Pune Vidyarthi Griha's
College of Engineering and Technology & G. K.
Pate(Wani) Institute of Management, Pune

Department Of Computer Engineering

Academic Year: 2022-23

Hybrid Cryptography and Steganography

TEAM MATE:
AYUSH BOLLA
DEEP PAWAR
PRANIT RATHOD
VISHAKHA MATKAR

Internal Guide
Prof. D.D. Sapkal

LIST OF CONTENTS

PROBLEM STATEMENT

- Data stored in the cloud can be accessed or retrieved on the users request without direct access to the server computer.
- The security issue of data storage is a big problem in the cloud environment.
- Due to the openness of cloud and sharing virtualized resources by multiple users, user data may get accessed by other unauthorized users.
- So, the hybrid cryptography algorithm is proposed in order to achieve confidentiality and increase security by combining cryptography and steganography.
- The problem statement is defined as: Enhanced Encryption of Cloud data using hybrid cryptography and Steganography.

OBJECTIVES OF THE SYSTEM

The main objectives of the proposed system:

- To combine Cryptography and Steganography techniques.
- To ensure that the data file stored over the cloud is completely secured.
- To create secure and robust system.
- To make a data or record inaccessible to unauthorized persons.
- To reduce the complexity in generating and maintaining private key during encryption.

PROJECT SCOPE

- To propose a hybrid algorithm model(AES-ECC) which will use to enhance the security of data stored over cloud.

- To reduce the computational power for memory optimization.

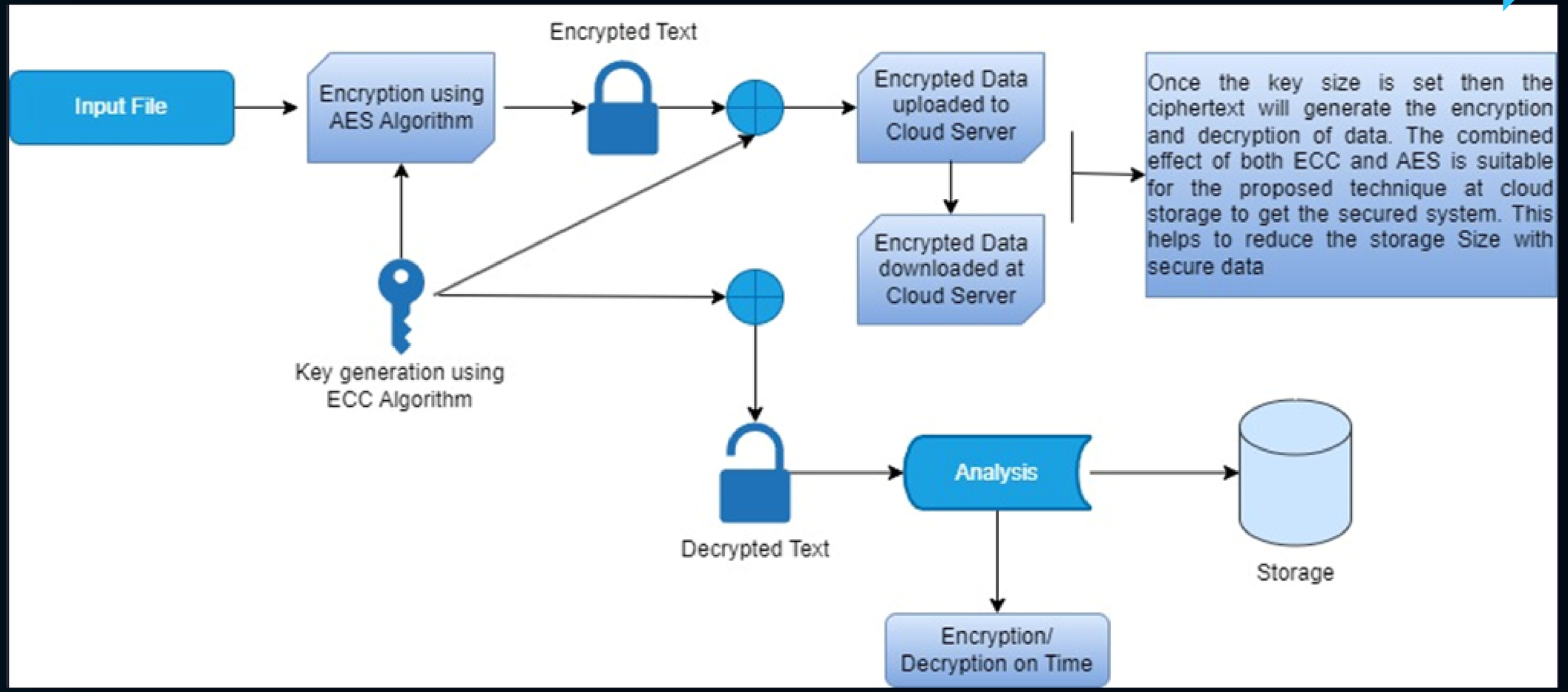
- To reduce storage and transmission requirements by reducing the key size using ECC algorithm.

- To compress encrypted data to reduce its size and allow more data to be hidden using steganography techniques.

