and interconnections of the picture steganography system's general architecture.
    - The aims and challenges mentioned in the problem description were taken into consideration when defining the requirements and specifications for each module.
    - Created a thorough data model to make it easier to embed and extract hidden info from digital photographs.
- **Development of algorithms:**
    - Developed a cutting-edge data embedding technique that increases data capacity while reducing observable visual distortions.
    - Mechanisms for encryption have been used to guarantee the confidentiality and integrity of secret data.
    - Bit-plane decomposition and adaptive embedding techniques were used to increase the algorithm's efficacy and efficiency.
- **Implementation of the System:**
    - The frameworks and programming languages to put the designed algorithm and system into practice.
    - Included the modules and parts that had been built to produce an effective image steganography system.
    - Extensive testing and debugging to guarantee the system's accuracy and correct operation.
- **Analysis and Evaluation:**
    - Used a variety of test cases and datasets to thoroughly test and assess the image steganography system.

- Examined the system's functionality in terms of data storage, security, and image clarity.
- To evaluate the effectiveness and improvements made, the results were compared to those of previous methods and industry standards.

- **Reporting and documentation:**
  - Maintained thorough documentation throughout the duration of the project, which included design guidelines, implementation specifics, and testing protocols.
  - Created recurring progress reports to monitor the project's development and spot any alterations or improvements that were required.
  - Created a thorough project report outlining the accomplishments and contributions of the work done by combining the findings, conclusions, and analysis.

2.4. Purpose of the Summer Internship

The summer internship program's aim is to get worthwhile learning and professional development opportunities over the summer. The purpose of the internship is to close the knowledge gap between academic theory and practical application in the workplace. An internship during the summer serves the following purposes:

- **Learning and skill development:** The internship offers a setting for students to pick up knowledge and practical skills in their desired sector. Through practical experience, training sessions, and mentoring, it enables individuals to put their academic knowledge to use and advance their development.
- **Exposure to the Professional Work Environment:** Internships give students the opportunity to experience the Professional Work Environment. They can watch and pick up knowledge from seasoned pros, comprehend industry standards and practises, and hone crucial work abilities like collaboration and problem-solving.
- **Networking and Connections:** Interacting with professionals, managers, and co-workers during an internship gives you the chance to expand your professional network. During the internship, networking might lead to collaborations, referrals, and future job prospects.
- **Career exploration:** Internships give students the chance to investigate several career trajectories in their area of interest. They can receive knowledge about various

professions, markets, and workplaces, which will aid them in choosing their future job options.

- **Building a Resume:** An internship experience enhances a student's resume by exhibiting real-world knowledge and showcasing their dedication to professional development. It can help a candidate stand out to prospective employers and raise their prospects of landing job opportunities in the future.
- **Self-discovery and personal development:** Internships give students a chance to discover their strengths, interests, and opportunities for growth. Interns can improve their resilience, flexibility, and self-assurance by facing problems and receiving feedback.
- **Impact and Contribution:** Interns have the chance to participate in genuine projects and initiatives within the company. Their efforts may have an effect, which makes them feel satisfied and accomplished.

The summer internship programme promotes study, skill development, exposure to the working world, networking, and personal development. By bridging the gap between the academic and professional worlds, it plays a significant part in preparing me for the future jobs. My internship experience improves my resumes, broadens my professional networks, and supports wise career choices. I can improve their employability and build a solid basis for my professional career by embracing the chances and challenges provided by internships.

2.5. Reason for Choosing the company:

Based on several aspects and remarkable statistics, Accenture distinguishes up as a standout option for a cybersecurity internship. First off, Accenture has a solid reputation and a wealth of experience in the field of cybersecurity, making it a recognised global leader in technology consulting and services. With more than 537,000 workers worldwide, Accenture operates in more than 120 nations, giving interns access to a variety of cybersecurity projects in a range of sectors and industries. The corporation invests $900 million per year in training programmes, demonstrating its dedication to lifelong learning and professional growth. This commitment offers interns unrivalled learning opportunities, allowing them to improve their technical abilities and keep up with the most recent business trends.

Additionally, Accenture's diverse workforce, which includes 52% women and a multicultural mix of professionals, reflects the company's collaborative work culture. This welcoming setting encourages collaboration and offers interns a conducive environment for learning and development. Interns at Accenture can interact with important businesses and broaden their professional networks thanks to the company's large network of clients and partners, which includes 91 of the Fortune Global 100 firms. Overall, these figures demonstrate Accenture's leadership in the field, dedication to employee growth, diverse workplace, and great clientele, making it an excellent option for a cybersecurity internship.

2.6. Nature of Work Carried Out:

During my internship I had the chance to work closely with Microsoft Azure for increasing security measures at Accenture as a cybersecurity associate. To improve the organization's cybersecurity posture, different Azure services and features were used. Azure Active Directory (Azure AD), which serves as the basis for identity and access management, was one of the major topics I paid particular attention to. I received practical experience setting up and maintaining Azure AD, including role-based access control, multi-factor authentication, and user provisioning. I helped to improve user authentication and authorization procedures by utilising Azure AD, lowering the possibility of unauthorised access.

In addition, I focused on putting Azure Security Centre, a strong solution for managing security across Azure resources, into operation. To do this, security policies had to be configured, security assessments had to be made, and vulnerabilities or incorrect configurations had to be found. I actively identified and mitigated possible vulnerabilities by utilising the features of Azure Security Centre, which improved the organization's overall security posture.

I also investigated Microsoft's cloud-native Security Information and Event Management (SIEM) tool, Azure Sentinel. I got the chance to install and set up Azure Sentinel, as well as set up security playbooks, log ingestion, and data connectors. I helped to automate threat detection and response, streamline the organization's security operations, and get useful insights through advanced analytics and threat intelligence by using Azure Sentinel. To secure network traffic and safeguard resources, I also worked on integrating other Azure services, such as Azure Virtual Network (VNet) and Azure Firewall. This required setting up firewall rules, defining network security groups, and keeping an eye on network activities for security

breaches. I actively conducted research on and experimented with fresh Azure security features and updates during the internship. This gave me the chance to keep up with the most recent developments in Azure's security features and investigate how I could use them to improve cybersecurity procedures.

Overall, using Azure services and features to increase security measures was a good hands-on learning experience I had while working with Microsoft Azure for cybersecurity at Accenture. I helped improve the company's cybersecurity posture and gain useful skills in securing cloud environments by utilising Azure AD, Azure Security Centre, Azure Sentinel, and other Azure services.

Chapter – 3

Technology Details

3.1. Technology Details:

Information must now be transmitted securely and covertly more than ever in the world of digital communication. An efficient answer to this problem is image steganography, a method of concealing data within images. Utilising the right technologies that offer the required resilience and functionality is crucial for the development of an image steganography project. In this situation, a solid foundation for building an effective and secure image steganography system is provided by the combination of cryptographic principles, the adaptability of the Python programming language, and several modules designed for image processing and data manipulation.

3.1.1. Cryptography:

The fundamental idea behind safe communication in image steganography is cryptography. Understanding the security mechanisms used in the project requires knowledge of hashing methods, symmetric and asymmetric cryptography, encryption, and decryption. These ideas serve as the cornerstone for guaranteeing the privacy, accuracy, and integrity of hidden information in photographs.

- Understanding and using encryption methods are crucial for protecting the secret information included in the photos. For encrypting and decrypting the hidden data, the project may use symmetric encryption methods like AES (Advanced Encryption Standard) or asymmetric encryption techniques like RSA (Rivest-Shamir-Adleman).

- Cryptographic systems rely on key management to guarantee the privacy of the secret data. The task could involve creating, preserving, and managing encryption keys in a secure manner. To keep the hidden data private, proper key management procedures, including key generation, key exchange, and key storage, are necessary.

- By utilising both steganography and encryption methods, the security of the concealed information is improved. To add an additional degree of protection, the project may investigate strategies for encrypting the message before embedding it within the image. This makes sure that the secret information is encrypted and inaccessible without the decryption key even if the image is intercepted.

- Digital signatures offer a way to confirm the integrity and veracity of the concealed data. The project can be sure that the secret message hasn't been tampered with or changed during transmission or storage by implementing digital signatures. Understanding cryptographic hash functions and asymmetric encryption methods is necessary for putting digital signatures into practise.

