Data Embedding Technique for Image Steganography in Cloud Computing

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Software Engineering

Submitted by

Surbhi Singla

Roll no: (801631019)

Under the guidance of

Dr. Anju Bala

Assistant Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
PATIALA-147004

June 2018

Certificate

I hereby certify that the work which is being presented in the thesis entitled, ***Data Embedding Technique for Image Steganography in Cloud Computing***, in partial fulfillment of the requirements for the award of degree of Master of Engineering in **Software Engineering** submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of **Dr. Anju Bala** and refers other researchers work which are duly listed in the reference section. The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature

Surbhi Singla

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Anju Bala

Assistant Professor,

CSED

Abstract

The cloud computing security is the set to protect the data, applications stored on the cloud. The security on cloud is the concerned issues by the cloud providers as well as to the cloud users as the cloud network is prone to number of attacks such as network-based, virtual machine based, storage based, and application based attacks etc. Data embedding is the technique used for hiding the information by using the steganography and cryptography technique in a hybrid way.

Different techniques have been used for providing security to the digital data by using cryptography and steganography techniques. The cryptography algorithm encrypts the sensitive data but leave the mark that data is processed. On the other side, in steganography, the sensitive data is hide behind the cover media and leave no mark and imperceptible to un-authorized parties that data is processed. In steganography, security is dependent on how much visual quality is preserved after data embedding. Hence, Least Significant Bit (LSB) is the most used technique for data hiding in which cover media LSB bits are replaced with data bits and required 8 pixels. To improve the capacity, 2/3/4 bits of LSB has been replaced with data bits that influenced the visual quality of cover media. Hence, a layer of cryptography is added on the sensitive data before data hiding in the cover media that provides confidentiality and imperceptibility.

The main goal of this dissertation is to provide high level of security for sensitive data that is stored on the cloud database. In the proposed technique, Firstly, the sensitive data is encrypted using Advanced Encryption Standard(AES) algorithm. Next, in steganography, cover media is processed to form nonogram puzzle inside the symmetric shapes. The selection of nonogram puzzle and symmetric shape is done on the fly based on output of random number generator. Lastly, the encrypted information is hidden inside the nonogram puzzle by using 2-bit LSB technique. For experimental analysis on standard dataset images, the proposed technique is simulated and analyzed in terms of visual quality, PSNR and Embedding capacity.

Acknowledgements

I would like to express my deep gratitude to my supervisor Dr. Anju Bala for their invaluable advice and encouragement at every step of my M.E. program. Without her unfailing support and belief in me, this thesis would not have been possible. Their contribution to this thesis goes well beyond their role as an academic supervisor and includes constant support on a personal level without which this journey may never have been completed. And for this, I am truly grateful. They are great mentor for my life as well. I would like to express my gratitude to Professor and Head, CSED Dr.Maninder Singh for his constant motivation and encouragement.He sets high principles for his students and motivates and guides them to meet those principles.

Before ending I would like to thank my parents and friends for their love, motivation, support and blessings. They have been a constant source of love, concern, support and strength for me all these years.

Finally, I would like to thank the management of Thapar Institute of Engineering and Technology for providing me a great opportunity for learning, not just in academics but also in many other creative things.

I sincerely regret any inadvertent omissions. With my heartiest thanks to all.

Surbhi Singla

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IT	Information Technology
IAAS	Infrastructure as a Service
PAAS	Platform as a Service
SAAS	Software as Service
VM	Virtual Machine
AU	Audio
MP3	MPEG Audio Layer III
DSSS	Direct Sequence Spread Spectrum
LSB	Least Significant Bit
BPP	Bit Per Pixel
RGB	Red Green Blue
PVD	Pixel value differencing
QIM	Quantization index modulation
MBNS	Multiple base notational system
EV	Error values
JPEG	Joint Photographic Experts Group
DCT	Discrete cosine transformation
DWT	Discete Wavelet Transform
IQM	Image Quality Measure
RSA	Rivest Shamir Adleman
MD5	Message-Digest algorithm 5
USB	Universal Serial Bus
AES	Advanced Encryption Standard
HMAC	Hashed message authentication codes
MRSE	multi-keywords ranked search over encrypted
MCDB	Multi cloud database model
TMR	Triple-mode redundancy
DB	Decibel
GLM	Gray level modification

SNR	Signal to noise ratio
PSNR	Peak signal-to-noise ratio
IWT	Integer wavelet transform
MSE	Mean Square Error
NP	Nondeterministic polynomial
JPG	Joint Photographic Experts Group
EC	Embedding capacity
VT	Visualization technology

Chapter 1

Introduction

This chapter can include an introductory part of the work which highlights the goals to achieve security for the cloud computing. The chapter is closed with a brief summary of the work done in cloud computing, its attacks and countermeasures.
Cloud computing which is a kind of Internet based computing platform like other form of computing, delivers computing assets and services centered on the request of users and pay for their amenities and computing assets which they use[1]. Cloud computing comprises events like the use of social networking sites and other forms of interactive computing; yet, most of the time cloud computing is worried with retrieving online applications, information storage and handling power. It is necessary to securely manage, store, share and examine huge amount of composite data in order to provide better protection and discover substitute energy.

At present, the cloud providers have many services such as Infrastructure as a Service, Platform as a Service, and Software as Service and many more. [1] A cloud computing has different features such as pay on per-use service, global system access, source sharing and fast resistance.

A brief description of cloud platform is described in Figure 1.1. The cloud-computing network contains high-speed servers, large amount of database and high-speed internet network to provide services to cloud users as shown in Figure 1.1. Cloud users can access the cloud network to perform complex operations, backups, and on demand pay for dierent services. The performance, reliability and security are key parameters required in the cloud computing. Therefore, the server equipments are attached by means of an interior network. Sometimes, attack on system can generate an effect in the form of information transfer delays. [1] Instead of all the disputes of cloud, consumers are still willing to setup their organization in the cloud. The cloud providers manage customers account and maintain the cloud. [8]

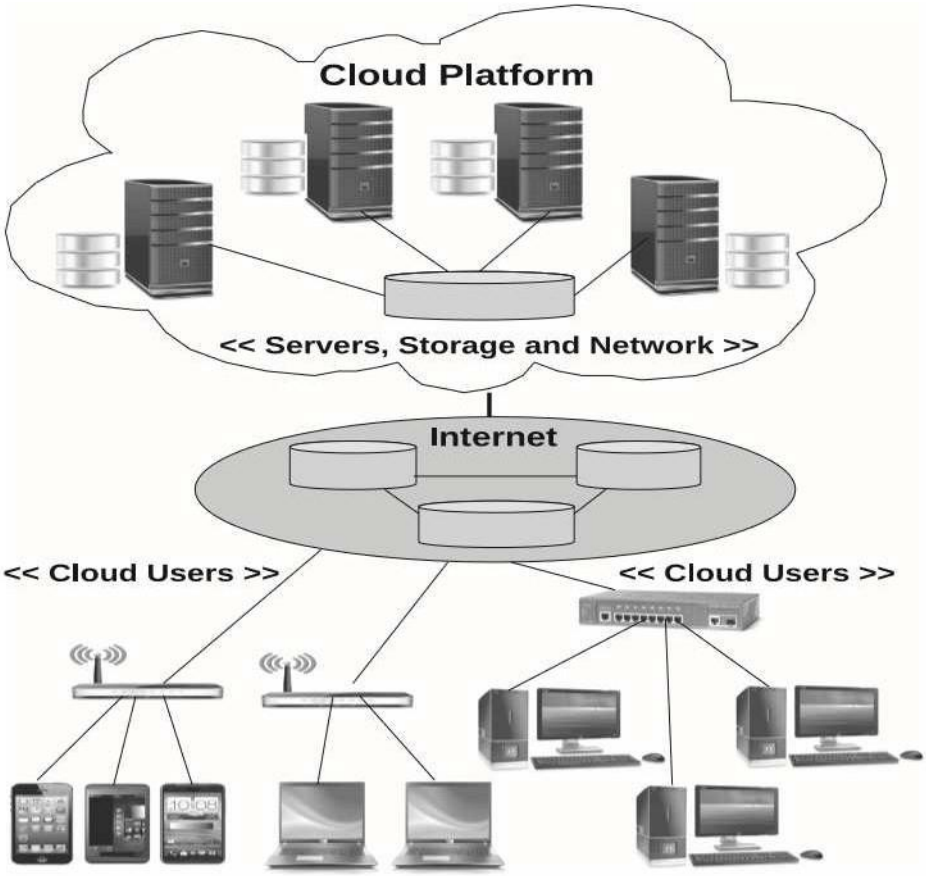

Figure 1.1: Block diagram of Cloud computing [1]

1.1 Security Issues: Cloud Computing

There is enormous amount of security problems in cloud environment.For instance it comprises various set of tools involving databases, virtualization, networks, operating systems, source scheduling and memory management.
Therefore, there are several security issues related with number of dimensions in cloud atmosphere. Authors states that, certain security issues: source location, validation and need of information attained, network based, storage based, VM based and application based issues: [39] [1]

- Source location: End-users unknowingly practice the facilities that cloud sources provide them since the location of the resources for such services are not known to them. This creates a problematic situation when objections occur. The data that is warehoused at the cloud sources are not only affected by the source policies, but furthermore by the law of the nations where the

holder exists in.[8]

- Network based attacks: The cloud computing architecture is connected with the users through internet network. The attacker attacks on the network to degrade or quality of the cloud services. There are number of network attacks such as IP spoong, port scanning and botnets.
- VM based attacks: The virtual machine is an imitation of a computer system and mostly used in the cloud network for number of services. The attackers attacks on the virtual machine to add malicious codes and try to determine secure keys, resource usage, and physical system information.[8]
- Storage based attacks: In the current scenario, large amount of users stored their sensitive information on the cloud database. The attackers try to access, destroy, or duplicate the database to aect the services.
- Application based attacks: In the cloud network, the upper most layer is application layer through which number of users interact. The attackers try to determine execution path, traces and hijacks the web services and protocols.
- Validation and dependence of information attained: The crucial data is placed in the cloud organization; the crucial data may be changed without the consent of the holder. The data changed is then processed by the holder to make judgments. The crucial step is to validate the data and should be definite.