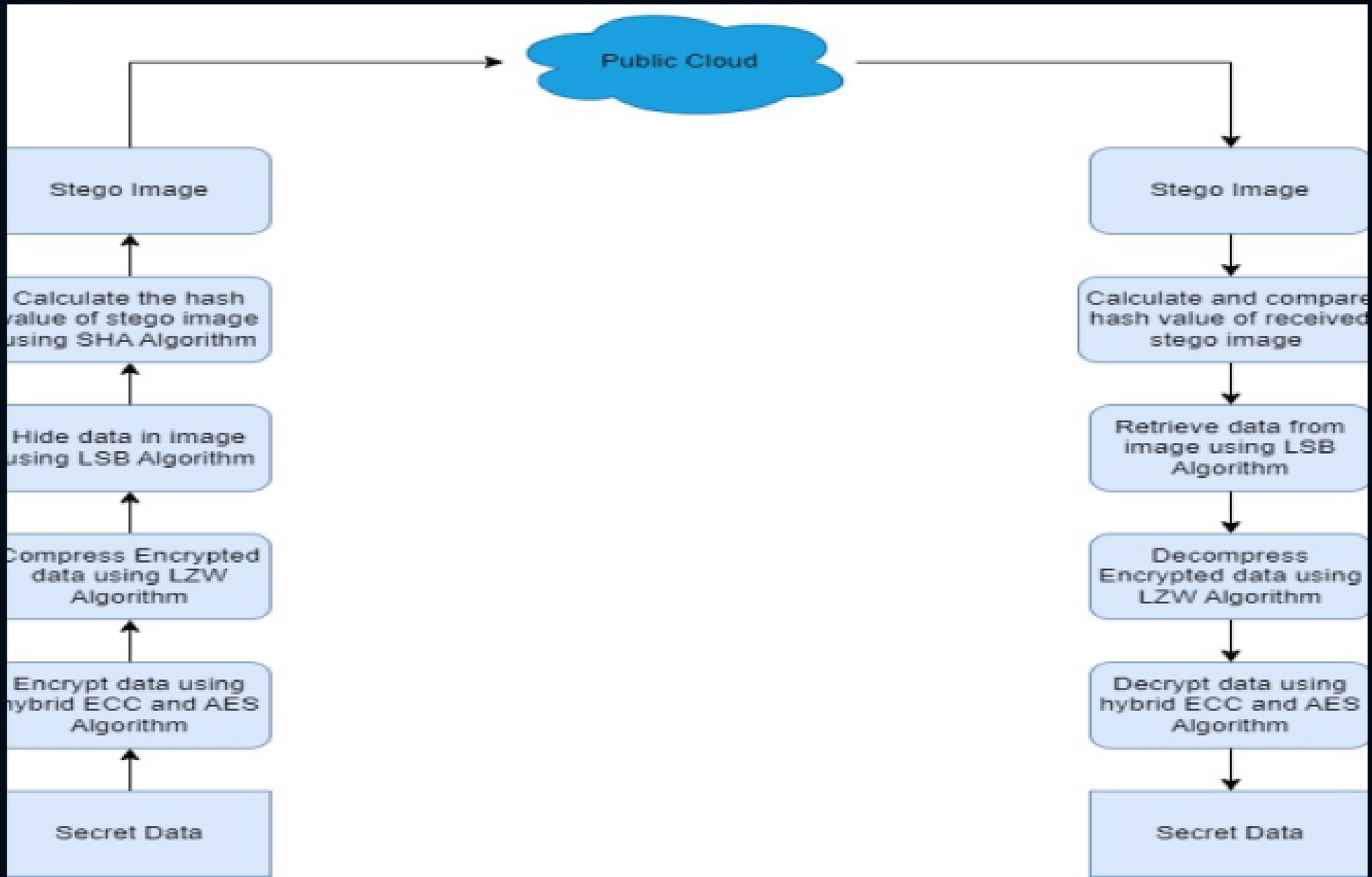
LITERATURE SURVEY

IEEE Paper Name	Published Year	Author Names	Features
Securing of Cloud Data with Duplex Data Encryption Algorithm	April 2021	C.A. Subasini, S. Nikkath Bushra	In proposed work, a cryptographic tool is proposed by utilising a combination a AES and RSA algorithms to establish a secure sharing of information.
Secure File Storage on Cloud using Hybrid Cryptography	October 2021	Vivek Sharma, Abhishek Chauhan, Harsh Saxena,	The proposed system introduces a hybrid cryptographic mechanism that involves multiple techniques to encrypt and decrypt the data. In this proposed system 3DES (Triple Data Encryption Standard) and Blowfish algorithms are used to provide security.
Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography	April 2020	Mustafa S. Abbas, Suadad S. Mahdi, Shahad A. Hussien	In this proposed work, hybrid encryption consists of the AES-256 and RSA algorithms, where both RSA and AES are effective algorithms used in the cloud environment. Encrypted data will be compressed to reduce its size and allow more data to be hidden using steganography techniques. The hybrid encryption depends on dividing secret data into odd and even data based on location in the data array.
A Survey on Steganography using Least Significant bit (LSB) Embedding Approach	June 2020	Kriti Bansal, Aman Agrawal, Nency Bansal	The proposed work gives a survey on the LSB approach used in this area. Here, LSB technique is used for image, audio as well as video steganography.