- Cryptographic hash functions are crucial for ensuring the accuracy of the concealed data. The project might produce distinctive hash values for the hidden information using hash methods like SHA-256 (Secure Hash Algorithm 256-bit). You can compare these hash values to ensure that the extracted hidden data is accurate.

- To provide a secure communication channel between the transmitter and recipient of the secret information, secure key exchange systems are essential. To safely exchange encryption keys without the chance of interception or eavesdropping, the project may investigate key exchange protocols like Diffie-Hellman key exchange.

- The project's implementation of encryption and decryption procedures can be made simpler by utilising cryptography tools and APIs. Python has libraries like hashlib and cryptography that give functions and methods for performing cryptographic operations. To guarantee the privacy, accuracy, and integrity of the hidden data, use these libraries.

3.1.1.1. Suitability to the Project:

The project involving image steganography makes excellent use of and benefits from the use of cryptography. The research attempts to improve the security and secrecy of the concealed data included in the photographs by applying cryptographic techniques. To make the hidden data secure, encryption methods transform it into an unintelligible format. As a result, the sensitive information is more protected and is more difficult for unauthorised parties to access or comprehend. Only parties with the proper authorization have access to the keys needed to decrypt the encrypted data, thanks to good key management procedures. The project also considers using digital signatures to confirm the legitimacy and integrity of the concealed information, giving confidence that the data was not altered during transmission or storage. The project's use of cryptography strengthens the system's overall resiliency, maintaining data secrecy, and guaranteeing the security of the concealed information.

3.1.2. Python:

Image steganography projects are well suited for Python, a well-liked and adaptable computer language. It is the best option because of its clarity, readability, and robust library ecosystem. Python has a large selection of internal and external modules that make it easier to analyse images, perform cryptographic operations, and manipulate data.

- Large library ecosystem: Python offers a wide selection of libraries and modules made expressly for data manipulation, image processing, and cryptography. Many different functions and tools are available for loading, processing, and analysing images in these libraries, including Pillow, OpenCV, and scikit-image. These activities, which are necessary for image steganography procedures, such as extracting pixel values, resizing images, and applying filters, are made simpler.

- Simplified Syntax and Readability: Python's code is simpler to comprehend and maintain because of its clear, readable syntax. When using sophisticated image steganography methods, this quality is especially beneficial. Python's syntax is straightforward, which lowers the possibility of mistakes and increases overall development effectiveness.

- Python is a cross-platform language, which means that code created on one operating system can be executed on many systems without requiring major changes. Regardless of the operating system being used, the project can be readily deployed and run on a variety of platforms because to its adaptability.

- The ability to manipulate individual bits within the binary representations of images is made possible by Python's built-in bitwise operators and bit shifting features. A key component of image steganography, these features make it possible to perform precise bit-level operations for hiding and extracting data from certain image channels or pixels.
- Python provides a variety of encoding and decoding techniques that are essential for image steganography. Binary data can be transformed into ASCII characters using encoding systems like Base64, which makes it possible to transform message data into

a format that can be embedded into image pixels. Like encoding techniques, decoding schemes make it easier to extract secret information from encoded visual data.

- Supportive Community: Python has a sizable and vibrant development community, which translates to a wealth of online seminars, documentation, and tools. It is simpler to overcome obstacles and get help during the development process thanks to this community support. Additionally, it makes it possible for the project to benefit from the expertise and experience of other Python programmers working on related projects.

3.1.1.2. Suitability to Project

Python's versatility and conformance to the project's specifications make it an excellent choice for the image steganography project. Python is the ideal choice for the project's requirements since it provides a wide variety of features and packages that are especially suited for image processing, cryptography, and data manipulation. Python's clear and intelligible syntax improves code comprehension and maintainability, which makes it simpler to construct the intricate algorithms needed for image steganography. Python's simplicity lowers the possibility of mistakes and boosts development effectiveness. Additionally, Python's cross-platform interoperability makes it possible to deploy and run the project without any issues on a variety of operating systems. A key component of image steganography is the precise manipulation of individual bits within the binary representations of images, which Python's bit manipulation capabilities make possible. The project's capacity to conceal and extract information from the image data is further improved by the support for data encoding and decoding. Finally, Python's active community offers a wealth of online seminars, documentation, and other tools that are invaluable for assistance and direction during the development process. Overall, Python is the ideal choice for implementing the image steganography project because to its adaptability, simplicity, cross-platform interoperability, and supportive community.

3.1.3. Powerful image processing modules:

There are powerful image processing modules are available in Python, including Pillow, OpenCV, and scikit-image. The utilities for loading, modifying, and analysing photos are provided by these modules. They make it possible to do critical image steganography activities such extracting pixel values, scaling images, using filters, and changing the image data without the human eye noticing the changes.

- Pillow is a robust image processing toolkit that offers a wide range of features for importing, modifying, and storing images in different formats. It enables image scaling, cropping, rotation, and filtering—operations crucial to the image steganography endeavour.

- OpenCV (Open-Source Computer Vision Library) is a popular library for image processing and other computer vision-related applications. It provides a variety of image editing features, including thresholding, morphological operations, and image enhancing methods. Before using steganography techniques, the photos can be pre-processed using OpenCV.

- NumPy (Numerical Python) is a crucial package for Python-based scientific computing. It offers a multidimensional array object that is useful for manipulating and storing the values of picture pixels. Accessing image regions, changing pixel values, and running mathematical operations on images are all made possible by NumPy.

- Scikit-Image is a library for image processing that provides a full range of tools and algorithms for a variety of image modification applications. It offers tools for geometric manipulations, image segmentation, and feature extraction. These features can be used in the project for advanced processes including image steganography.

- During the planning and testing stages of the project, Matplotlib is a plotting package that is helpful for visualising and analysing images. To better comprehend the steganography techniques used, it enables the development of histograms, heatmaps, and other visual representations of the image data.

3.1.1.3. Suitability to Project:

Because of their reliable functioning and suitability for the project's requirements, the image processing modules are excellent choices for the picture steganography project. These modules are crucial for implementing many facets of image steganography since they include a comprehensive range of tools and algorithms created especially for image modification and analysis. These modules offer a comprehensive variety of features that may be smoothly incorporated into the steganography algorithms, ranging from fundamental actions like loading

and storing images to more complicated ones like resizing, cropping, filtering, and modifying images. Additionally, the project's flexibility in handling a variety of image kinds is ensured by its compatibility with many image formats. Furthermore, these modules' excellent documentation and community assistance make it simpler to understand and make use of their functionality. In general, the image processing modules chosen for the project are excellent choices since they offer the tools and capabilities needed to carry out the essential picture modifications and analysis for the proper implementation of the image steganography techniques.

3.1.4. Cryptography Libraries:

Python includes cryptography libraries like hashlib and cryptography that provide a variety of cryptographic methods and algorithms. Digital signatures, hashing, symmetric and asymmetric encryption, and key management are all supported by these libraries. By utilising these libraries, secure encryption and decryption processes that are necessary for concealing and removing information from the images can be implemented. Bit Manipulation: Bit manipulation is essential to image steganography because it makes it possible to conceal and retrieve data at the bit level. The precision with which bits can be moved and manipulated inside binary representations of images is made possible by the built-in bitwise operators and bit shifting capabilities of Python. For embedding and extracting hidden data from certain image channels or pixels, this functionality is essential.

- Cryptography is a strong library that offers several cryptographic functions. It provides hash operations, message authentication codes (MAC), symmetric and asymmetric encryption techniques, and key elicitation procedures. The project may implement encryption and decryption operations, create safe cryptographic keys, and guarantee data integrity and authentication thanks to this library.

- PyCryptodome is a vast repository of cryptography protocols and methods. It supports several encryption techniques, including elliptic curve cryptography (ECC), DES, RSA, and AES. Data encryption and decryption features, secure random number generation, and digital signature implementation are all provided by PyCryptodome. It also contains tools for managing keys and generating keys.

- Cryptographic hash functions are offered by the hashlib library, which also includes well-known algorithms like SHA-256 and MD5. The generation of hash values that

uniquely identify data and guarantee its integrity depends on these hash functions. The project can calculate hash values for the hidden data and check their accuracy during the extraction process thanks to the hashlib package.