From the discussion, there are many attacks in cloud that should be addressed by cloud users to use the technology. But the privacy is one of the upcoming issue in cloud system and the main aim is to secure the storage sensitive data on the cloud and to assure that cloud data reliability and confidentially is accomplished while they are stored in cloud system.[8] To overcome from these issues, both algorithms are used for secure communication.

1.2 Overview of Cryptography and steganography

The concept of traditional cryptographic approach is used to achieve information encryption and steganography techniques will be used to hide the secret information.Therefore, both techniques will provide security.Also, these techniques are widely used to manipulate data in order to provide multi-layer security.[24]

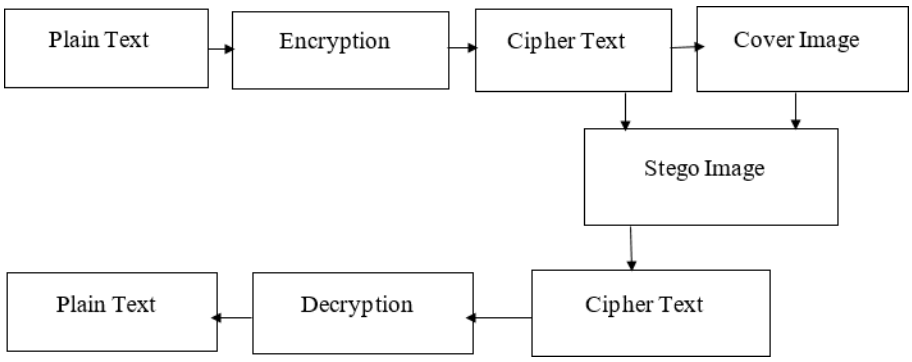

Figure 1.2: Flow diagram of Cryptography and Steganography[24]

The basic model of cryptography and steganography is depicted in Figure 1.2. From Figure 1.2, data is transformed into cipher message and the cipher message will be hidden into a visual image file. Further, stego image can be transmitted through some carrier and hide its presence.Hence,cryptography and stegangraphy can efficiently hides a message in a image and provides an additional layer of protection and reduces the chance of detection.

1.2.1 Overview of Cryptography

There are several security services in cloud computing which are delivered by using cryptographic algorithms. It defines various set of technologies and device which are used to protect the information and facilities.[42] Cryptography is basically for secret writing.

Furthermore, Cryptography deals with the encryption and decryption method of the information that is spread through an system. The Figure 1.3 shows that in cryptography algorithm where the user encrypts the information through some key and then key is exchanged with the receivers to decrypt the expected encrypted

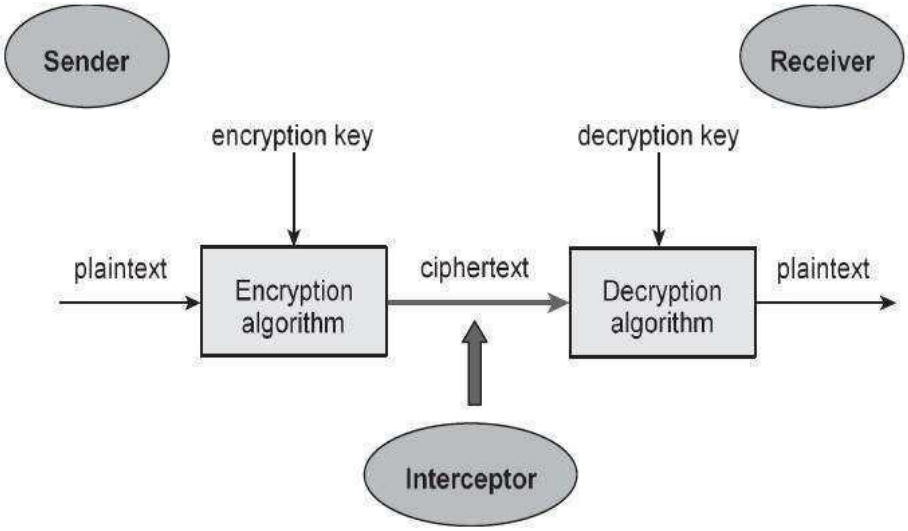

Figure 1.3: Basic Model of Cryptography [42]

message. whereas an encryption algorithm is a function of the key. If any bit change in key will affect the number of bits in cipher data. [44]

1.2.2 Taxonomy of Cryptography Technique

It can be further divided into different types: Secret and Public based cryptography. In the prior situation, with secret based cryptography, the similar key is used for encryption/decryption.

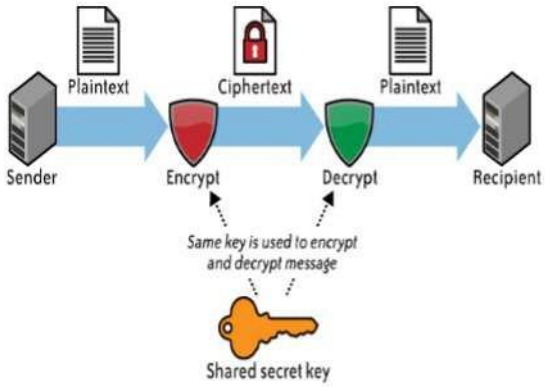

Figure 1.4: Secret based Cryptography [5]

The Figure 1.4 defines a symmetric key encryption which offers privacy between two communicate parties. A sender and recipient must already have a shared key that is known to both. Key sharing is a tricky problem.
Symmetric key cryptography is usually very fast and encrypting huge amounts of

data as compared to asymmetric key cryptography. [44].

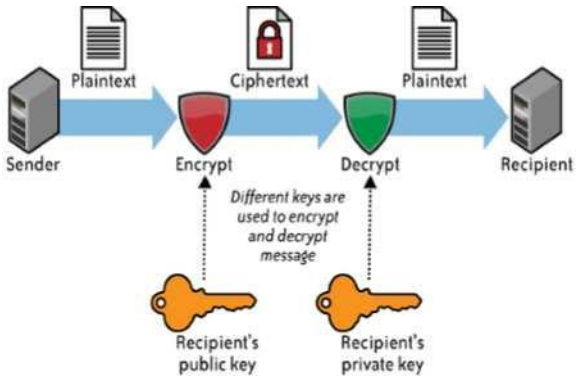

Figure 1.5: Public based Cryptography [5]

In the latter case, asymmetric or public based cryptography uses two keys: public based and secret based key. The Figure 1.5 defines the asymmetric key algorithm where the private key can kept secret data at all times, but the public key may be easily spread. Therefore, there is no need of key exchange. [5]

1. Various Objectives of Cryptography: The Cryptography algorithms have required several objective when it is design. In this section, our secure system should offer numerous assurances such as: [5]

   - Confidentiality(secrecy)- Only the sender and intended receiver should be able to understand the contents of the transmitted message.
   - Authentication-Both the sender and receiver need to confirm the identity of other party involved in the communication.
   - Data integrity-The content of their communication is not altered, either maliciously or by accident, in transmission.
   - Non-repudiation-An entity is prevented from denying its previous commitments or actions.

In this modern era, several techniques have been proposed. Mainly, cryptography transmit the secret data in such a way that it becomes an unintelligent data to attackers. So, it draws attention. Therefore, it is essential to resolve this issuse which has led to expansion of steganography system. Steganography is

used for securely transmit secret data which can not be identifiable by human eye. [19]

1.2.3 Overview of Steganography

The another offered security device on Internet is steganography technique. Steganography can be defined as a process of message hiding so that to prevent the presence of secret data.