BLOCK DIAGRAM

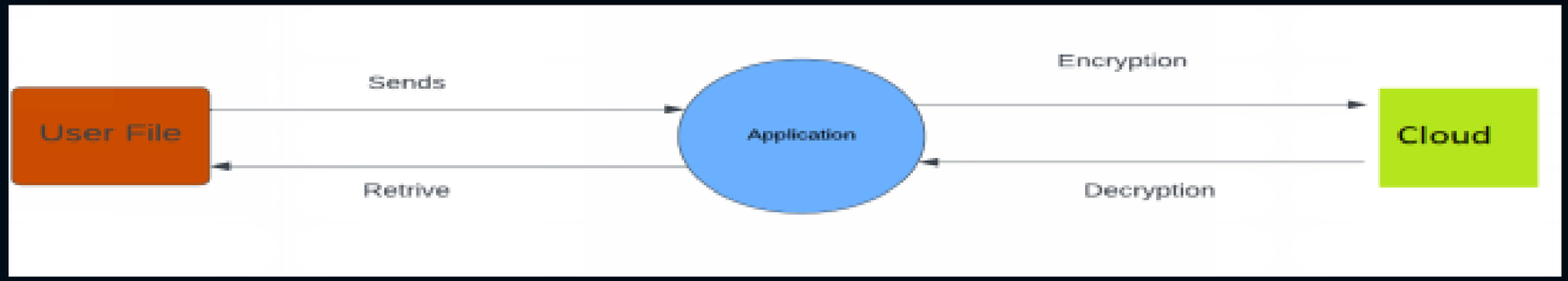


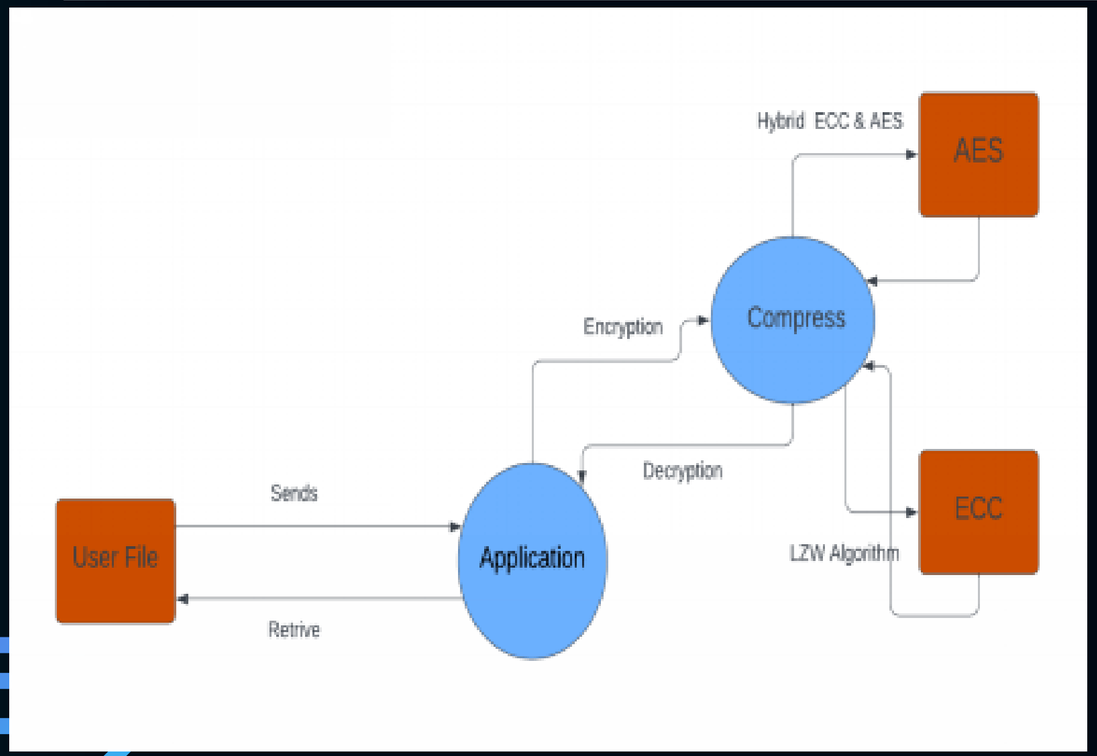
SYSTEM WORKFLOW



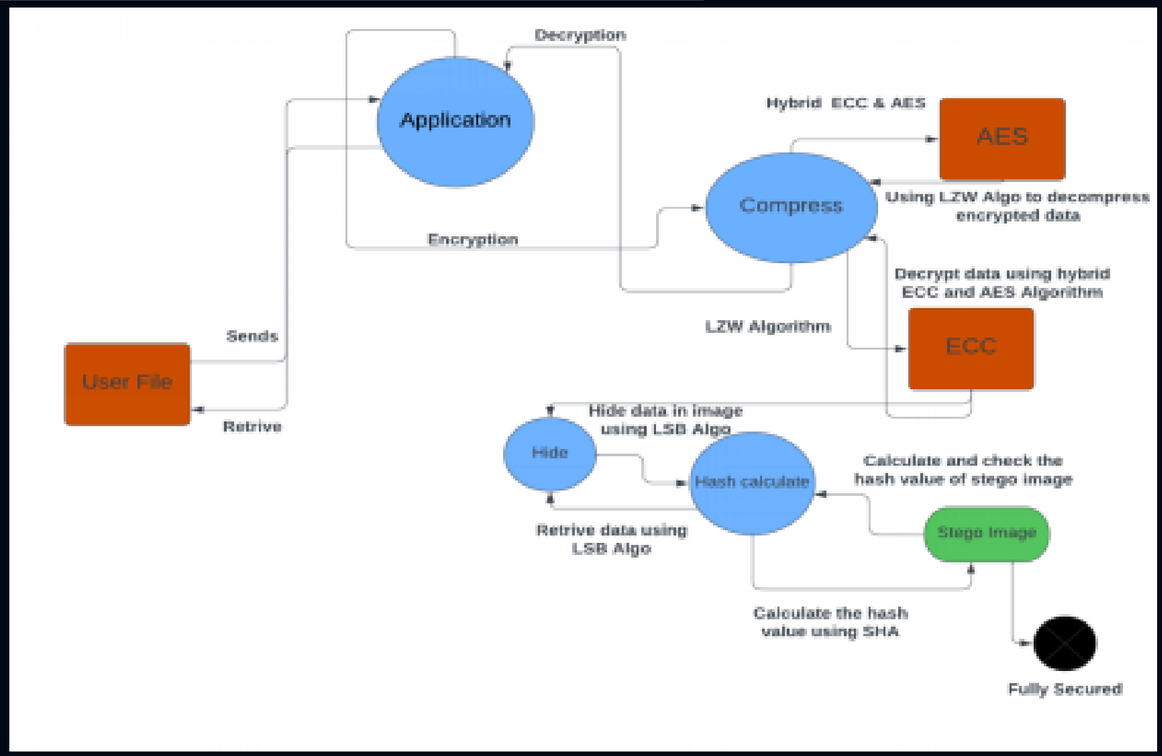
DATA FLOW DIAGRAM

DFD LEVEL 0



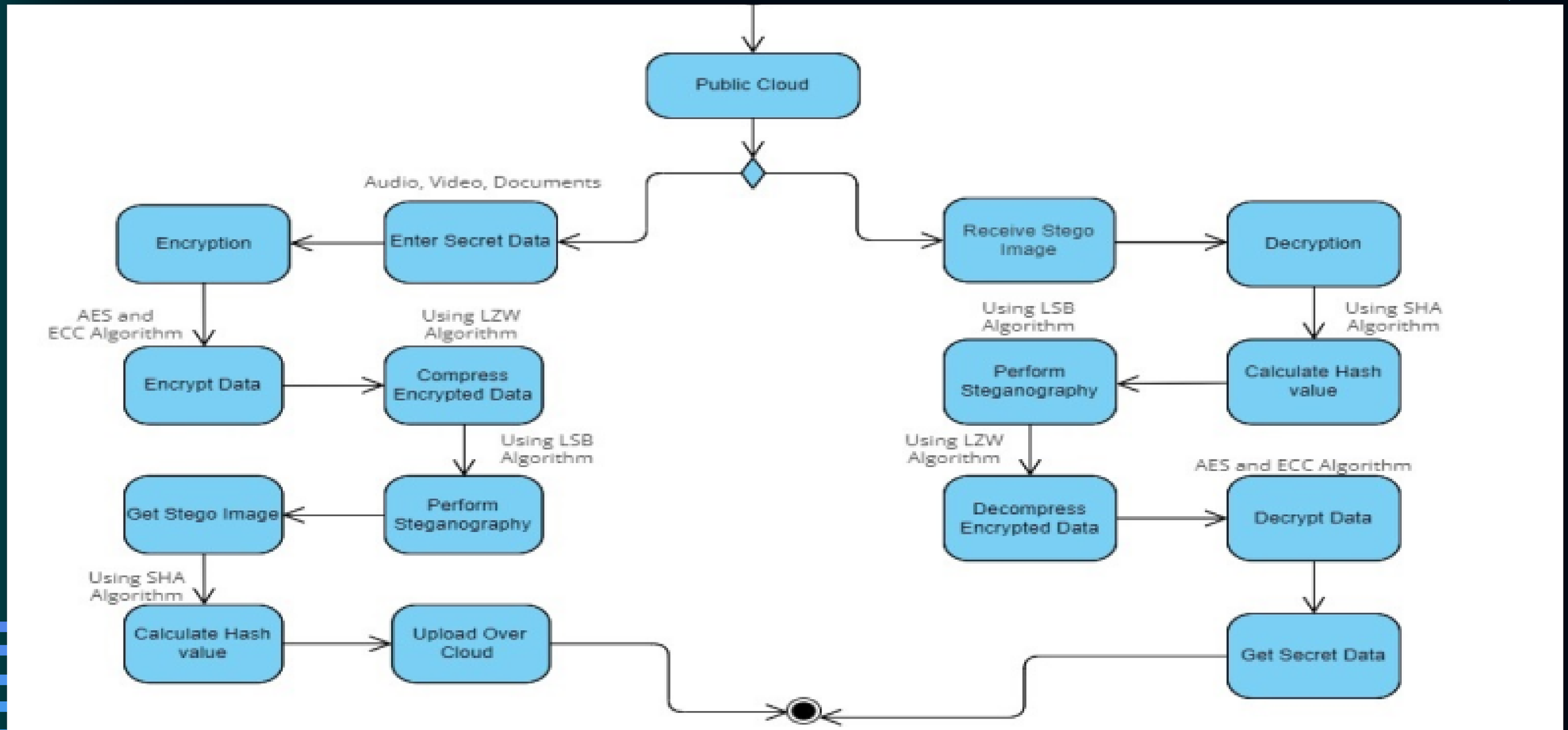


DFD LEVEL 1

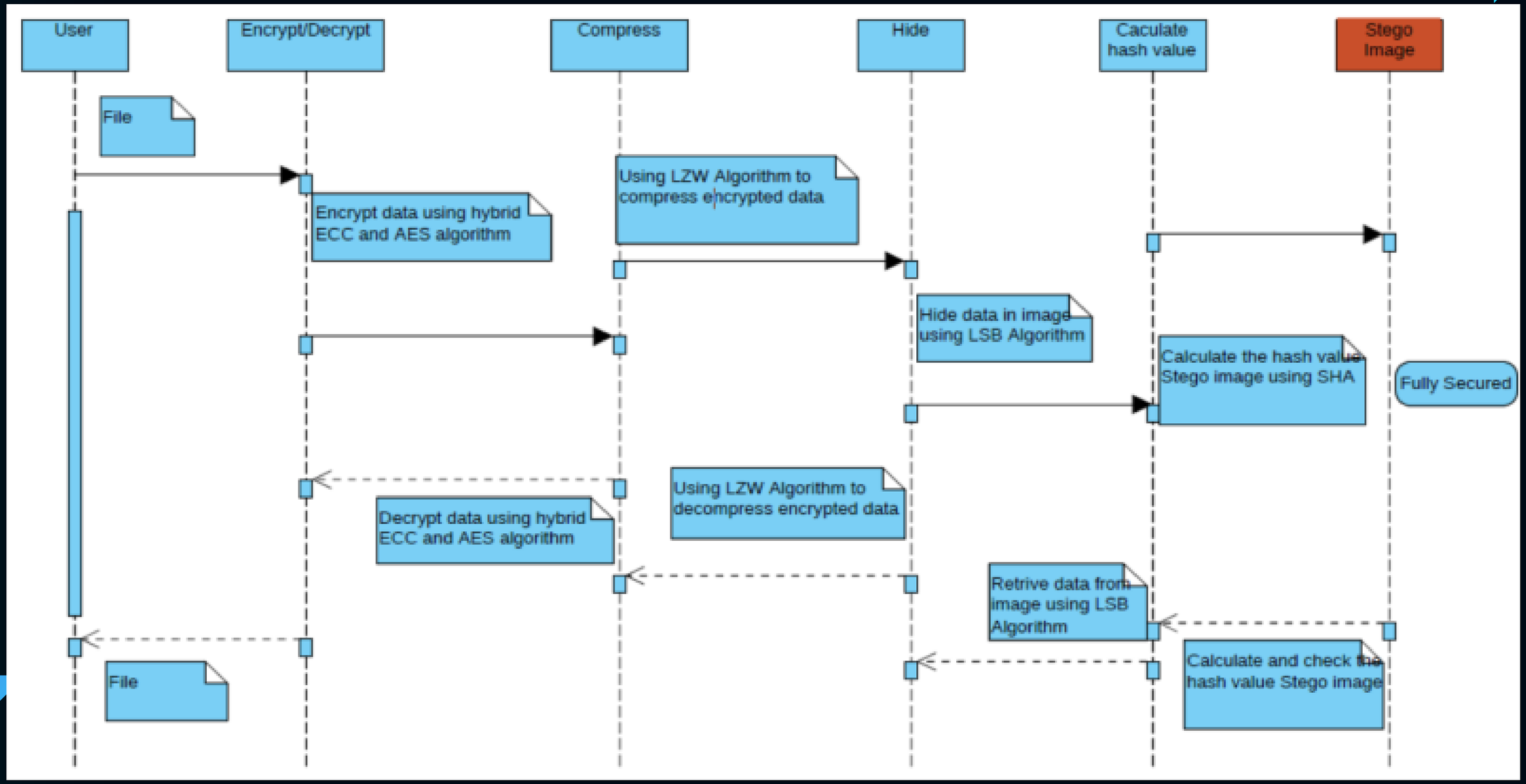


DFD LEVEL 2

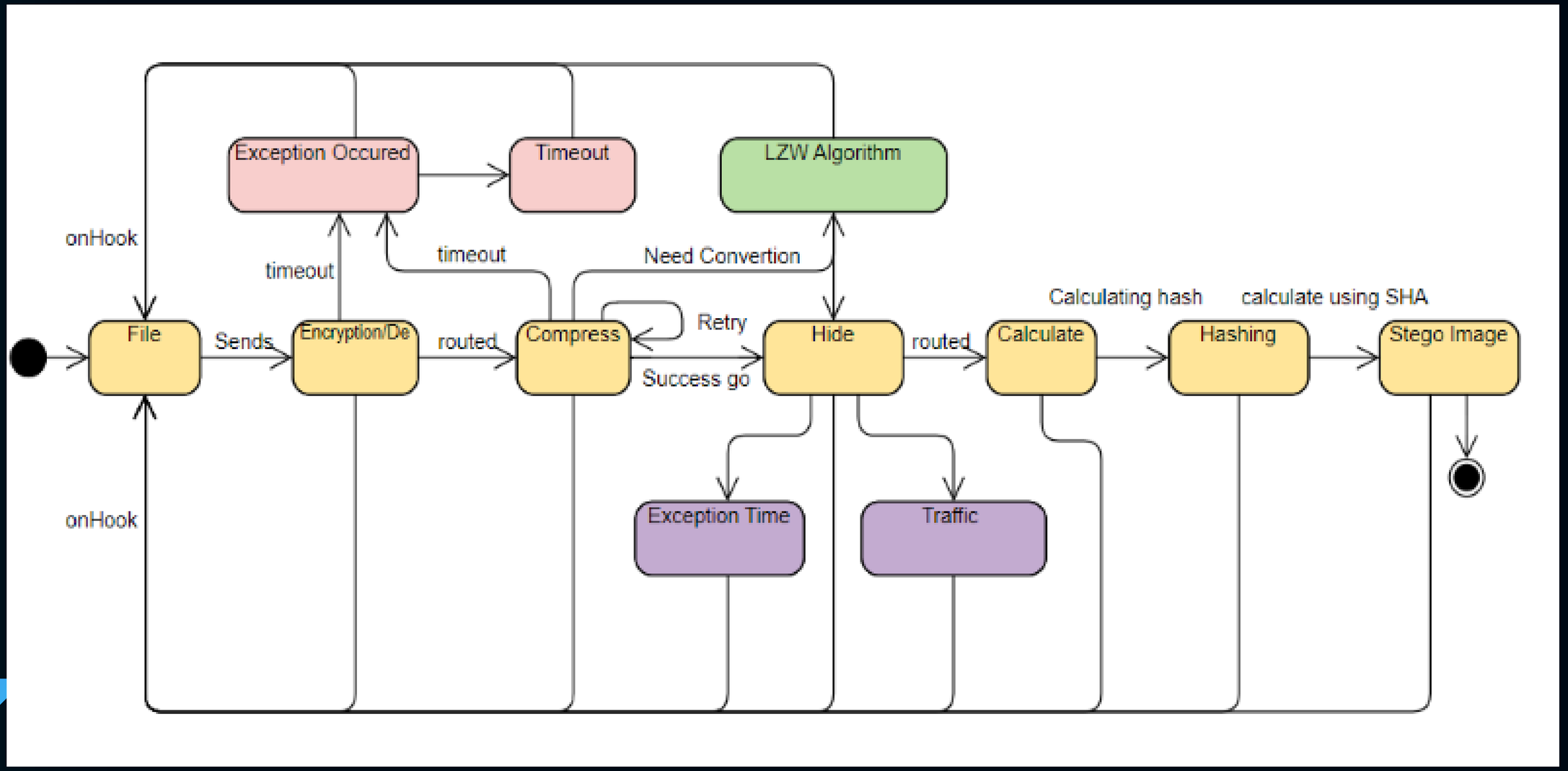
ACTIVITY DIAGRAM



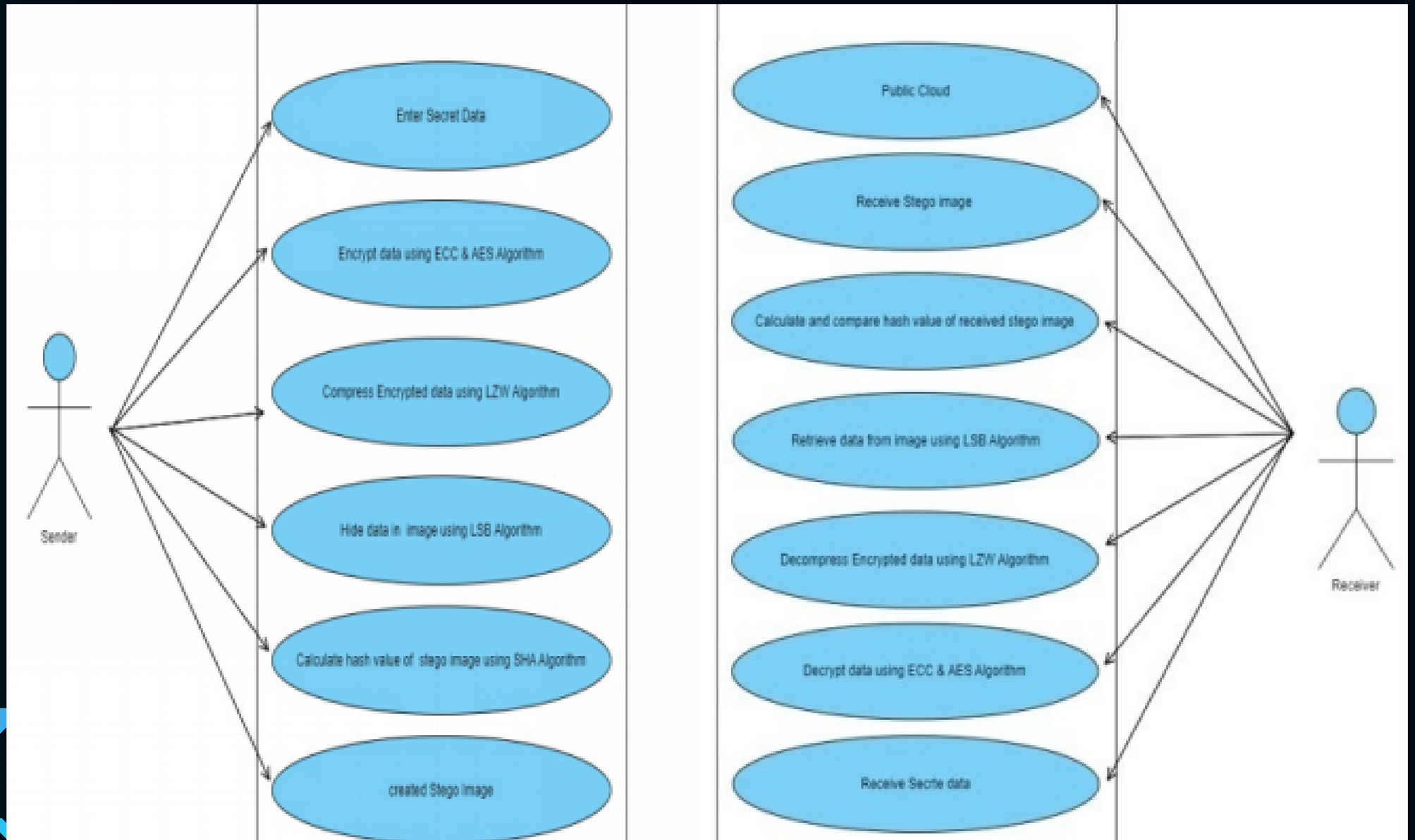
SEQUENCE DIAGRAM



STATE DIAGRAM



USE CASE DIAGRAM



FUNCTIONAL REQUIREMENTS

ID	REQUIREMENT
FR01	Every user must be registered with valid ID.
FR02	Every user must have a unique ID for reference.
FR03	The system shall be able to upload different data documents (Text, audio, video files) over cloud securely.
FR04	The system should encrypt the data and create stego image by applying different cryptography and steganography algorithms before storing on cloud.
FR05	The key for decryption and Hash value should be transported at the receiver side.
FR06	The proposed system must authenticate all authorized users to upload or receive data from cloud securely.
FR07	Hash value must be compared and verified at receiver's end for verifying data integrity.
FR08	The system should alert user if the hash value is different as compared to the hash value send by sender.

NON-FUNCTIONAL REQUIREMENTS

- Performance :
  It should perform its objectives efficiently and effectively as per the requirements.