- AES (Advanced Encryption Standard) encryption is supported by the Python package payes. It offers an easy-to-use interface for AES-based data encryption and decryption. This library is appropriate for situations where efficiency and simplicity are crucial because it is compact and simple to include into the project.

- Symmetric encryption is the focus of the cryptography. Fernet module, which is a component of the Cryptography library. It provides a high-level interface for applying the message authentication and symmetric encryption Fernet encryption method. This module makes the encryption and decryption process simpler, making it appropriate for situations where security and simplicity are top priorities.

3.1.1.4. Suitability to Project:

The chosen cryptographic libraries are excellent choices for the picture steganography project because of their reliable functionality and conformance to project specifications. These libraries include a complete selection of cryptographic protocols and algorithms that enable secure hashing, encryption, and digital signatures. They provide a wide range of functions and techniques for carrying out different cryptographic operations, guaranteeing the privacy, integrity, and reliability of the concealed data in the steganography project.

For instance, the Cryptography library offers comprehensive support for hash functions, key derivation functions, and both symmetric and asymmetric encryption methods. To implement encryption and decryption operations, create secure cryptographic keys, assure data integrity, and perform authentication, it provides a versatile and potent interface. The project can because several encryption techniques are readily available.

3.1.5. Data Encoding:

Data encoding is a crucial component of picture steganography because it makes it easier to convert binary data into a format that can be embedded inside the pixels of an image. Python has several encoding techniques, including Base64, which transforms binary data into ASCII letters. The compatibility and seamless integration of hidden messages inside the visual data are ensured by these encoding techniques.

- Binary Encoding: A key method in image steganography for representing data as a series of binary digits (bits) is binary encoding. It entails transforming the data into binary form, where each bit is represented by a 0 or 1. The project may interact directly with the discrete pieces of the hidden data thanks to binary encoding, which facilitates their embedding into the image pixels.

- Base64 encoding is frequently used to convert binary data into a format that can be sent over the internet or kept securely. It transforms binary data into text using only a small number of letters (the '+/' symbol, A-Z, a-z, and 0–9). When it's required to represent the concealed data in the project as text, like when storing or sending the steganographic image, Base64 encoding comes in handy.

- Huffman Encoding: Based on the frequency of occurrence of certain symbols, Huffman encoding assigns variable-length codes to those symbols. Before encoding the concealed data into the image, it is appropriate to compress the data first. By reducing the quantity of the data, Huffman encoding enables more effective storage inside the constrained pixels of the image.

- Characters from many writing systems and languages are represented using the Unicode encoding. When steganographic images contain text-based data, it is especially helpful. The project can handle multilingual or special characters within the hidden data because Unicode encoding assures compatibility and accurate representation of varied characters.

3.1.1.5. Stability to Project:

The data encoding methods selected are appropriate for the image steganography project because they offer efficient ways to represent and securely store the concealed information. By allowing for the direct manipulation of individual bits, binary encoding facilitates the embedding process within the image pixels and allows for seamless integration. When working with text-based systems, base64 encoding assures compatibility and secure transmission or storage of the steganographic image. By compressing the data, Huffman encoding makes the most of available storage space while retaining data integrity. Multilingual and special characters are supported by Unicode encoding, guaranteeing proper representation of textual

information in the concealed data. Together, these data encoding methods improve the project's capacity for information retrieval and concealment within steganographic images.

3.1.6. File Handling and I/O:

Image steganography depends on the ability of Python's file handling features to read and write image files as well as other types of data files. The built-in file input/output (I/O) capabilities and image processing modules give file handling workflows the tools they need to easily include image steganography techniques.

- Reading and Writing Image Files: For this project, input photos are read and steganographic images with embedded data are written. The efficient reading and writing of picture files in a variety of formats, such as JPEG, PNG, or BMP, is made possible through file management. Python comes with several libraries, such Pillow or OpenCV, that support manipulating image files and offer functions to read and write images without any issues.

- Operations on Binary Files: In steganography, the concealed data is frequently represented in binary format. File handling makes it easier to read and write binary files, ensuring that the secret information is accurately retrieved and stored. The built-in file handling features of Python, such as opening files in binary mode and employing the proper file read/write methods, enable productive operations on binary files.

- Handling metadata: Metadata, which includes details about the image such its size, resolution, or colour space, is frequently present in image files. During the steganography process, the project may demand the preservation or modification of metadata. To maintain the integrity and consistency of the picture file attributes, file handling makes it possible to extract and modify information.

- Handling faults and exceptions that could arise during file handling and I/O operations, such as file not found errors or permission problems, is essential. Python offers strong error handling features, such try-except blocks, to catch and properly handle such occurrences. The smooth execution of file operations and increased project reliability are both guaranteed by proper error management.

- File Compression: To optimise storage space or minimise the size of the steganographic images, file compression techniques may be used, depending on the project requirements. As part of the steganography process, file handling permits the reading and writing of compressed files, enabling effective compression and decompression operations.

3.1.1.6. Suitability to Project:

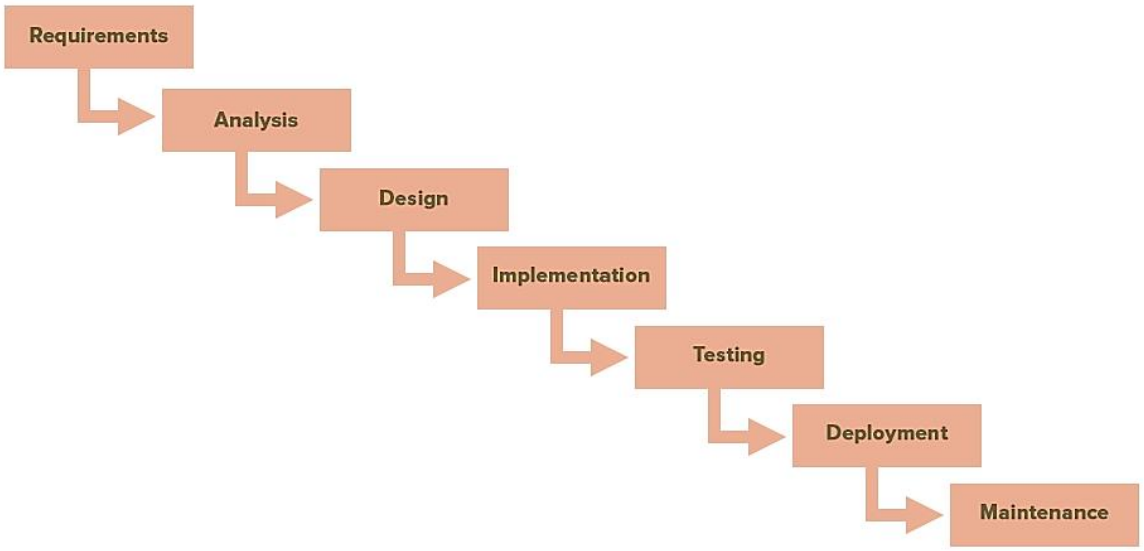
For the picture steganography project, file handling and I/O operations are crucial since they offer the functionality required to read, write, and manipulate data effectively. To access and alter image files, the project depends on file handling, which enables the seamless integration of hidden data. Through libraries like Pillow or OpenCV, Python's rich image file manipulation support guarantees compatibility with various image formats and makes reading and writing operations simple. Furthermore, Python's file handling features enable exact processing of binary files, ensuring the accurate recovery and archiving of the secret data. Python offers a reliable environment for managing binary file operations thanks to its support for opening files in binary mode and its usage of appropriate read and write techniques. Additionally, file handling is necessary for working with picture file metadata, allowing for the extraction, alteration, and retention of important data. To ensure the dependability and stability of file operations throughout the project, proper error handling and exception management must be used. In general, file handling and I/O activities are well suited for the project of picture steganography because they enable the smooth manipulation of image files, binary data, and metadata, facilitating the effective application of the steganography techniques used.

Chapter – 4

Project Methodology

4.1. Methodology:

To ensure a methodical and organized process, the development of Image Stenography will adhere to a planned project methodology. The Agile technique, specifically Scrum, was selected for this project because it encourages iterative development, collaboration, and adaptation to changing requirements. The project will be broken up into several sprints, each lasting a particular amount of time and producing a set of deliverables. Stakeholders will be consulted on a regular basis in meetings and feedback sessions to assess progress, make necessary changes, and guarantee project goals are being met.