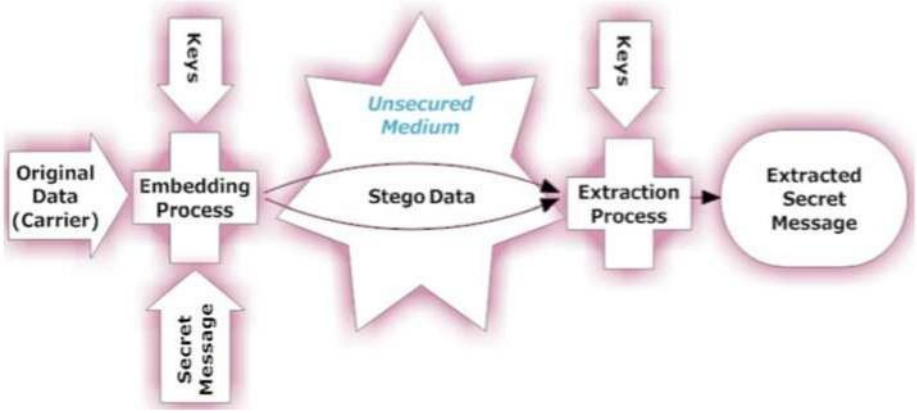

Figure 1.6: Basic Model Diagram of Steganography [34]

Figure 1.6 illustrates the basic concepts of block diagram of steganography, it is a secret communication in a suitable conveyor, e.g., picture, audio, video and so on. In image steganography, the secret information can be embedded in such a way that the detection of data is invisible. After injecting the secret information, it can be denoted as stego-medium. Where a stego-medium is mainly used for secret hiding scheme to limit discovery and abstraction of the embedded information. In case, existence of secret data is exposed or even doubted, the determination of steganography is beaten, even the message content is not removed. [34]

As from the research work, steganography is basically used for cover writing. Thus, there are number of issues of steganography are: - [14]

- Security of data Hidden Communication: There is rise in uncertainties of eavesdroppers, and particular screening of method recognition, the secret data must be unseen statistically.
- Payload Size: In Contrasting watermarking, steganography focuses on a

goal of hidden communication and thus, they generally needs a necessary embedding capability. Necessity for high payload and safe communication are generally inconsistent. Focusing on a particular application scenarios, a balance is being required. The next section will briefly explained the highlights of different methods of steganography.

1.3 Taxonomy of Steganographic Techniques

There are several methods in categorizing steganographic techniques.

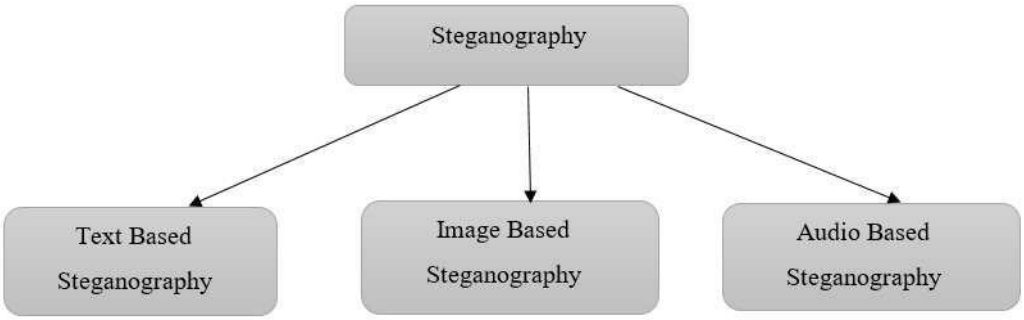

Figure 1.7: Types of Steganography [17]

These techniques can be categorized by depending on cover image which is used for secret communication. Another possibility can be done by sorting the type of cover image that is applied in the process of embedding. [16] Therefore, in Figure 1.7 illustrates the techniques of steganography which is classified as depending on the media in which secret data is hidden. These can be text, image and audio: [17]

I. Text Steganography: This approach uses the text based media for hiding data in a cover image called as text based Steganography. There are various methods used to embed information in text documents. [17]

- Design Based approach: This method involves the modification in the current data to embed the information in such a way that it contains the addition of spaces, text resizing, transformation the format of data.
- Unsystematic and Arithmetical approach: In this method, symbols are hidden in randomly manner. These technique determines the statistics

such as mean, variance and so on which measures the amount of duplicate data to be hidden secretly within the media.

- Dialectology approach: It is the mixture of grammar and semantics. Syntactic attacks gives the exact arrangement when text is produced from syntax.

II. Audio Steganography: This method uses the digital based media to hide the secret information, the method is known as audio steganography. Secret data can be embedded in AU and MP3 audio documents. Audio Steganography can be classified into various categories: [17]

- Truncated Bit Encrypting Method: This method involves pitch prediction which is accompanied through truncated bits of speech encoding. Therefore, it maintains the management between data hiding and speech coding.
- Segment Encrypting Method: In this approach, stream data breaks audio into stream and embed hidden sequence into phase spectrum of the first stream.
- Spread Band Encrypting Method: Mostly used approach of spread based encrypting is DSSS. It can extent steganography by adding with some pseudo-random order.

III. Image Steganography: This is the most popular method used for Hiding data inside the media. This approach uses the image to embed secret message.[19]

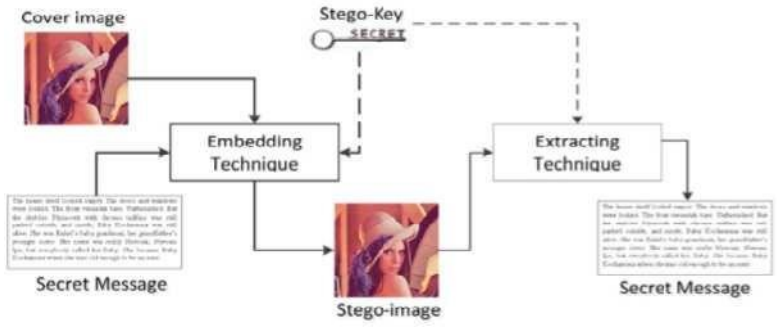

Figure 1.8: Image Steganography [19]

The Figure 1.8 illustrates the basic model of image steganography diagram. This

Figure defines the cover source which is treated as a media i.e. image and the data which is to be transmitted safely are files, audio or image and the process of embedding has been executed by spatial or frequency areas. Both these areas are used for embedding the bits of message into the steganography processes.

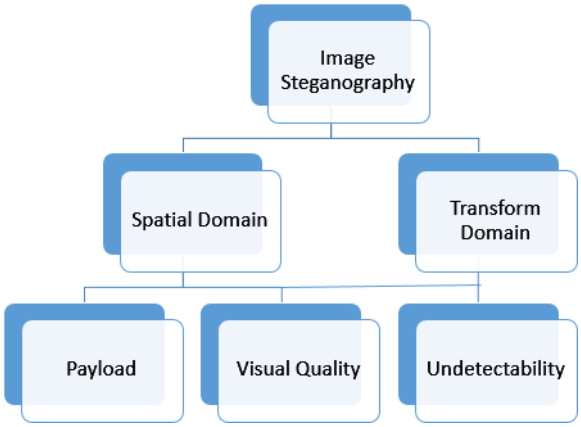

Figure 1.9: Image steganographic fields with various goals [19]

Many research works on image based steganography, to embed the data inside the cover image without altering its visible assets, the source image can be changed into noisy regions through numerous color distinctions, so less alteration will be done. There are various techniques used for these modifications which involves the usage of the LSB, concealing, sifting and conversions on the cover image. These methods can be used with fluctuating units of accomplishment on various forms of pictorial documents. [19]

From Figure 1.9, Image steganographic fields describes spatial domain for secret data hiding into the cover image pixels, the main goal of spatial steganography is to directly modify the picture pixel values for hiding information. In contrast to transform image, the cover pixel is first converted into transform based domain, then hidden message is embedded into transform constants. [19] To enhance the embedding capacity, image quality and security so number of techniques has been proposed in the spatial and frequency field.

Most of the work concentrated on image steganography, an image steganographic method is defined by these purposes:[19]

- Embedding capacity: How many number of bits which is inserted into one cover pixel. It can also be defined as a capacity of a cover image that contains secret message.

- Visual image quality: How much the degree of stego-image which is same to its cover pixel. After embedding the hidden message in the cover image, superiority of the stego image should be similar and no one can privilege about imperceptibility.

- Security: How silently the cover image is exposed of having a secret data or how vigorous the embedded secret data is being resist the steganalysis detection attacks. Therefore, Confidentiality is used to defend information from unauthenticated people.

Thus, the basic steganographic technique must achieve the above goals concurrently. [14] So, Image steganography is classified two domains: [43]

I. Spatial domain steganography: Spatial domain is defined as the directly modification of picture pixel values for hiding information in the cover image pixels. The degree of embedding is defined in bit per pixel (bpp). In Figure 1.10 shows various methods of spatial domain. Firstly, The LSB pixels have been used to embed the message bits by using spatial domain which may alter the image histogram. In few techniques, the actual image must be retrievable in destination side. These systems are called as reversible steganography. [43]

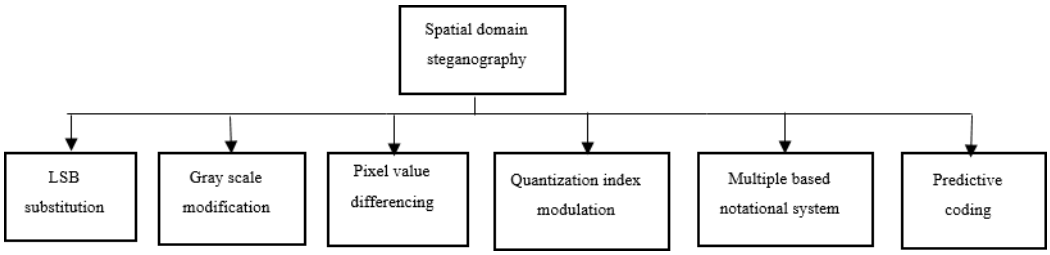

Figure 1.10: Techniques of spatial Domain Steganography [43]