- Security :
  Only authorized users can be able access the system

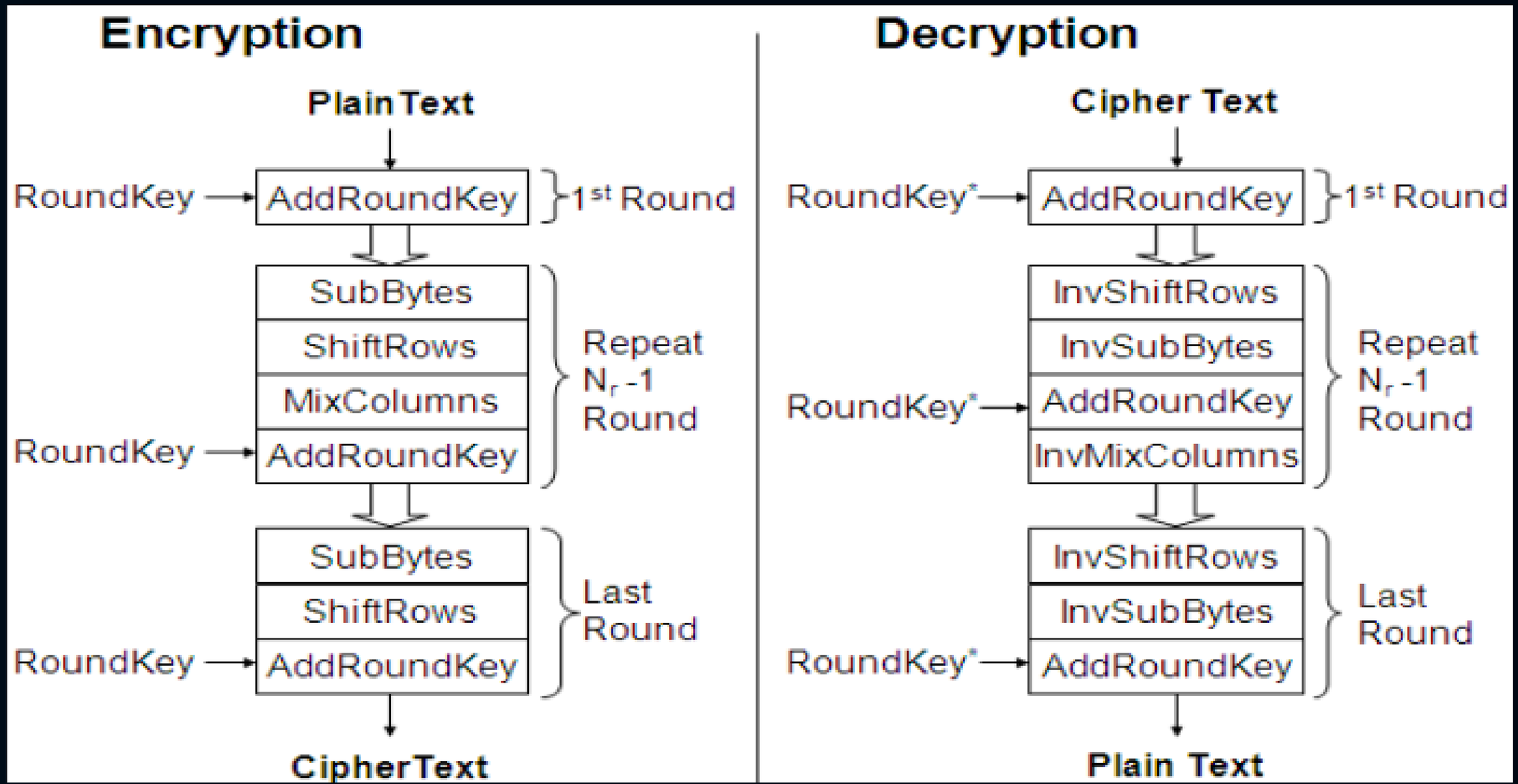
- Storage :
  It should use cloud storage for storing data.

- User Interface :
  It should provide "click and go" type of graphical interface with buttons

- Flexibility :
  Multiple users should be able to use the system (Application) at a same time from any location.