4.1. Project Methodology

- **Requirements Gathering:** During this stage, precise needs for the picture steganography project were gathered and thoroughly analysed. Discussions with stakeholders were necessary to determine the intended functionality, including support for multiple picture formats, the ability to conceal text or other sorts of data within photos, and the necessary level of security. The project's limitations, including those related to performance standards and system compatibility, were also considered. The

thorough requirement gathering procedure made sure that the project's goals were clearly stated and in line with what the stakeholders expected.

- **Research and planning:** A thorough investigation into several steganography techniques and algorithms appropriate for the project was conducted. This required researching several techniques, such as LSB (Least Significant Bit) steganography, which modifies the image's least significant bits to incorporate the secret information. To speed up development, study was also done on already-existing frameworks, libraries, and open-source implementations. The project timeframe, funding allocation, and identification of the requisite tools and technologies for development—such as the Python programming language and pertinent libraries like Pillow for image processing—were all part of the planning phase.

- **Design and Architecture:** The overall system architecture and component interactions were defined during the design and architecture phase. The data encoding, picture processing, cryptography, and user interface modules were all included in the structure of the image steganography project. Scalability, adaptability, and modularity were all guaranteed by the architectural plan. To enable seamless integration and effective processing, the data flow between modules was carefully organised. To safeguard the hidden data, security considerations including encryption methods and key management were also built into the architecture.

- **Implementation:** The implementation stage entailed turning the architecture and design concepts into working code. Python's extensive library system and user-friendliness led to its selection as the top programming language. The developed steganography methods, such LSB steganography, allowed for the concealment and retrieval of data within of images. To perform image alteration tasks like pixel-level operations and colour space conversions, image processing techniques were used. The integration of cryptographic methods enables secure data encryption and decryption. To assure the quality and maintainability of the software, thorough code reviews and adherence to coding standards were also part of the implementation phase.

- **Testing and Quality Control:** The picture steganography project's performance, functionality, and security were all thoroughly tested. To verify the various modules'

functionality, unit testing was done. To ensure flawless interaction between the project's many components, integration testing was done. During user acceptability testing, the project was checked against the predetermined requirements while user feedback was gathered to optimise the system. To find and fix any potential security flaws, security testing such as penetration testing and vulnerability assessments was also carried out.

- **Documentation:** Throughout the process, documentation was essential. To record the project requirements, design choices, implementation specifics, and user instructions, extensive documentation was produced. This documentation helped with future maintenance, knowledge transfer, and troubleshooting by ensuring that the project was thoroughly documented. It also functioned as a reference for programmers and users, giving them a clear grasp of the functionality and application of the project.

- **Deployment and Evaluation:** The final stage involved setting up the picture steganography project in the required setting and checking that it was compatible with the target platforms. In comparison to the established objectives and success criteria, the project's efficacy and performance were assessed. To do this, it was necessary to measure the precision of data hiding and retrieval, evaluate the effectiveness and speed of the applied algorithms, and solicit user input to assess the entire user experience. Based on the evaluation's findings, any adjustments or improvements that were required to guarantee the project's ideal performance and usability were made.

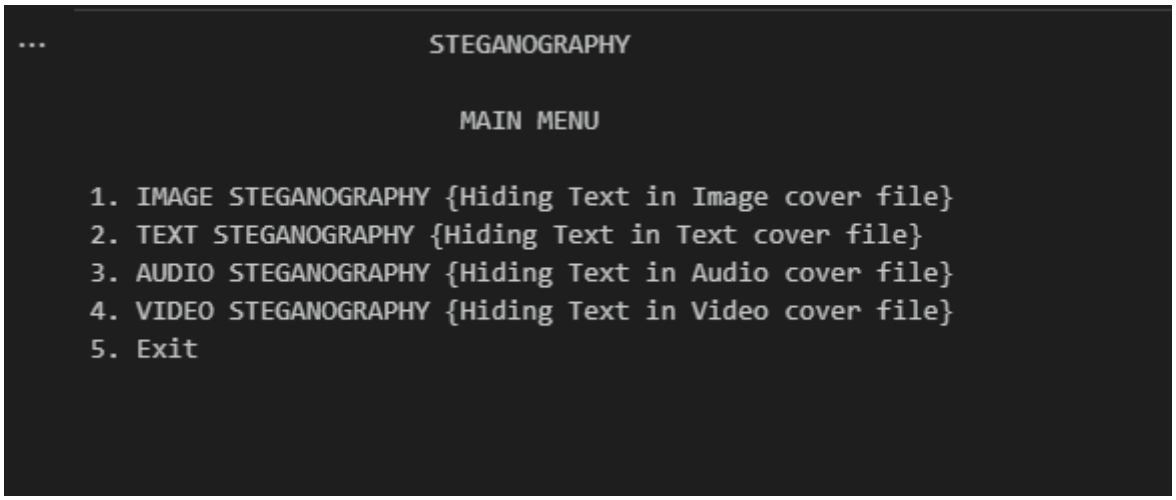


Fig4.2 Menu Page

4.2. Project Flow:

To effectively hide and retrieve data from images, the project flow combines image processing, data encoding, steganography methods, and data extraction approaches. Python is a great choice for implementing the necessary functionalities because of its large library, ability to work with picture pixels, and capacity to execute numerous data operations. The project strives to achieve a balance between data security, image quality, and user friendliness.

- **Input Image Selection:** The project is compatible with several image formats, including JPEG, PNG, and BMP. The selected image acts as the cover image or carrier image for the data that will be concealed within it.

- **Data Encoding:** The project encrypts user data before it is ready to be embedded in a picture. This may require encoding the data using encoding techniques like ASCII or Unicode and converting it to binary form. You can use compression algorithms to shrink the size of the data while maintaining its integrity, like Huffman coding or Run-Length Encoding. Additionally, Reed-Solomon encoding, and other error-correction strategies may be used to improve the hidden data's dependability.
- **Image processing:** To alter the pixels of an input image while keeping its aesthetic integrity, image processing techniques are used. To access and modify individual pixels, the project makes use of Python's image processing tools, such as Pillow or OpenCV. Common actions to make sure the hidden data is seamlessly included into the image include altering brightness, contrast, or colour levels. Depending on the steganography method selected, spatial domain techniques like pixel intensity manipulation or frequency domain techniques like Discrete Cosine Transform (DCT) may be used.
- **Data Embedding:** To embed the encoded data within the altered image pixels, the project uses a selected steganography algorithm, such as LSB (Least Significant Bit) steganography. The least significant bits of the pixel values are swapped out for the secret data bits in LSB steganography. To boost the data hiding capacity or improve the security of the concealed information, further cutting-edge techniques like bit-plane complexity segmentation or high-capacity steganography algorithms may also be used. The initiative makes sure that the changes are undetectable to the human eye, preserving the image's visual quality and integrity.

- **Output Image Generation:** To create a steganographic output image, the project modifies an image and saves it with concealed data. To maintain compatibility, the output image is often saved in the same format as the original image. Additional choices for modifying the output image attributes, such as resolution, compression ratio, or metadata preservation, may be made available by the project. The objective is to create a visually unrecognizably image while successfully hiding the underlying information.
- **Data Extraction:** The project uses the reverse method to extract the concealed data from the steganographic image. The modified image pixels are examined once more using the steganography process to separate the contained data bits. To correctly detect the updated pixel values and retrieve the proper bit sequence, much care is taken. Any lost or corrupted data that was extracted may be recovered using error correcting procedures.
- **Data decoding:** To return the extracted data to its original format, it must first be decoded. Based on the encoding scheme employed during the data embedding phase, the project applies the necessary decoding procedures. This can entail using decryption techniques if encryption was used to increase data security, reversing compression algorithms, or transforming binary data back to its original form. The project minimises any potential information loss or distortion by ensuring the correctness and integrity of the extracted data.
- **Output Presentation:** The presentation's structure is determined by the hidden content's type. For instance, if the hidden data is text, it can be saved as a text file or displayed on the user interface. If the secret information is a picture or a file, it can be preserved in that format and used later. Users will be able to access and utilise the retrieved data effectively because to the project's seamless and easy user experience.