Furthermore, most of the researchers recommended for high capability steganography that are histogram shifting based techniques, path quantization based methods, interruption based techniques, pixel rate differencing based methods and etc. From these systems, the core objective is to achieve a high embedding level with

less number of variations in the quality of stego-image. According to the embedding method, we explored different types of steganography in the following as:

- Least Significant Bits: The most popular technique used for embedding data in cover image is LSB. It is the easiest method to embed the message bits into LSB level of the cover image in a particular sequence. The secret information is directly embedded in an image; an appropriate cover image is required. By means of a 24-bit color picture, each bit of the RGB color modules can be used, thus, complete 3 bits can be kept in each pixel. For instance, the subsequent network is taken 3 pixels of a 24-bit color picture by using 9 bytes of memory: [17]

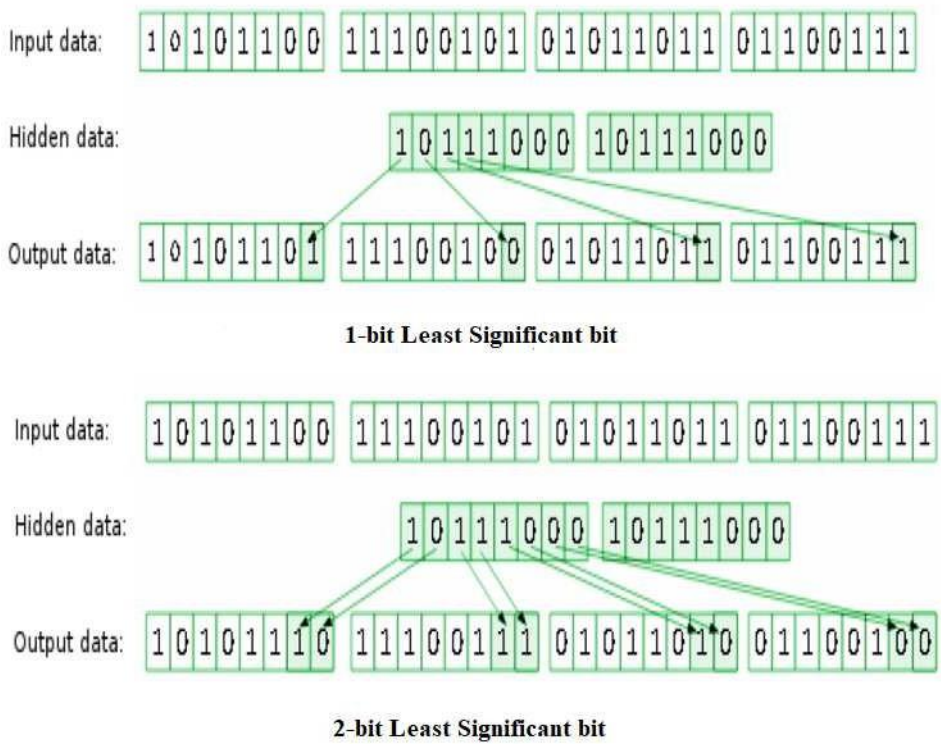

Figure 1.11: Least significant hiding Technique[31]

The basic least significant hiding techniques is shown in Figure 1.11. This Figure defines operation of one or two bits that are required to be transformed to supplement the character effectively. Only partial message bits in a picture will required to be changed for secret hiding using the maximal cover size. We have analyzed that the LSB of third color is persisted without

any variations. It can be used for examining the accuracy of 8 bits which are inserted in these 3 pixels. Also, it could be used as equality bit.

- Gray level modification: This method is mainly used for combining the information by changing the gray planes of pixels. This method mainly uses the idea of both odd and even records which combine an information with in a cover image. The main importance of this technique comprises less computational complexity and high data hiding capability. e.g. 1 is mapped with odd value and 0 is mapped with even values. [43]

- Pixel value differencing (PVD): Some authors established an innovative embedding idea depend on difference between various pixel values. Embedding of secret bits based on whether the pixel value is in edge region or in smooth region. Therefore, in order to deliver safe communication and reverse numerical issuses, various methods depend on PVD are establised. [43]

- Quantization index modulation (QIM): QIM refers to embed the data in cover intermediate by initially modifying the key or arrangement of keys within the embedded data and then quantizing the host indicator with the related quantizer or order of quantizes. [43] However, the main issue of QIM is that it is sometimes more difficult to modify an index while embedding.

- Multiple base notational system (MBNS): A method can be act as a notational method with several bases to limit a private data to be concealed. In other words, a secret message is transformed into a sequence of characters with different bases and changed data carrying capabilities.[43] Mostly, the secret data is a binary stream and a quantity of data embedded in each character is accurately one bit.

- Predictiion steganography: Embedding by changing the pixel standards directly leads to major changes in stego image causing less hiding capability and reduced the pictorial quality. To overwhelmed this problem, predictive coding method is proposed where pixel values are predicted by using estimator and instead of changing the pixel values, estimation error values (EV)

are altered to embed secret information.[43]

Therefore, spatial domain steganography systems attain high embedding capabilities. Thus, they are susceptible to any slight alterations. Also, these approaches can recompense the numerical assets of image, representing bad strength against lossy density and image filters. Thus, frequency domain steganography is choosen.[43]

II. Transform domain Steganography: In this technique, the cover image is firstly transformed into transform domain, then hidden message is embedded into frequency constants. In this, secret message is hidden in major areas of covered image, which provides enhanced level of security to steganography technique then result into the expansion of algorithms. [25]

To get the transform representation, transformation of image is used.In general, the basic model for frequency steganography can be explained in Figure 1.12. Image can be used to carry hidden data i.e. cover media is engaged as an input. Cover media breakdown can be obtained by forward conversion to get coefficients. These transform coefficients can be changed for hiding secret information. With the help of chosen embedding scheme, hidden information can be embedded in appropriate frequency coefficients. Then, apply reverse frequency domain to develop stego image. For Decryption, related steps can be performed to recover cover image and hidden information. [43]

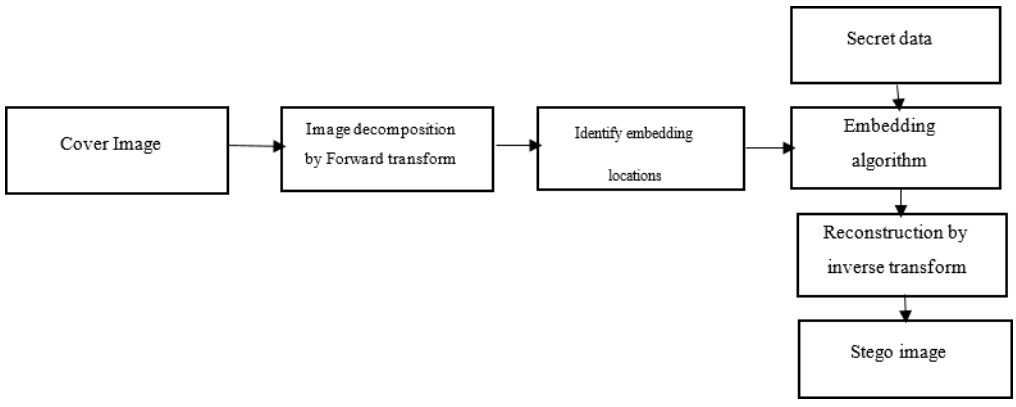

Figure 1.12: Block diagram of frequency domain image steganography [43]

- Discrete cosine transformation steganography: JPEG is most popular and mostly used file format on web. For conversion, JPEG usually practices

DCT which transforms spatial to frequency domain. The main importance of DCT is that it takes interrelated input information and concentrates its energy in initial frequency coefficients.

- Discrete Wavelet Transform steganography: DWT decomposition may results in four groups. Bottom sub group has the most significant and contains relevant data and the higher sub band has finer details. Most of the energy is compressed into some frequency coefficients-an entropy coder traces them and encrypts.

- Classical based steganography: The author suggested the indication of classical based steganography that depends on some numerical assets of the cover intermediate. So, it is called as adaptive based steganography.

- Image quality measure (IQM): IQM is used to provide quantitative information on the fidelity of condensed images. Usually, the quality of an image synthesis technique can be estimated by using statistical method which try to quantify reliability using image to image comparisons.

So, from the above analysis, it is concluded that spatial domain methods are more relevant than frequency domain due to the sensitivity in embedding and retrieval process. [19]Also, spatial domain can provide high image quality and embedding capacity as compared to transform domain. The explained difference between these two domains are shown in Table 1.1

Table 1.1: Comparative analysis between spatial and transform domains

Key Features	Spatial Domain	Transform Domain
Security	Susceptible to geometric attacks	Resilient to geometric attacks
Robust	Extremely prone	Fewer prone
Type of System	Simple system	Difficult system
Image Quality	High	Less manageable
Pixel Handling	Direct	Indirect
Implementation	Simple	Difficult
Embedding Capacity	High	Less capacity

As discussed about the various techniques of steganography and their impact on target organization have been defined. Further, researchers have tried to combine both with the aim to provide better security.

1.4 Fusion of Cryptography and Steganography: Cloud Computing

Steganography and cryptography are interlinked with each other. Many researchers can also apply cryptographic algorithm to the secret data before embedding it to provide additional security. According to [14], Steganography is used in place of cryptography, not replace it. It provides high level of security. If a secret data is encrypted, it must also be decrypted if exposed.The distinction between these technologies is significant one, and is summarized by the Table.