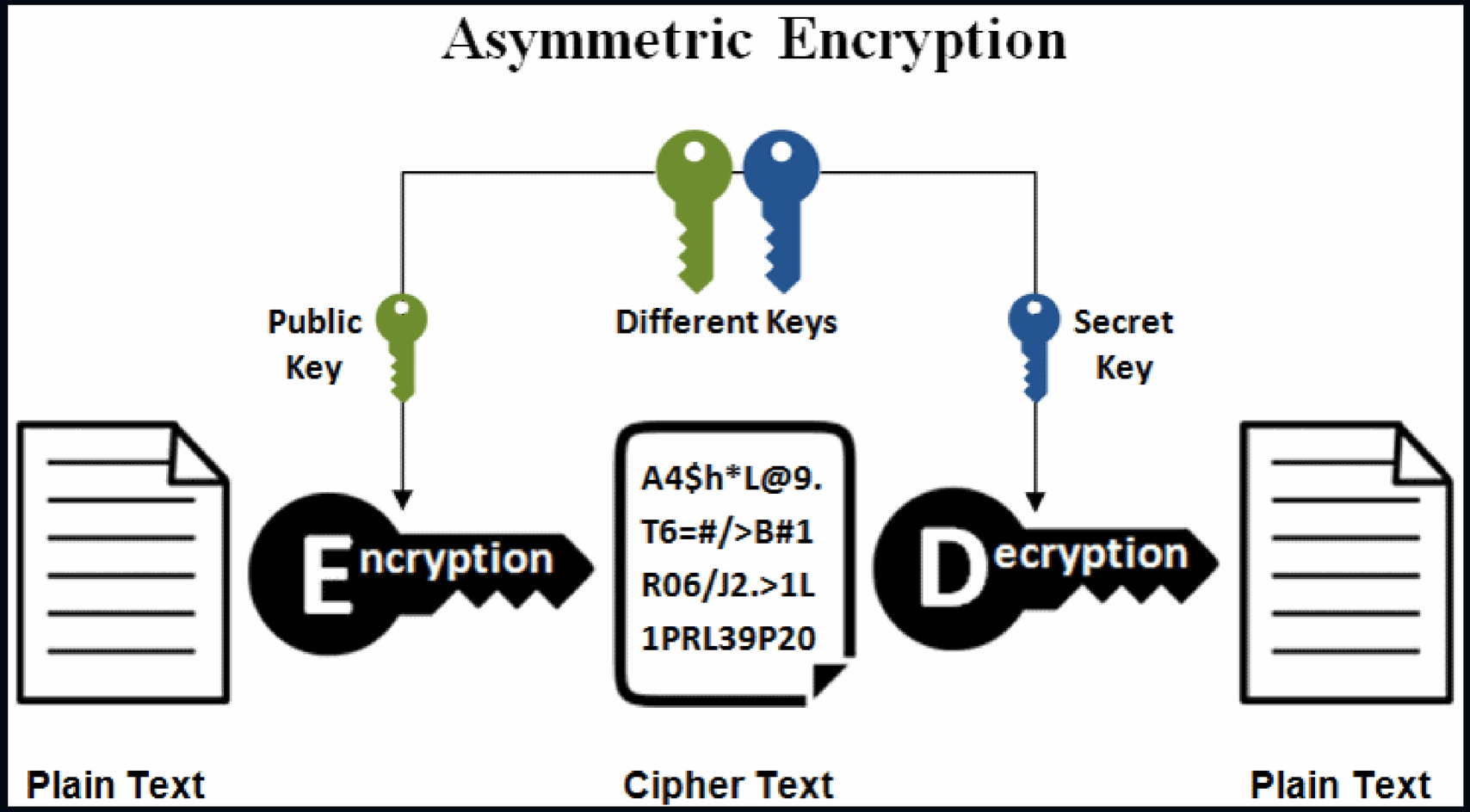
MODULES

Encryption and Decryption using AES Algorithm



MODULES

Encryption and Decryption using ECC Algorithm



MODULES

Data Compression using LZW Algorithm

BABAABAAA ↑ P=A C = empty

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA

LZW compression step 1

BABAABAAA ↑ P=B C = empty

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA
65	A	257	AB

LZW compression step 2

BABAABAAA ↑ P=A C = empty

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA
65	A	257	AB
256	BA	258	BAA

LZW compression step 3

BABAABAAA ↑ P=A C = empty

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA
65	A	257	AB
258	BA	258	BAA
257	AB	259	ABA

LZW compression step 4

BABAABAAA ↑ P=A C = A

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA
65	A	257	AB
258	BA	258	BAA
257	AB	259	ABA
65	A	260	AA

LZW compression step 5

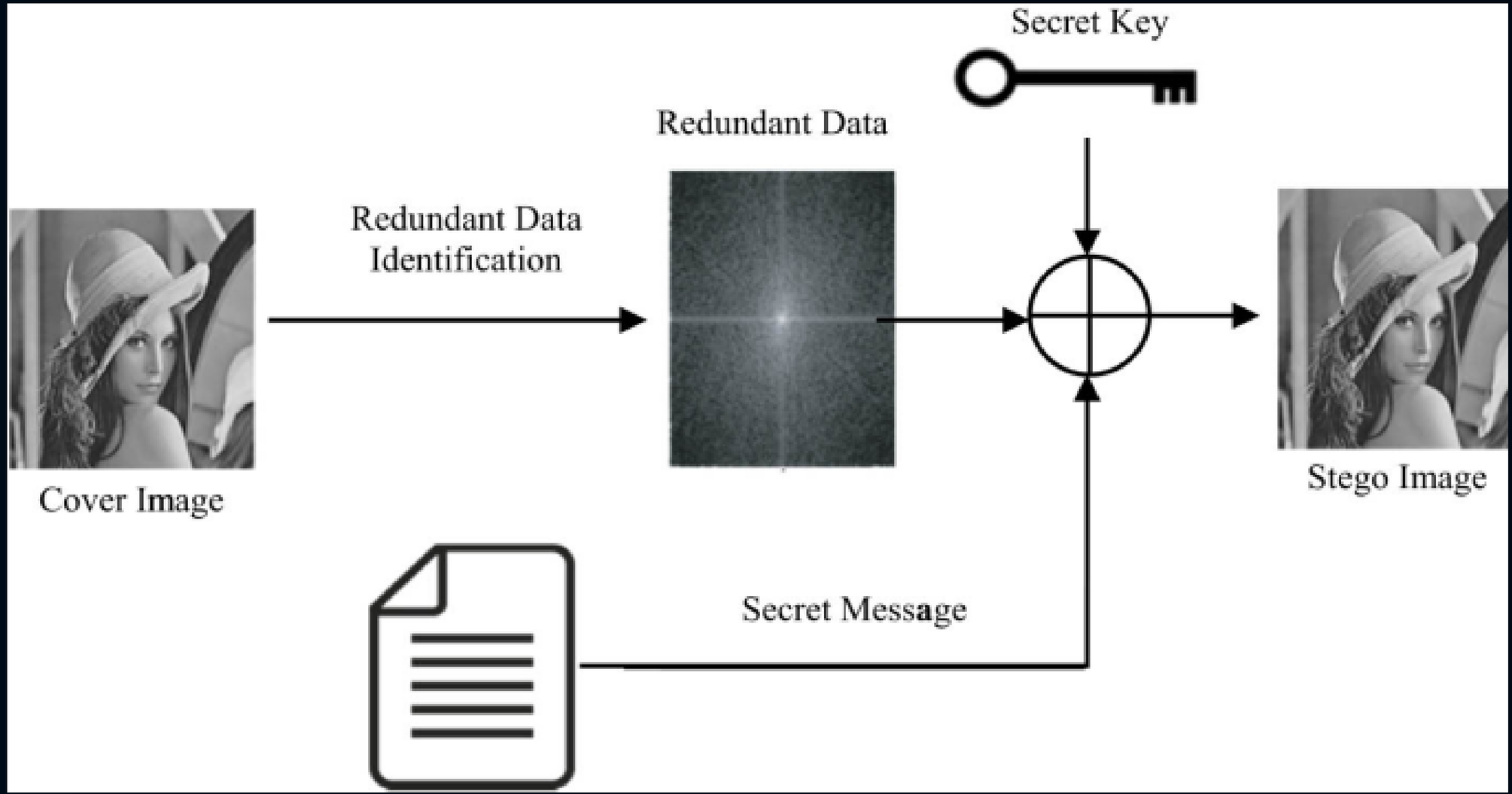
BABAABAAA ↑ P=AA C = empty

Encoder Output		String Table	
Output Code	representing	codeword	string
66	B	256	BA
65	A	257	AB
258	BA	258	BAA
257	AB	259	ABA
65	A	260	AA
260	AA		