4.3. Project Details:

Images are being shared and received on networks more frequently these days. The network's security is a key problem because more and more information is being exchanged daily. As a result, protecting against unauthorised access and use requires both data masking and data permission. This is the primary reason why the field of data concealment has expanded. Data hiding is the practise of concealing information so that no one outside the intended recipient and the source of the data may access it. It conceals information, including text, audio, video, and image files. The data is concealed in the image using a method known as steganography.

The image itself may contain the data that is concealed in it. Data that is hidden should be retrievable. Volatile data concealing is a characteristic that was initially used for authentication and is crucial because it conceals secret data in a digital image in a way that only an authorised individual can decrypt and backup the original image.

Numerous data-hiding techniques have been developed. A volatile data contained algorithm's payload size, complexity, visual quality, and security all affect how well it performs.

4.3.1 Approach/Solution:

The original image is encrypted using the stream cypher, often known as symmetric key encryption, making the image impenetrable. Every key is used to encrypt every piece of data. For data concealing and image encryption, two distinct keys are used: encryption key and data hiding key. To keep the data private, Data Hider constricts of chosen bits gathering from the encrypted image. Using a distributed source decoder, the receiver uses an encryption key to decrypt the sensitive data and obtain the original image. The desired outcome was obtained without any data or image loss. As a result, our approach increases the security of the encrypted data and the image in which the data is disguised. The decryption key for the information and image, followed by the key for extracting the data from the image, should all be in the possession of the recipient.

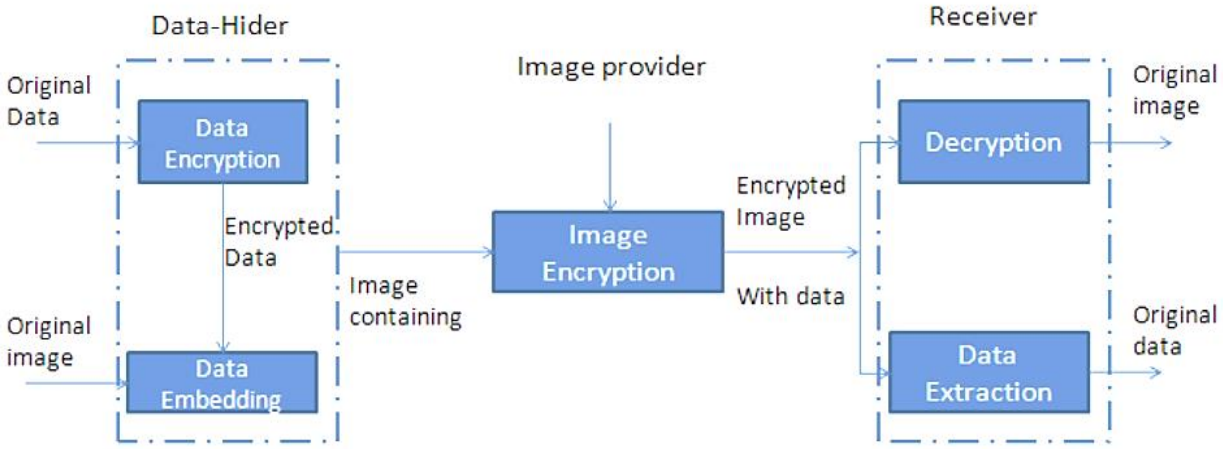


Fig 4.3 Architecture diagram of proposed system

Phase of embedding:

- First, remove every pixel from the provided image and place it in an array called "imagearray."

- Step 2: Extract all the characters from the message file and place them in the messagearray array.

- Is obtaining the characters from the Stego key and placing them in a Keyarray array. To prevent the embedded data from being discovered or recovered, the hiding process is controlled by a stego-key.

- Insert the first pixel and the characters from the Key- array into the pixel's first component. Place the remaining characters in the first component of the following pixels if the Key array has additional characters.

- Insert a terminating sign to denote the key's end. In this procedure, the terminal symbol is set to 0.
- Replace each component of the following pixel with a character from the message array.
- Repetition of step 6 is required to embed all characters.
- Reposition a terminating symbol to signify the end of the data.
- The obtained image will conceal every character entered.

The most straightforward steganography methods deterministically embed the message bits into the cover image's least significant bit plane. Because the amplitude of the shift is modest, modulating the least significant bit does not produce a difference that is noticeable to humans. A suitable cover image is required to conceal a secret message inside of an image. A lossless compression format must be used because this method uses bits from each pixel in the image; otherwise, the concealed information will be lost during the transformations of a lossy compression algorithm. A bit of each of the red, green, and blue colour components can be used in a 24-bit colour image, allowing for a total of 3 bits to be recorded in each pixel. As an illustration, the grid below, which uses 9 bytes of RAM, can be thought of as 3 pixels of a 24-bit colour image:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

The following grid is created when the character A, whose binary value is 10000001, is inputted.

Results:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this instance, the character might be correctly inserted by changing just three bits. When selecting the maximum cover size, only half of the bits in an image will typically need to be changed to conceal a hidden message. The information is effectively concealed because the least significant bit changes that are created as a result are too minute for the human visual system (HVS) to pick up on. As you can see, the smallest portion of the third colour has remained unchanged. It can be used to verify if the 8 bits that are embedded in these 3 pixels are valid. It might therefore serve as a parity bit.