Table 1.2: Comparative analysis between cryptography and steganography

Description	Cryptography	Steganography
Description	Cryptography	Steganography
Goal Achieved	Confidentiality	Imperceptibility
Carrier File	Plaintext	Image, Video, Audio, Plaintext
Key	Required	Optional
Output File	Cipher File	Stego file
Information Transparency	Visible	Non Visible
Security Level	Depend on key and encryption algorithm	Depend on Hiding Technique
Goal Failed	Plaintext Recovered	Communication Detected

The comparitive analysis of cryptography and steganography as been shown in

Table 1.2. With cryptography, it is the most popular technology and comparison is done between portions of simple text and encryption text. With steganography,it is less known technology and comparison is done between encrypted media, stego image and portion of the data. [29].

1.5 Thesis Organization

A brief description is given below:

- Chapter 1: This chapter defines the goals to achieve security for the cloud computing. The chapter is closed with a brief summary of the work done in cloud computing, its attacks and countermeasures. This chapter also presents a survey of the literature in the related area and identified the prominent research gaps.Further, research objectives are defined with the research methodology used in this study.
- Chapter 2:Chapter2 describes the work done by various researchers in the field of Cloud security.This chapter also presents the necessary background needed for proposed work.Further, various cryptographic and steganographic concepts are discussed to enable secure communication.
- Chapter 3: In this chapter,problem was discussed which was seen in the analysis done in chapter2.The research gaps were discussed and the objectives were formulated to overcome the research gaps and the problems faced.
- Chapter 4: This chapter describe the proposed methodology to meet the required objectives formulated in Chapter3. The techniques are used for detail description of the proposed technique and its components.Also, this chapter presents the multi-layer security system by using cryptography and steganography algorithms which are discussed in detailed and the various algorithms are formulated.
- Chapter 5: This chapter study the performance of technique and the multi-layer security.Further, the chapter represents the proposed technique which is simulated and performance analysis is done to show the robustness against visual attacks. Various encryption algorithm are discussed and results are

compared with other techniques.

- Chapter 6: This last chapter gave the conclusion from the implementation and the result formed for achieving the desired objectives for this thesis. The future scope of the thesis have been discussed.

All the above brief descriptions are discussed in subsequent chapters. The further chapters are enclosed with a brief description, motivation and literature survey of the work done in the thesis.

Chapter 2

Literature Review

In this chapter, the work is done by various researchers in the area of Cloud security has been discussed. The main aim of information hiding is to address the security of information by concealing the protection of secret information. Section 2.1 below discusses the work done by various researchers to provide survey on numerous important cryptographic concepts and their significance in embedded system applications. Section 2.2 discusses some of the existing information hiding techniques in steganography to enable secure information transmission over the essential communication network.

2.1 Cryptography based Techniques

We believe that cryptographic devices realized on embedded methods. In this section, a number of papers are reviewed which have worked on security parameter for cloud computing.

Sakinah Ali Pitchay, et al. [37] proposed a concept which employed AES and RSA using USB device. In the cloud, all files are encoded until the univbersal serial bus (USB) device was plowed into the computer. In this approach, system sensed the universal serial bus (USB) that comprised of the isolated key and uses the files that was copied from the cloud.

Navia Jose, et al. [23], provides a technique by the use of Rivest Shamir Adleman (RSA) algorithm and MD5 to construct a protected atmosphere for cloud computing. Authors were mainly worried about the user authentication and data protection.

As reported by Akshita Bhandari, et al.[9] introduced a model using data hashed message authentication codes (HMAC) and index building for determining the errors and raises the efficiency. They also evaluated the Performance of Encryption algorithms based on confidentiality, integrity and availability.

Ning Cao, et al. [10] proposed an idea to outline and explain privacy problems by

using multi-keywords ranked search over encrypted cloud information (MRSE). The suggested scheme probed security and efficiency guarantee. In the former system, the focus was on a single keyword search or a Boolean keyword search and search outcomes were sorted. The author proposed a scheme that presented less amount of overhead on calculation.

Raj kumar Chalse, et al. [11] focused about the safety in case of reliability which is furthermost significant characteristic in cloud computing situation. The author used demonstrable data possession scheme that reduced data chunk access and quantity of calculation on the client server to confirm the precision of users data in a cloud warehouse.

Ranjit kaur, et al. [27] had put the limelight on about the security by using Novel Encryption techniques. It limits unofficial objects to regulate the users data and offers defense in contradiction to numerous safety gaps.

Ashalathar.et al. [7] came with an idea of visualization technology. The main emphasis was on concentrated resource utilization and high flexibility. Since visualization allow multiple users to share a physical server.

Mohammed A. Al Zain, et al.[4] proposed a novel model MCDB and also adopted a TMR method which improved the proposed cloud computing and enhanced security aspect. The main concern was on data privacy and in addition to reliability and user-friendliness.

Randeep Kaur, et al. [26], had focused on the security issues of cloud. They presented an idea of defining two techniques: pixel key pattern and image steganography technique. The main concern was to preserve confidentiality and integrity. With this level of issues in cloud computing, an organization agreed a decision that was based on benefits to risk ratio. Since the use of the above mentioned techniques can encrypt the original data so that the confidentiality of data can be achieved.

Justin LeJeune, et al.[33], suggested a noval security scheme for an account recovery of files which are stored on the cloud. MIST and Malachi were the two algorithms used to protect customers data through account security. The main fo-

cus was to keep the private data stored more efficiently as it offered an innovative methodology of shielding accounts in systematic logins.

Shipra Shukla, et al. [41] developed security policies for cloud computing system in the multiple levels against threats, risk and vulnerability. The author proposed a technique called object oriented technology to provide the cloud environment which was more reliable and trustworthy. This approach was able to overcome the security and compliance issues and provided organization issues.

Divya Prathana Timothy, et al. [45] , work provided the safety for the data that is movable over internet so that any intruder is not able to alter the data in advance. Authors provide more trustworthy, precious and harmless atmosphere for cloud computing with use of combination of blowfish symmetric and RSA algorithm. The usage of above mentioned technique was able to reduce or overcome the issues of data security and primary issues in cloud.

Table 2.1: Cryptography Based Classification

Author	Technique Used	Parameters	Advantages	Challenges
Randeep Kaur et al. [14](2015)	Pixel Key Pattern and Steganography	Confidentialty.	Reduce default rate, Localization of points and Distinct reaction to an edge.	Ethical Challenge.
Navia Jose et al. [6](2013)	Three layer architecture i.e. MD5 and RSA	User Authentication,Data Protection.	Fast recovery of data.	Separation of Sensitive Data and Access Control.
Divya Prathana Timothy et al. [13](2017)	Blowfish and RSA and SHA-2	Data confidentiality Authentication.	High security, proper network access and storage application.	Key management becomes complicated and time consumption.
Justin LeJeune et al. [8](2016)	MIST and Malachi	Data Integrity.	Account Recovery and protecting accounts for regular logins.	Zero confirmation after submitting of three Q and A.

to be cont'd on next page

Table 2.1: Cryptography Based Classification (Cont.)

Author	Technique Used	Parameters	Advantages	Challenges
Ning Cao et al. [4](2015)	MRSE	Performance, system usability and scalability.	Less overhead on calculation	Control search access are not within the possibility
Shipra Shukla et al. [12](2012)	Object Oriented Technique	Reliability and Trustworthy.	Provide clients with maximum visibility into the security.	Operational and management security controls.

The Table 2.1 critical analysis shows that combination of symmetric and asymmetric cryptography algorithms are used to provide confidentiality and authentication in cloud.

2.2 Steganography based Techniques

These illustrates several data hiding techniques in steganography to permit the secure transfer of critical data over the unsecure network. Steganography is sometimes erroneously confused with cryptography, but there are some distinguished differences between the two. In some conditions, steganography is mostly preferred to cryptography. Steganography is a useful method for storing sensitive information and provides an additional layer of protection and reduces the chance of detection. There are numbers of steganography embedding techniques offered in the literature.

2.2.1 Data hiding based on different Puzzles:

Chin-Feng lee, et al.[32] presented an information hiding scheme depend on magic matrix and concealed the confidential information that will be carried out by two cover pixels produced from square template to achieve the high embedding capability. The former system was focused on keeping good visual perception. The authors proposed a scheme that presented high embedding capacity of 2 bits per pixels and average PSNR of 44.7db.

C-F Lee, et al. [32] offered an information hiding system depend on magic matrix to change each cover pixel with the help of pencil shaped pattern to hide the secret information. In addition, the suggested scheme ensured high embedding capability of 2 bits per pixel and average PSNR of 44.7db. The author presented good image quality of stego image.

Ching-Chun Chang, et al. [12] introduced a well-known technique for hiding data named as Turtle Shell. In this scheme, hidden bits were implanted into cover pixel stream by generating a reference table. By using proposed scheme, the stego-image generated could exactly be related to cover image. The results ensured the high image quality and high embedding capacity.

The authors Kurup, et al. [30], used octagonal shape for data embedding capacity as compared to the other shapes. The magic square technique is used for scramble the secret data. The 4 bit LSB technique is used for data hiding.