LZW compression step 6

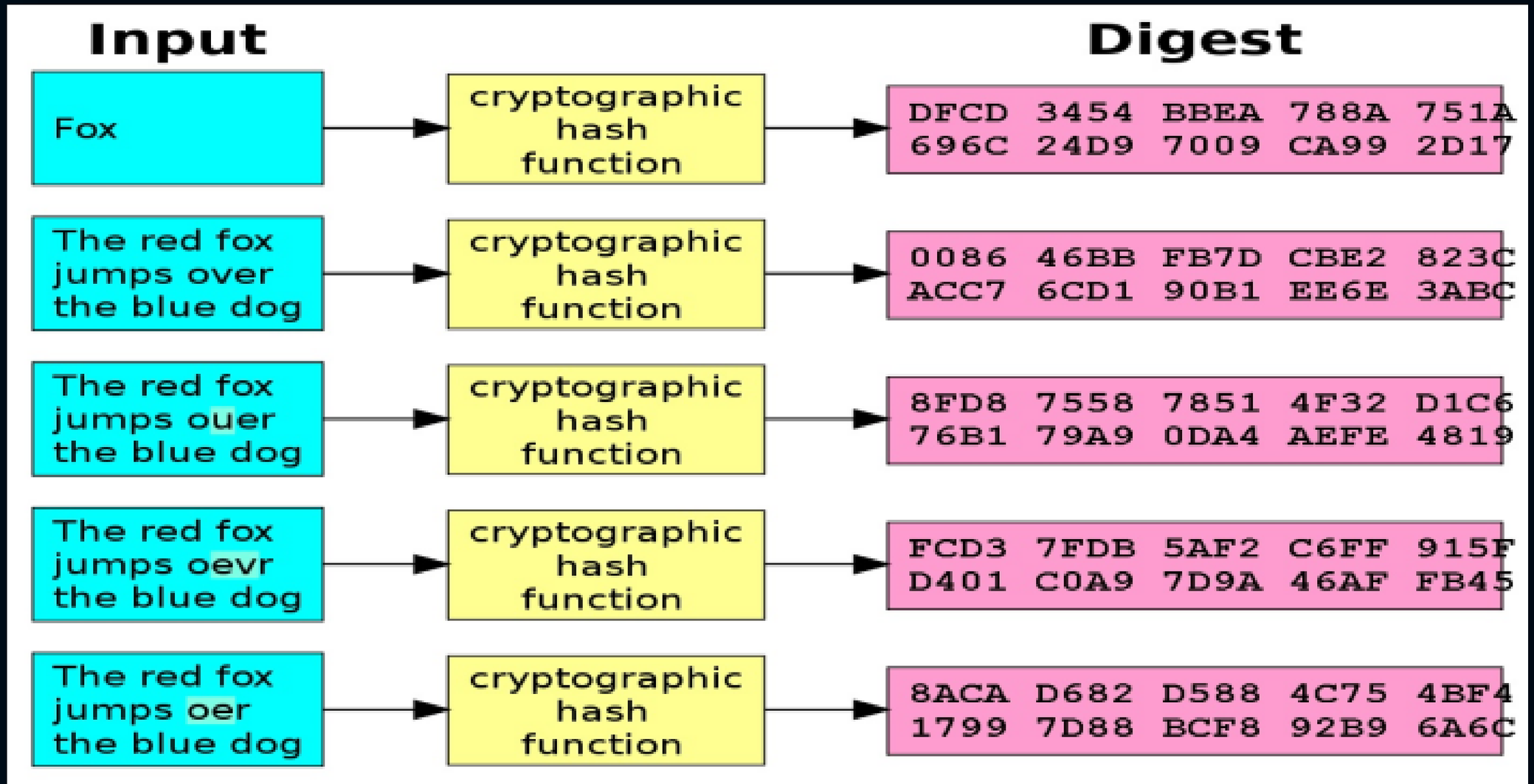
MODULES

LSB image steganography system



MODULES

Hashing using SHA-256 Algorithm



PROJECT PLAN(GANTT CHART)

PROCESS	SEMESTER 1						SEMESTER 2		
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Domain selection and exploring ideas									
Discussion of title with Guide									
Abstract and Title Submission									
Literature Survey									
Proposal Presentation									
Final Proposal Submission									
Redesigning Methodology									
Project Framework Design									
Development: Encryption Algorithm									
Development: Steganography Algorithm									
Designing Test Cases									
Accuracy and Efficiency Testing									
Applying changes									
Deployment									

TECHNOLOGOY USED

- **Java**

A wide range of software applications can be made using the highly well-liked programming language known as Java. It’s an object-oriented language.

- **MySQL**

A database management system is MySQL. A systematic collection of data is called a database. It might be anything, such as a straightforward grocery list, a photo gallery, or the enormous amount of data in a business network

- **Swing**

Swing is Provided to Design Graphical User Interfaces. Swing is an Extension library to the AWT (Abstract Window Toolkit).

TEST CASES

TC_ID	Test Case Description	Test Case Steps	Expected Result	Actual Result	Status
TC_1	To check whether admin can login to the system or not.	1. Run the project 2. Enter User ID and Password 3. Click on login.	It should log in successfully.	It is logged in successfully.	Pass
TC_2	To check whether New User can register or not	1. Run the project 2. Click on New User tab. 3. Enter the details.	It should create new user.	It creates the new user.	Pass
TC_3	To check whether it can browse the data to be encrypted.	1. Log in to the system. 2. Click on browse. 3. Select the data to be encrypted.	It should fetch the data to be encrypted.	It fetched the data.	Pass
TC_4	To check whether it loads the image after loading into the system.	1. Click on browse. 2. Select the image to be encrypted. 3. Click on Open and Load.	It should load the image.	It loads the image.	Pass
TC_5	To check whether it can generate the key or not.	1. Load the image. 2. Click on Generate Key.	It should generate the secret key.	It generates the secret key.	Pass

TEST CASES

TC_ID	Test Case Description	Test Case Steps	Expected Result	Actual Result	Status
TC_6	To check whether the data gets encrypted or not.	1. Load the image. 2. Generate the key. 3. Click on "Encrypt" to encrypt the data.	It should encrypt the data.	Data is encrypted.	Pass
TC_7	To check whether the key hides in the image or not.	1. Encrypt the data by clicking on "Encrypt" tab. 2. Click on "Hiding Key Generator" to hide the key.	It should hide the key.	Key is successfully hidden.	Pass
TC_8	To check whether the encrypted data gets send to the receiver or not.	1. Encrypt the data and Hide the key. 2. Click on "Send". 3. Enter receiver's data and click on "Send".	It should send the encrypted data to the receiver.	Data is sent to the receiver.	Pass
TC_9	To check whether the receiver can access the encrypted data or not.	1. Login as receiver. 2. Click on Image and Message Extraction Tab.	It should give the decrypted data to the receiver.	Receiver received the decrypted data.	Pass
TC_10	To check whether user can log out from the system or	1. Click on username. 2. From the options select Log out.	It should log out.	User is logged out from the system.	Pass

DEMONSTRATION

CONCLUSION

- The main aim of the proposed system is to securely store and retrieve data on the system that is only controlled by the owner of the data.
- The proposed system will solve storage issues of data security using cryptography and steganography techniques.
- Data security will be achieved using ECC and AES algorithm and key information will be safely stored using LSB technique (Steganography).
- Less time will be used for the encryption and decryption process using multithreading technique.
- With the help of the proposed security mechanism, we will accomplish better data integrity, high security, low delay, authentication, and confidentiality.

Thank You

Any Questions?