4.4. Flow Diagram:

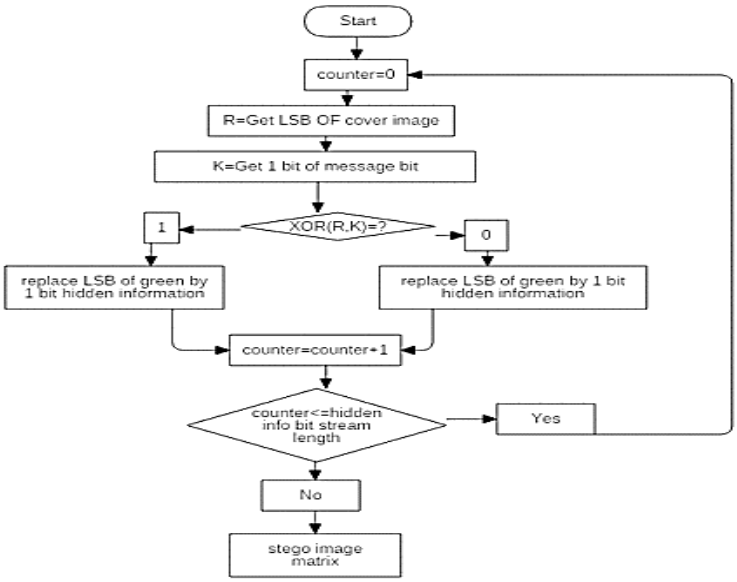


Fig 4.4 Encryption Flow Diagram

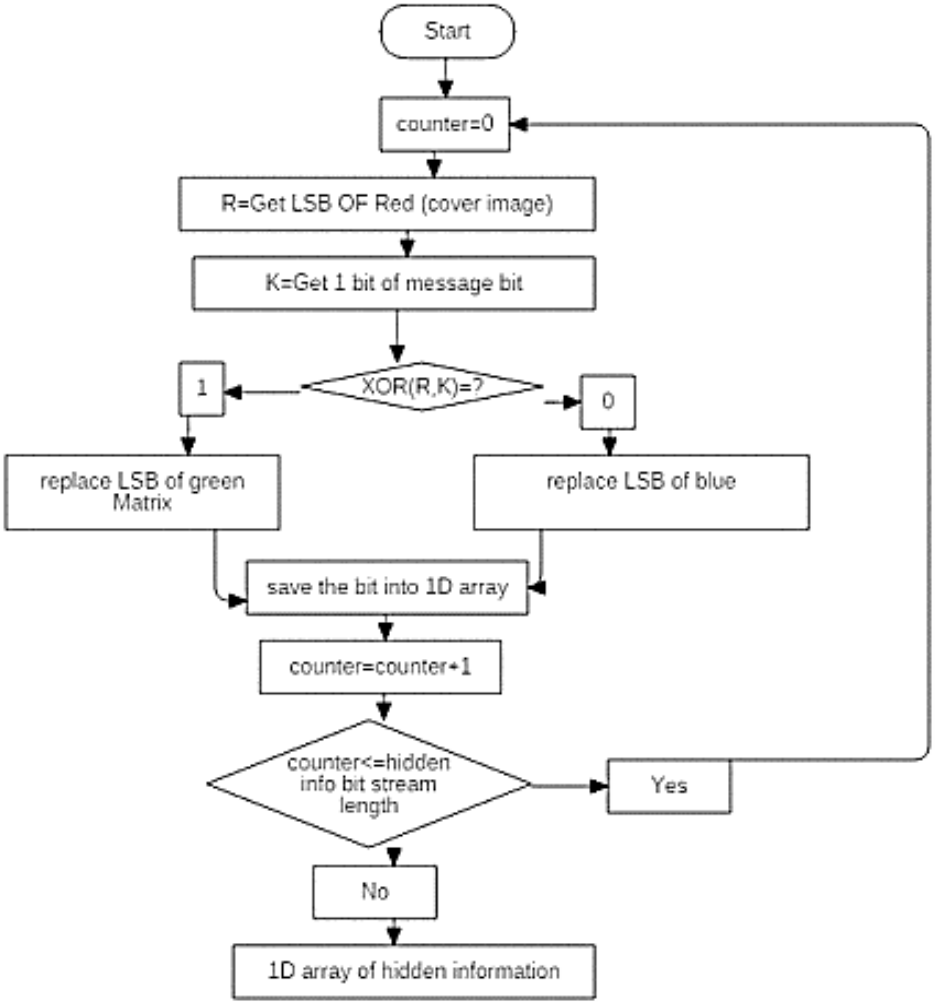


Fig 4.5 Decryption Flow Diagram

4.5. System Design:

4.5.1 Use Case Diagram:

At its most basic level, a use case diagram depicts how a user interacts with the system. User creates secret text first, then chooses a cover image with data hidden inside, and then sends stego image to recipient through image. The stego image is chosen by the user at the receiver side, who then decrypts the chosen stego picture. After that, he can access text that is buried within text.

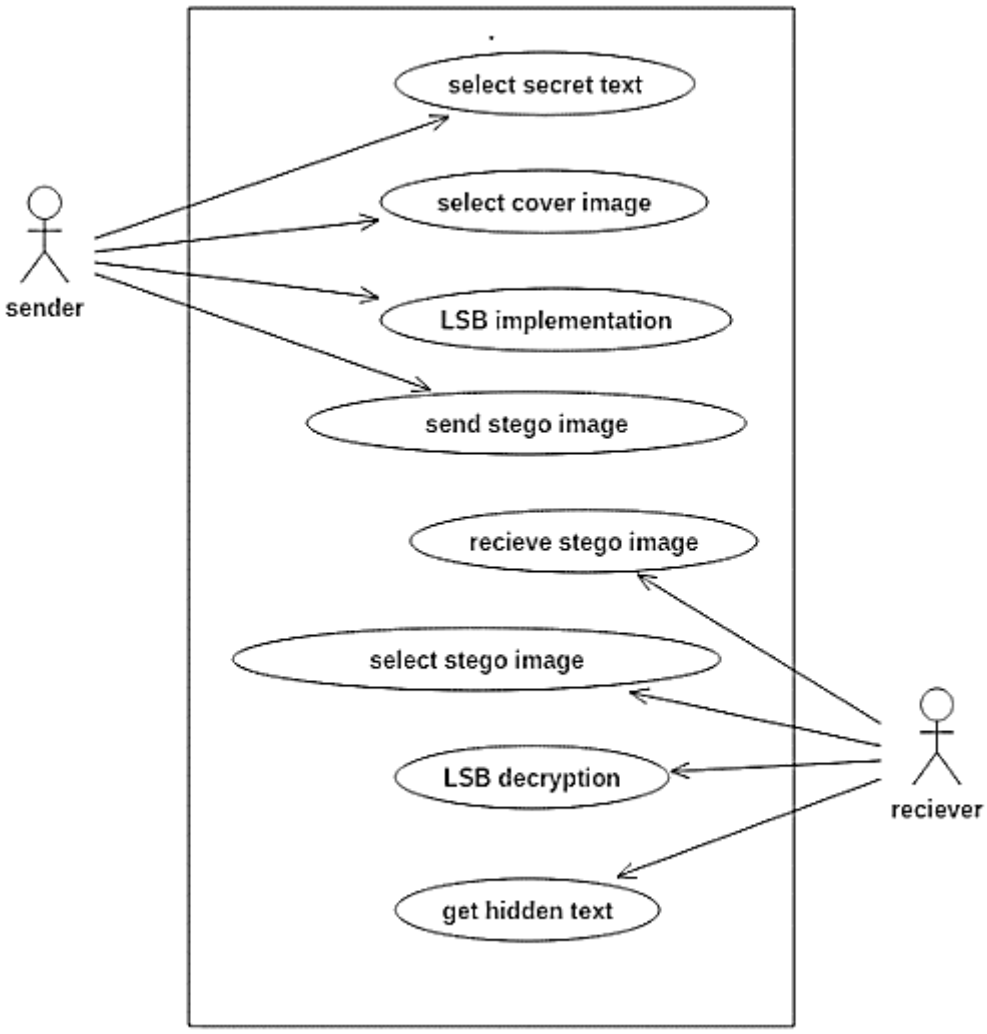


Fig 4.6 Use Case Diagram

4.5.2: Activity Diagram:

The STEGO programme must be opened to begin any activity. The Stego software requests usernames and passwords for authentication. If the user is authenticated by Stego software, the username and password are correct. The user is presented with four alternatives as Create a stego image, first. Obtain the secret code. 3. Post an image About 5. Please.

- A stego image can be created by the user and include secret data.
- By decoding an image, a user can discover his secret code.
- The transmit image option on Stego allows users to share images to other users.
- By selecting the "about" option, users can learn more about software.
- If the user needs assistance, he can look for it.
- By selecting log out, the user can end the Stego software.