Bin-Bin Xia, et al. [46] presented data embedding technique by using 3-D Sudoku. The proposed scheme can embed a 6 bit of secret data into 3 pixels and pixels of cover image are changed in 8x8 plane or 4x4x4 sub cube. The former technique was focused on keeping high security and improving the image quality of average of 41db. Therefore, embedding capacity of scheme was also increased.

Xiao-Zhu Xie, et al. [47] defined data hiding technique by using 2-layer Turtle Shell Matrix based technique. The former scheme has proposed an extra attribute which was represented by four-ary digit that was given to each elements of matrix with similar division. These scheme aimed to achieve higher embedding capacity up to 2.5 bits per pixels by embedding 2 more bits into each pixel value pair and also increased visual quality.

B. Santhi, et al. [40] introduced embedding in medical images by using unique key generation based on Sudoku Puzzle scheme. The edge pixels of cover image were used and LSB of pixels were modified by XOR coding based on embedding of secret data and generation of key. In this scheme, embedding of data was done in different planes of RGB which improved embedding capacity. The former methodology has achieved maximum PSNR of 87.5325 and gave high level of

security and imperceptibility.

The authors En-Jung farn and Chaur-Chin Chen, [13], used jigsaw puzzle for data embedding. Their experimental results show that their technique is robust to format and loss compression and undetectable under visual attacks.

Ijeri, et al. [20], used 9x9 Sudoku puzzle as reference matrix for data embedding and improved 4.5bits/pixel as compared to existing technique C. Chang et al. (3bits/pixel). To improve security and robustness data encryption and compression techniques also applied before data embedding.

The authors K.M. Jeevan and S. Krishna Kumar [21], are used pseudo-hexagonal approach for data hiding. They have well explained characteristics of hexagonal shapes selection such as symmetricity,high pixels, constant connectivity, and high effectiveness in place of other shapes. The LSB technique is used for data hiding.

2.2.2 Data hiding using different Techniques

J. Jennifer Ranjani, et al. [38] presented a pseudo magic square for data hiding by using the knights move method. By using the proposed method, the momentous property is used to generate one stable model to an embedding parameters. From performance analysis, the suggested algorithm is aimed to achieve high payload but also improved the security by using randomizing secret bits with less distortion.

Gyan Singh Yadav, et al. [48] have suggested another information hiding scheme depend on key and an embedding pattern generated through mid-point cycle algorithm. This proposed scheme that defined a secret key used for hiding secret data either in image or in text by ensuring secure locations. The main key feature of this scheme is to provide high security by changing in one bit of key and in LSB position, the security location of secret data has been changed. Thus, it was difficult to retrieve the hidden data by using guess key.

Embrahim Alrashed, et al. [3] gave a scheme by introducing an un-patterned quadric embedding result with unbounded parameters using the traditional LSB

insertions. The embedding technique used the data dependent and non-bounded process for building decoding infinite. The proposed approach reduced a noise rising while embedding of secret data by reducing modified bits. These can be possible by using Hungarian algorithm to improve security and value of PSNR and SNR.

Swati Goel, et al. [15] developed a concept which employed Integer Wavelet Transform(IWT), LZW compaction and changed pixel indicator techniques, the secret data was compressed using LZW algorithm then further transformation can be done using LSB of high integer wavelet transform(IWT) which can be done using changed pixels. These methods have improved the robustness and imperceptibility of image and also gave better PSNR.

K. Muhammad, et al. [35] proposed an idea to outline and explained security concern by using Cyclic Steganographic technique for various color images based on randomization. The author has provided both Subjective and Objective analysis depending on various parameters such as PSNR, MSE and histogram changeability. These can be done in Randomized Cyclic Manner and proposed results gave improvements in terms of security, robustness and imperceptibility.

Wein Hong, et al. [18] gave an another information hiding scheme depend on pixel pair matching. The proposed scheme used values of pixel pair as a referred position and found a position in an adjacent sets of the pixel pair according to a smallest notational system. These scheme was not only improved low payload problem but also offered safe communication.

Qiang Jin, et al. [22] proposed data embedding technique to hide a secret message by using Particle Swarm Optimization(PSO) to further minimize the alteration of cover image depending on Turtle Shell Pattern. These scheme has provided multi-layer security in which firstly matrix was generated depending on turtle shell. Further, the value of matrix was repeated by near optimal table to improve modification in the image. The results have showed that a method had high image perception and improved PSNR value.

Fei Peng, et al. [36] presented data embedding scheme based on Integer Trans-

form(IT) and Adaptive embedding. The proposed scheme allowed embedding of message bits into smooth areas by selecting different blocks. Therefore, the suggested scheme aimed to achieve high embedding capability of 2.17 bpp and improved PSNR value of 20.71db while having low computational complexity.

Gyan Singh Yadav and Aparajita Ojha [48], designed a mid-point circle generation algorithm in which they have used a hidden key to produce secure information hiding locations on the pixels of the image. The algorithm provides large key space and fast computation. The algorithm provides high security and robustness.

The authors are shown that with just changing 1-bit in the key, the 50 Nilizadeh, et al. [6], is designed matrix pattern based approach for the information hiding. In initial process, the color picture is split into RGB plane and split into the non-overlapping bits. Further, dierent unique 95 adaptive sized matrix pattern is produced based on the green plane 4th and 5th bit and which are alloted to 95 English keyboard symbols. The blue plane is used for hidden data hiding by combining matrix pattern that is assigned to symbols of the hidden data. Their analysis has shown that their technique resistant to various attacks which includes regulate singular, sample pair, steganalysis attack and PVD. Their proposed technique improved capacity by 27bpp.

Table 2.2: Steganography Techniques Classification

S.No.	Author	Year	Technique Used
1	Chin-Feng lee, et al.[33]	2017	Magic matrix
2	C-F Lee, et al.[34]	2018	Magic matrix
3	Ching-Chun Chang, et al.[35]	2014	Turtle Shell
4	Kurup, et al.[36]	2015	Octagonal shape
5	Bin-Bin Xia, et al.[37]	2016	3-D Sudoku

to be cont'd on next page

Table 2.2: Steganography Techniques Classification (Cont.)

S.No.	Author	Year	Technique Used
6	Xiao-Zhu Xie, et al.[38]	2018	Two-layer Turtle and Shell Matrix based scheme
7	B. Santhi, et al.[39]	2016	Sudoku Puzzle scheme
8	En-Jung farn, et al.[40]	2009	Jigsaw puzzle
9	Ijeri, et al.[41]	2016	9x9 Sudoku puzzle
10	K.M. Jeevan, et al.[42]	2018	Pseudo-hexagonal approach
11	J. Jennifer Ranjani, et al.[43]	2017	knights move algorithm
12	Gyan Singh Yadav, et al.[44]	2017	Mid-point cycle algorithm
13	Embrahim Alrashed, et al.[45]	2017	Blowfish symmetric and RSA algorithm
14	Swati Goel, et al.[46]	2014	IWT, LZW compression and modified pixel indicator techniques
15	K. Muhammad, et al.[47]	2014	Cyclic Steganographic technique
16	Wein Hong, et al.[48]	2012	Pixel pair matching
17	Qiang Jin, et al.[49]	2017	Particle Swarm Optimization(PSO)
18	Fei Peng, et al.[50]	2012	Integer Transform and Adaptive embedding
19	Gyan Singh Yadav, et al. [51]	2017	Mid-point circle generation algorithm
20	Nilizadeh, et al. [52]	2013	Matrix pattern based approach

The analysis and research done by different authors in cryptography and steganography to provide secure communication discussed in the above sub-sections have been summarized in Table 2.2

Chapter 3

Problem Statement

3.1 Problem Statement

In the cloud computing, most of the sensitive data is uploaded, processed and downloaded by number of users. Hence, data security on the cloud is a big concern. The cloud database is secured using the encryption algorithm or by embedding the secret data inside a cover media that provides imperceptibility to un-authorized users. In the encryption algorithm, AES is the most used algorithm and LSB technique is used in the steganography. To improve the capacity, number of data bits/pixel is increased in the cover pixels that also enhanced the variability and gives attention to the attacker. Hence, robust steganography data embedding technique is required to secure the data. In addition, encryption of the sensitive data before data embedding also improves the security.

3.2 Research Gaps

The literature survey shows that there are number of issuses on cloud such as network, Virtual machine(VM), storage and application based attacks [1]. To overcome these attacks cryptography and steganography algorithms are used in the cloud for security purposes [2]. In cryptography and steganography, AES and LSB data hiding are the most used algorithm [17]. To improve the capacity, security and visual quality in steganography algorithm, authors are worked on selecting symmetric shapes [30] [21] (that includes hexagonal and octagonal), different puzzles [20] [13] and modified LSB technique [3]. Based on this analysis found that the authors used static symmetric and puzzle for data hiding.

The puzzle index information is communicated separately or synchronized the transmitter and receiver.

- How to design dynamic symmetric and puzzle which provide security and difficult to steganalysis.[21]

- How puzzle indexed is communicated with secret data.[20]

3.3 Research Objectives

- To study and explore various cryptography and steganography techiques for data hiding.
- To proposed and design data embedding technique for Image steganography in cloud computing.
- To validate the performance analysis for the security algorithm and comparative analysis with the proposed technique are done by using the parameters such as MSE, PSNR and Embedding capacity.