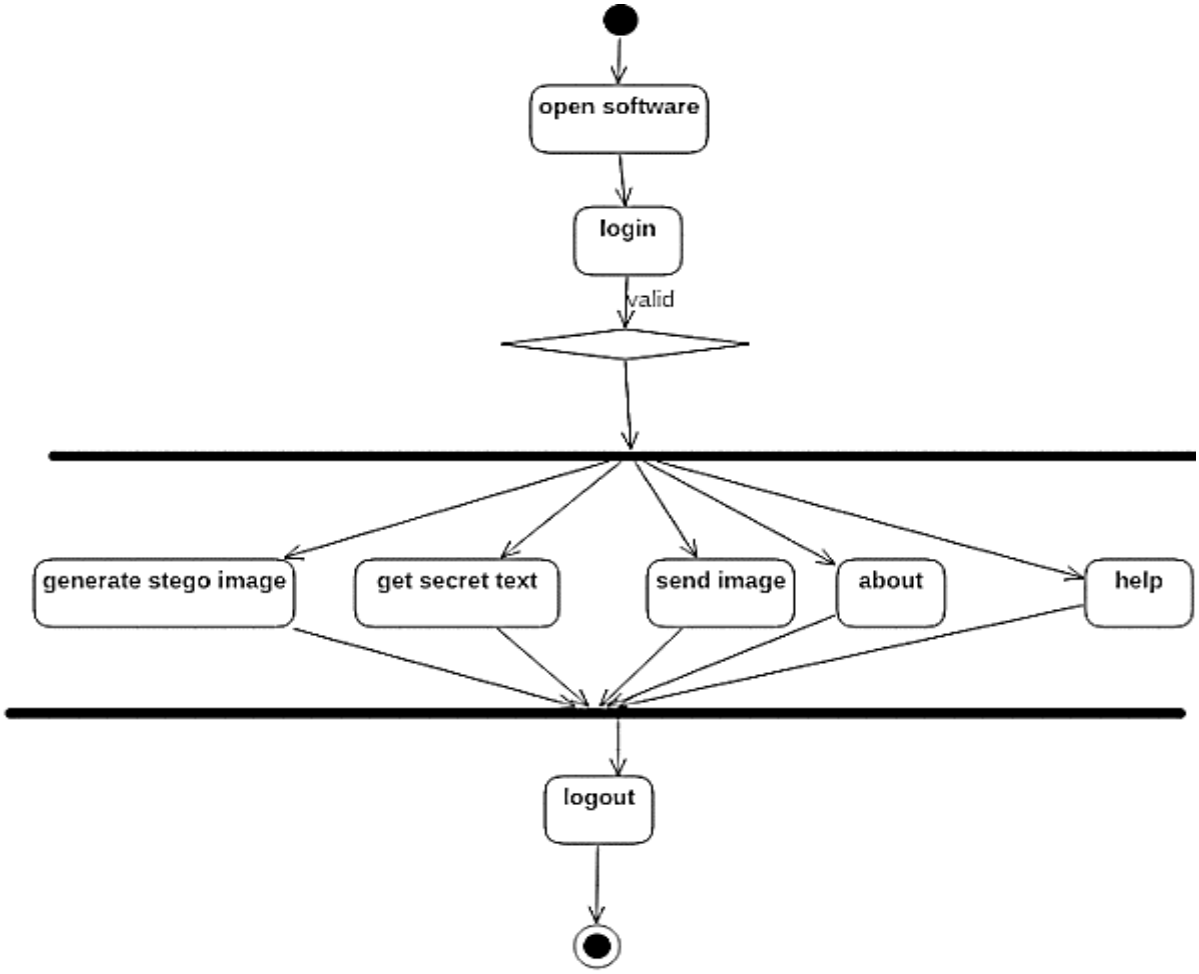


Fig4.7 Activity Diagram

4.5.3. Data Flow Diagram:

4.5.3.1. DFD Level 0:

The steganography system generates a stego image using inputs like a cover image and a secret text message.

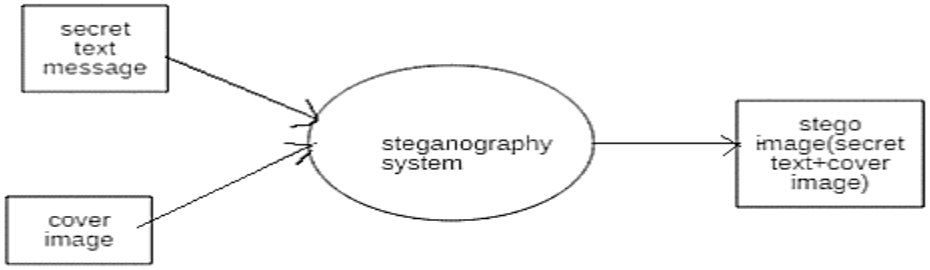


Fig4.8 DFD Level 0

4.5.3.2. DFD Level 1:

The primary function of DFD Level 1 is the addition of a secret text message to a picture by changing a few bits, which is then delivered through email to the recipient side.

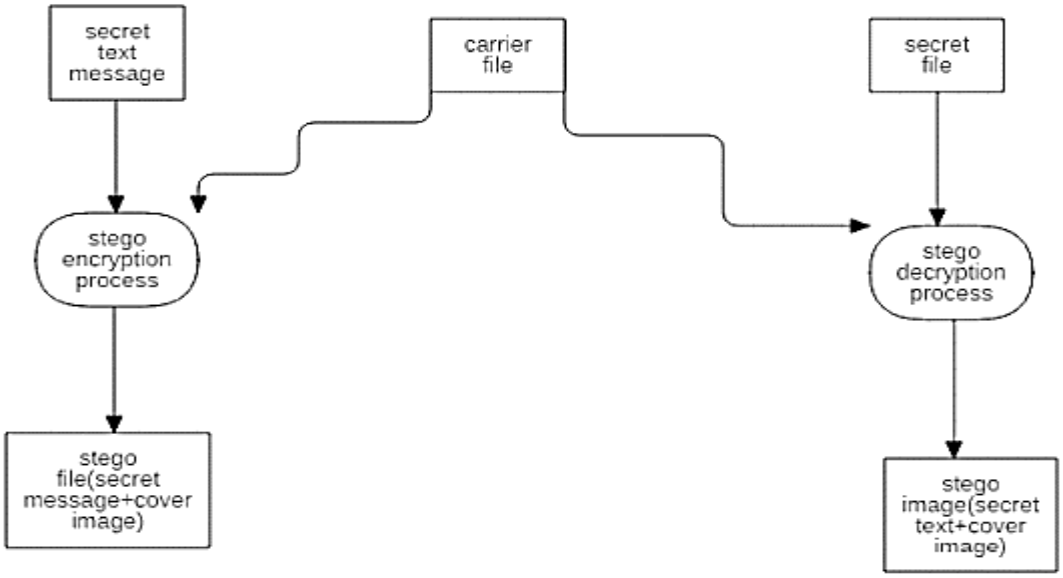


Fig4.9 DFD Level 1

3.5.3.3. DFD Level 2:

Least Significant Bits (LSB), in which the least significant bits are altered and a stego file is formed, are used to add secret text to a picture. to obtain a secret message by decrypting an image.

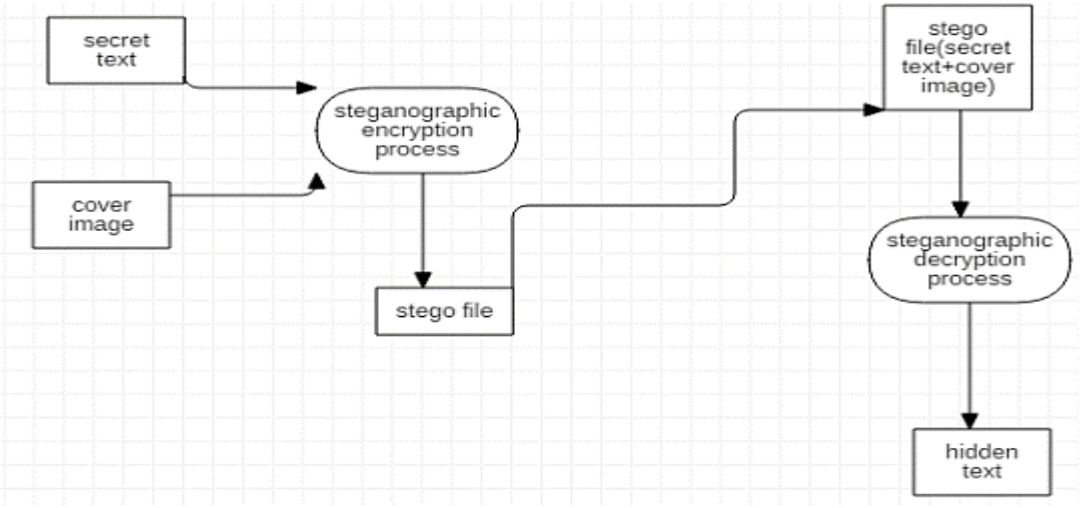


Fig4.10 DFD Level 2

Chapter – 5

Project Challenges and Benefits

5.1. Project Challenges/Solutions:

To design a reliable and effective system for secure data concealing within digital photographs, the image steganography project required overcoming several obstacles. To ensure the best performance, security, and user experience, several factors were carefully reviewed and handled throughout the project. The following bullet points outline the main issues that were encountered throughout the project and the solutions that were put in place to address them.

- **Data Capacity and Image Quality:**
    - **Challenge:** Finding a balance between the quantity of data that can be concealed inside an image and the maintenance of image quality was one of the key challenges. The image may become degraded or exhibit obvious artefacts as the hiding capability is increased. To provide maximum data capacity while keeping acceptable image quality, relevant steganography algorithms and image processing methods were carefully chosen.
    - **Solution:** putting into practise sophisticated steganography techniques that maximise data capacity while reducing visual artefacts. To balance hiding capacity and image quality, approaches like adaptive embedding, spatial domain methods, or frequency domain methods are used. To guarantee the flawless integration of the concealed data while maintaining the overall visual quality of the image, image processing methods are also used.

- **Robustness against Attacks:**
    - **Challenge:** The project attempted to strengthen the steganographic system's resistance to possible assaults or attempts to uncover the concealed data. Using adversarial methods like statistical analysis, it is possible to find hidden information. The security and safety of the system was ensured by the implementation of countermeasures to reduce the likelihood of detection and survive various attack scenarios.
    - **Solution:** using dependable steganography approaches that can endure many kinds of detection. To make the hidden data resistant to identification attempts, sophisticated algorithms like distortion-minimizing steganography, histogram

shifting, or statistical analysis-resistant approaches are used. To increase the security of the embedded data, the system additionally uses encryption techniques, making it more difficult for unauthorised users to find the hidden data.

- **Computational Efficiency:**
  - **Challenge:** The project struggled to analyse and execute data in a timely manner, especially when working with large photos or complicated data. Algorithms for data encoding and decoding were streamlined using optimisation techniques. To guarantee the system's responsiveness and scalability, memory management and algorithmic effectiveness were carefully considered.
  - **Solution:** utilising data structures and algorithms that have been optimised to boost the effectiveness of steganography and image processing. To reduce processing times and improve system responsiveness, methods like parallel processing, memory management, and algorithmic optimisations are used. To further improve computing efficiency, the project also investigates hardware acceleration possibilities, such as making use of GPU capabilities.

- **Interoperability and Compatibility:**
  - **Challenge:** A hurdle was ensuring compatibility with various picture formats, operating systems, and software environments. The project's objectives were to support common picture formats and provide seamless platform interaction. Enhancing interoperability and offering a flexible solution for various users required compatibility testing and adherence to industry standards.
  - **Solution:** wide-ranging image format support and cross-platform compatibility. The system makes use of frameworks and libraries that offer complete support for well-liked image formats including JPEG, PNG, and BMP. To provide easy integration with various operating systems and software environments, it also complies with industry standards. To find and fix any compatibility issues, compatibility testing is done on many systems.

- **User-Friendly Interface:**

- **Challenge:** To assist ease of use and improve user experience, it was essential to design an intuitive and user-friendly interface. The aim was to create a user interface that is both aesthetically pleasing and responsive while guiding users through the various steps of the steganography process. To iteratively improve the interface's usability and address any usability challenges or issues, extensive user testing and feedback gathering were carried out.
- **Solution:** creating a user-friendly, intuitive UI that makes steganography easier for users. Users are guided through the processes of choosing an image, encoding, and embedding data, extracting data, and decoding data using the interface's clear instructions and visual cues. The interface is improved, and any usability issues are addressed with the help of user input and usability testing, making it more user-friendly and open to users with different degrees of technical skill.

- **Data Integrity and Error Correction:**
  - **Challenge:** Maintaining the buried data's integrity and ensuring error-free extraction presented difficulties, particularly when the carrier picture was subjected to image processing or alteration processes. To identify and fix any data loss or corruption during embedding and extraction, error correction techniques like Reed-Solomon encoding were used.
  - **Solution:** putting error correction strategies into practise to guarantee data integrity during embedding and extraction. To find and restore any corrupted or lost data, error detection and correction codes like Reed-Solomon encoding are used. To guarantee the integrity of the concealed data and reduce the possibility of data loss or corruption during the steganography process, the system additionally includes checksum checking.

- **Ethical Considerations:**
  - **Challenge:** The project also discussed ethical issues related to the application of steganography techniques. To guarantee that the initiative is used properly and ethically without jeopardising people's privacy or engaging in criminal activity, appropriate rules and safeguards have been put in place.
  - **Solution:** incorporating moral principles and security measures to guarantee ethical steganography system usage. The project emphasises the value of

employing steganography for appropriate reasons while promoting ethical awareness. It has safeguards against abuse, such as watermarking or authentication systems, which deter unauthorised or malicious behaviour. Additionally, the system offers consumers explicit usage instructions and informs them of the ethical and legal ramifications of steganography.

5.2. Benefits to the Company:

The company's image steganography initiative, which makes use of cutting-edge methods for safe data concealing within digital photos, offers several noteworthy advantages. The organisation boosts its cybersecurity capabilities, acquires a competitive edge in the market, expands its service offering, improves client happiness and trust, and investigates research and development potential by creating and implementing this creative solution. Additionally, the project helps employees expand their skills by giving them the chance to become knowledgeable in software development, image processing, and cybersecurity. The growth, reputation, and success of the company in the cybersecurity industry are all influenced by these advantages. Let's examine the precise benefits the project offers the business.

- **Enhanced Cybersecurity Capabilities:**
    - The initiative gives the business cutting-edge tools for safe data concealment, guaranteeing the privacy and accuracy of sensitive data.
    - It improves the business's capacity to safeguard client information, thwart unauthorised access, and lessen future security breaches.
- **Competitive Benefit:**
    - The business acquires a competitive edge in the cybersecurity sector by providing a cutting-edge image steganography solution.
    - The organisation stands out from its rivals thanks to its capacity to offer cutting-edge solutions for data protection and secure communication.
- **Enhanced Service Offerings:**
    - The initiative expands the company's service offering by include a new cybersecurity solution to meet a wider range of client needs.
    - This helps the organisation to satisfy the demands of customers looking for cutting-edge data protection methods, resulting in corporate growth and revenue diversification.
- **Trust and client satisfaction:**

- By putting the image steganography project into practise, the business can offer clients increased security options.
- The initiative raises client satisfaction and trust in the business' cybersecurity capabilities by resolving concerns about data privacy and confidentiality.

- **Opportunities for research and development:**
  - The image steganography project offers the business beneficial chances for research and growth.
  - Investigating state-of-the-art cryptography, image processing, and algorithmic techniques fosters innovation and encourages a culture of lifelong learning.
- **Development of Employee Skills:**
  - Employees have the chance to advance their knowledge and abilities in software development, image processing, cybersecurity, and cryptography through the picture steganography project.
  - The practical experience gained via the project benefits the business in terms of employee competencies and aids in their professional development and job happiness.

Chapter – 6

Conclusion

During my Internship I was a cybersecurity associate intern at Accenture, and I was successful in completing the internship's goals. In terms of my professional development and scientific knowledge, I acquired useful capabilities. I gained a deeper grasp of cybersecurity concepts, particularly as they relate to Microsoft Azure, through practical experience and advice from industry professionals. I actively took part in numerous cybersecurity-related projects and duties throughout my internship. I had the chance to work with actual situations, examine security flaws, and put suitable precautions in place to reduce risks. The practical experience helped me improve my problem-solving abilities and gave me great insights into the difficulties faced in the field of cybersecurity.

The value of teamwork and efficient communication was one of the major lessons learned during the internship. Working alongside seasoned experts gave me the chance to observe their knowledge, gain from their perspectives, and improve my teamwork skills. My technological expertise also increased, particularly in the areas of Microsoft Azure, Windows Server 2016, ITIL, SIME, computer networks, and cryptography. During my internship, I had several difficulties, including adjusting to the hectic work atmosphere and keeping up with the latest developments in cybersecurity. But these difficulties gave me great chances to learn, which helped me improve my capacity for flexibility, time management, and critical thought.

I gained a thorough understanding of cybersecurity procedures through my internship at Accenture, as well as exposure to real-world projects and the possibility to collaborate with professionals in the field. The experience improved my technical understanding, problem-solving skills, and professional development in addition to strengthening my technical knowledge. I am appreciative of the chance to support the company's cybersecurity activities, and I look forward to using the abilities and information I've acquired in the future.

References

[1] "Fortune Global 500 – The World's Biggest Companies – Accenture Profile 2011". CNN. Retrieved 24 March 2014.

[2]"Accenture," Wikipedia, The Free Encyclopaedia. [Online]. Available: https://en.wikipedia.org/wiki/Accenture. [Accessed: May 30, 2023].

[3] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." IEEE security & privacy 99.3 (2003): 32-44.

[4] Henri Gilbert and Helena Handschuh, “Security Analysis of SHA-256 and Sisters*”, 2003.

[5] Charles G. Boncelet, Jr., Newark, DE (US); Lisa M. Marvel, Churchville, MD (US); Charles T. Retter, Belcamp, MD (US). “Spread spectrum and image steganography”, 2003.

[6] Shailender Gupta, Ankur Goyal, Bharat Bhushan, “Information hiding using least significant bit steganography and cryptography”, DOI: 10.5815/ijmecs.2012.06.04, 2012.

[7] J. Anderson, et al. Computer Security Technology Planning Study. Technical Report ESD-TR-73-51, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC), 1972. Vol. 1.

[8] A. Ghosh, J. Wanken, and F. Charron. Detecting Anomalous and Unknown Intrusions Against Programs. In Proceedings of the Annual Computer Security Application Conference (ACSAC'98), pages 259-267, Scottsdale, AZ, December 1998.

[9] K. Ilgun, R. Kemmerer, and P. Porras. State Transition Analysis: A Rule-Based Intrusion Detection System. IEEE Transactions on Software Engineering, 21(3):181-199, March 1995.

[10] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/ hipods/library.html, October 2007, pp. 4-4