Chapter 4

Research Methodology

In this chapter, detail description of the proposed technique and its components are given. In the proposed technique, multi-layer security system is designed using cryptography and steganography algorithms. In the proposed technique, the secret data is encrypted using AES approach. Next, the cover image is read and symmetric shapes that includes rhombus, hexagonal, and octagonal are determined. Further, the Nonogram puzzle is formed inside symmetric shapes for data hiding. Also, one random number generator is used in the proposed technique which determine different shapes and nonogram puzzle for data hiding as shown in Figure 4.1 and Pseudocode is explained in Algorithm 4.1. The components plays an important role in the proposed technique that are explained below.

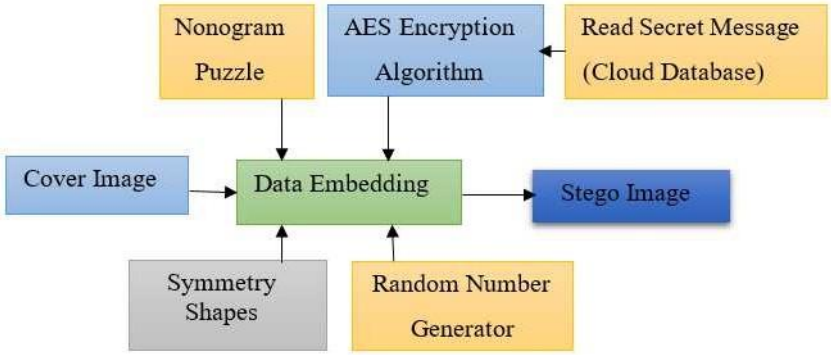

Figure 4.1: Proposed Steganography Technique for Data Hiding

Algorithm 4.1 Pseudocode for Data Hiding Technique

- Read the cover image.
- Read the block from the image.
- Two random number is generated for determine symmetric shape and Nonogram Puzzle
- Determine pixels, which contribute in the symmetric shape.
- Design the Nonogram Puzzle inside symmetric Shape.
- The secret data bits hiding is done in the pixels, which contribute in the puzzle.
- The indexes are embedded in the symmetric shape.
- Reconstruct the image.
- The performance analysis is done using Avalanche Effect, Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR).

4.1 Symmetric Shapes

The symmetric shapes are covered with maximum pixels, connectivity, and best for human perception as compared to other shapes. Therefore, symmetric shapes are deployed in steganography for data hiding. The authors used hexagonal and octagonal shapes for data hiding.[32][21] In the proposed technique, the cover image is split into blocks (8X8) and three symmetric shapes that includes rhombus, hexagonal, and octagonal are formed in the block.

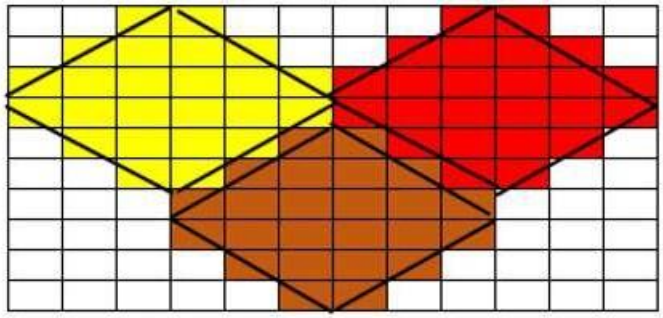

Figure 4.2: Rhombus Shape Formation Inside the Cover Image

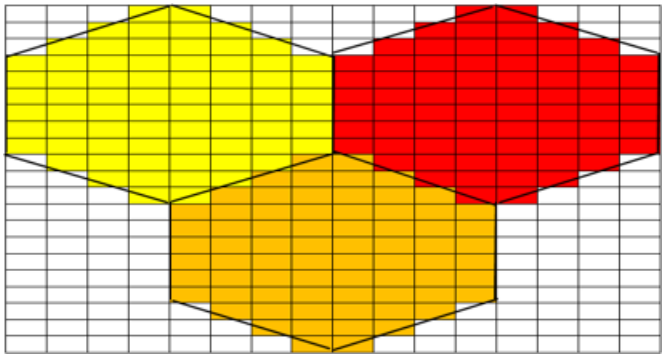

Figure 4.3: Hexagonal shape Formation Inside the Cover Image

The symmetric shapes provide maximum area and connectivity as compared to the others shapes. In the Figure 4.2, Rhombus shape are formed in the cover blocks. In the Figure 4.3, the hexagonal shapes are formed in the cover blocks and cover more pixels as compared to the Rhombus shape. In the Figure 4.4, the octagonal shape is formed into the blocks and approximate all pixels of the blocks are covered. In the proposed technique, a random number generator is used which give random number for select symmetric shapes for data hiding.

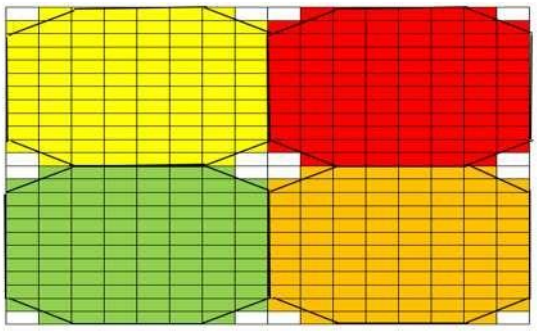

Figure 4.4: Octagonal Shape Formation Inside the Cover Image

4.2 AES Algorithm

Advanced Encryption Standard is block cipher in which secret data bits are break into fixed block and encryption algorithm is applied on each block. The block size 128 and three key variant 128, 192, 256 bits are available for AES algorithm.

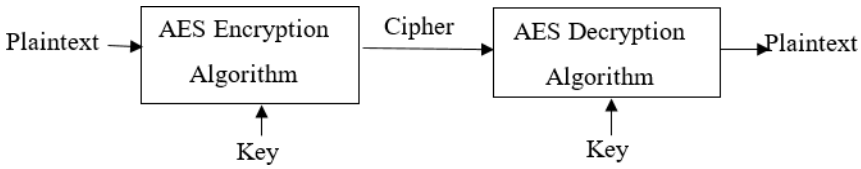

Figure 4.5: Block Diagram for Encryption and Decryption

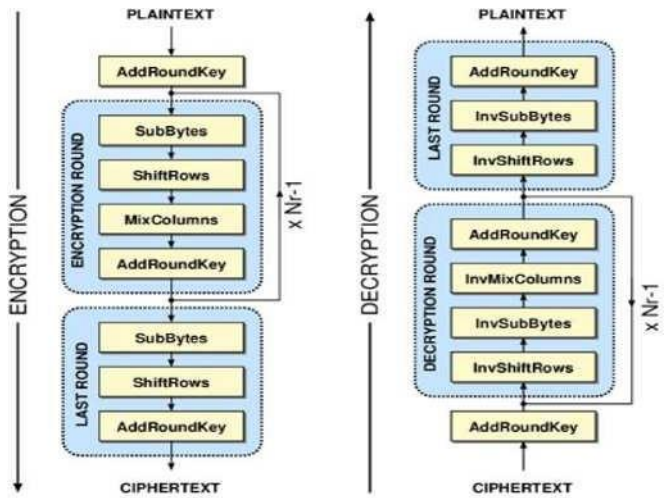

Figure 4.6: AES Encryption and Decryption Process

In addition, AES has three variant of rounds 10, 12, 14 according to key variant [28].The AES algorithm is symmetric cipher and same key is used for encryption

and decryption purposes as shown in Figure 4.5. The AES contains 4 layers (which includes S-Box, Shift-Row, Mix Column, and Add Round Key) in each round as shown in Figure 4.6 . In the AES algorithm, S-box layer is provided confusion and Shift row, Mix Column is provided diffusion in the logic. The AES Encryption Algorithm pseudocode is given in the Algorithm 4.2 and key scheduling in Algorithm 4.3 . In our work, the 128-bit block and key size is used. The data is arranged into 4X4 matrix and each element of matrix has 1-byte size.

Algorithm 4.2 Pseudocode for Encryption

- Read the secret message and divided into 128-bit blocks.
- Read the 128-bit secret key.

for i=1 to 9 rounds do

- The 4 layers (s-box, shift-row, mix-column, add-round key) applied.
- in the 10 round
- The 3 layers (s-box, shift-row, add-round key) applied.
- The cipher text is produced after 10 rounds and in the next block, same scenario is follow.

end for

Algorithm 4.3 Pseudocode for Key Scheduling

- Read the 128-bit key and arrange into 4x4 matrix.
- The 4th Column of the matrix is circular Rotated and passed through S-Box.
- The next key matrix is generated as
- Key Column1= (original Key Column1 XOR Updated 4th Column Value) XOR R-Constant
- Column2= Key Column1 XOR Original 2nd Key Column
- Column3= Key Column2 XOR Original 3rd Key Column
- Column4= Key Column3 XOR Original 4th Key Column

4.3 Nonogram Puzzle

The Nonogram is a logical game and most liked in Japan and Netherlands as shown in Figure 4.7. The nonogram is an NP hard problem. In the Figure 4.7 the left of a row and top of the column represents the length of black runs in the column or row respectively.

The aim is to paint cells to form a image that fulfiles the following constraints:

- Each cell must be colored (black) or left empty (white).

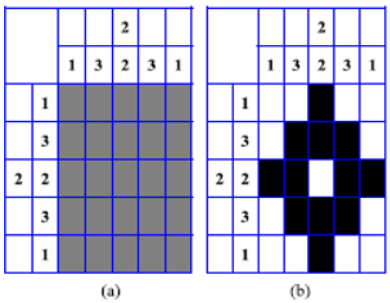

Figure 4.7: Nonogram Puzzle (a) Puzzle (b) Solution of the Puzzle

- If a row or column has k numbers: s1, s2,sk , then it must contain k black runsthe first (leftmost for rows/topmost for columns) black run with length s1, the second black run with length s2, and so on.
- There should be at least one empty cell between two consecutive black runs.

4.4 Nonogram Puzzle Formation inside Symmetric Shapes

In the proposed technique, different Nonogram puzzle is formed inside symmetric shapes for data hiding as shown in Figure. In the Figure 4.8, the Nonogram puzzles is formed in the Rhombus shape. The pixels are contributed in the Rhombus shapes are less. Therefore, small puzzles are formed. In the Figure 4.9 , the hexagonal shapes are covered more pixels than Rhombus shape so large puzzles are formed. In the Figure 4.10, the octagonal shapes are formed which cover all pixels of the block so provides maximum space to form complex puzzle as compared to Rhombus and Hexagonal shape. From the analysis, found that small nonogram puzzle is formed in the rhombus shape, moderate in hexagonal, and high and complex in octagonal shape. The octagonal shape has high embedding capacity as compared to rhombus and hexagonal shape.

In the proposed technique, different nonogram puzzle is formed and one look-up table is designed. A random number is generated which selects one shape and puzzle and data embedding process is done.

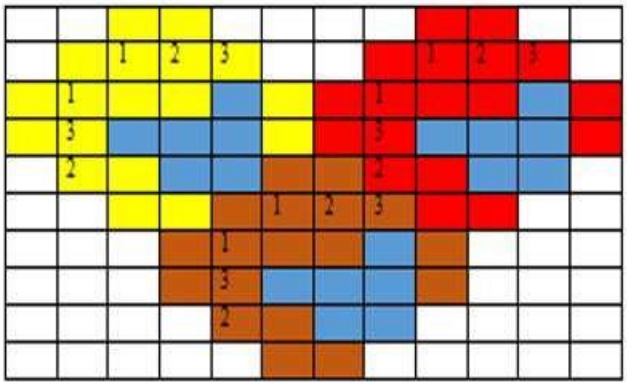

Figure 4.8: Nonogram Puzzle in Rhombus Shape

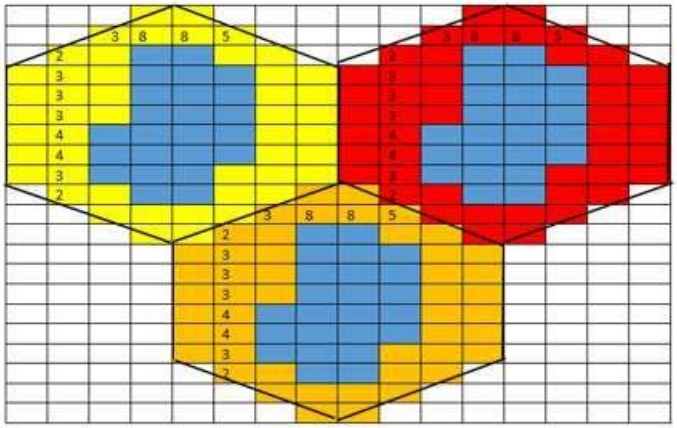

Figure 4.9: Nonogram Puzzle in Hexagonal Shape

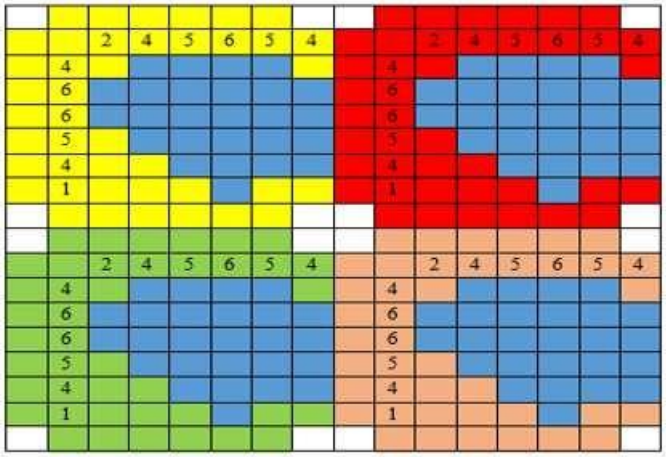

Figure 4.10: Nonogram Puzzle in Octagonal Shape

4.5 Data Embedding Techniques

In the spatial domain, least significant bit (LSB) technique is the most applied technique for data hiding as shown in Table 4.1 . In the LSB approach, the secret data is concealed in the LSB bits of the cover pixels [17].

Table 4.1: LSB Technique

Cover Pixels			
10101100	00110011	00011001	11111111
00110011	10101010	01010010	00000001
Secret Data:	10101101		
Stego Pixels			
10101101	00110010	00011001	
00110011	10101011	01010010	00000001

The LSB technique have 1-bit variability after data hiding and required 8 pixels to store 1byte. There are number of variant of 1 bit LSB technique available such as 2 bit, 4 bit LSB technique. The bits hiding per pixel if increased then data capacity increases, required less pixels for data hiding, and increase the variability in the stego image.

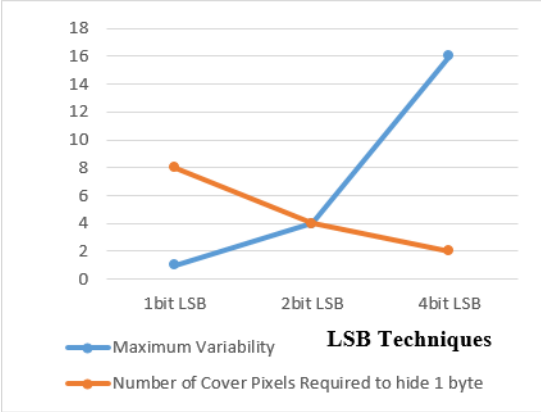

Figure 4.11: Different LSB Techniques Vs Variability and Number of Pixels Required

In the Figure 4.11 plot the different LSB technique vs variability and number of pixels required. In this paper, 2-bit LSB technique is selected for data hiding.

Chapter 5

Experimental Results

In this chapter, the proposed technique is simulated and performance analysis is done to show the robustness against visual attacks. The proposed technique is coded in MATLAB 2013a. The standard dataset cover images are taken for data hiding [16]. The cover dataset images are lena, baboon, pepper, advertisement, akiyo, jet plane, boat. The resolution of these images are 128X128 and JPG format.

In the proposed technique, the AES algorithm is applied on the secret data for encryption purposes. The AES algorithm security measure is done using avalanche effect. The avalanche effect parameter is defined that if any one bit is changed in the key then 50% cipher bits are changed ideally. The avalanche effect is measured using equation 5.1.

$$AvalancheEffect = \frac{TotalNumberofBitchanged}{TotalNumberofBits} * 100 \qquad (5.1)$$

Plaintext	Cipher	Avalanche Effect
1 5 9 13 2 6 10 14 3 7 11 15 4 8 12 16	78 216 249 230 118 40 39 222 84 90 246 204 104 230 197 107	50.23
1 4 9 13 2 6 10 14 3 7 11 15 4 8 12 16	39 97 88 63 61 146 213 201 73 205 117 84 78 213 132 210	

Figure 5.1: Avalanche Effect

In the Figure 5.1 for the one block of secret message avalanche effect is shown. The result show that AES have approximate 50% avalanche effect. Next, the symmetric shape and nonogram puzzle is determined and data embedding 2-bit

LSB technique is applied.

Cover Image	Stego Image for Rhombus Shape	Stego Image for Hexagonal Shape	Stego Image for for Octagonal Shape
 Lena.jpg			
 Baboon.jpg			
 Pepper.jpg			

Figure 5.2: Comparative Analysis between Cover and Stego Images

The visual comparative analysis between cover and stego image is shown in Figure 5.2. The Figure 5.2 shows that there is no visual impact after data embedding in the stego image.The cover image is tranformed into Red, Green and Blue plane Then it would result in stego image. Further,this resulting stego image is similar to cover image.

The proposed technique performance analysis is done based on Mean Square Error, Peak Signal to Noise Ratio [15], and embedding capacity. These parameters are explained below.

- Mean Square Error The Mean Square Error is used to determine pixel variability between stego image and cover image and calculated using equation 5.2.From Figure 5.3 ,it shows that octangonal has high MSE has compared to other symmetric Shapes.And the values of MSE for different shapes as shown in Table5.1.

$$MSE = \frac{\overleftarrow{M}_{x=1} \overleftarrow{N}_{y=1} (cover(x, y)) - stego(x, y)^2}{M * N} \tag{5.2}$$

Here, M, N is the size of the cover image and Cover and Stego is the input and output image after the data embedding.

Table 5.1: MSE for Different Cover Images

Cover Pixels	MSE Rhombus	MSE Hexagonal	MSE Octagonal
Lena.jpg	0.0161	0.1695	0.2882
Barbara.jpg	0.0131	0.1691	0.2882
Pepper.jpg	0.0161	0.1630	0.2750
Baboon.jpg	0.0142	0.1644	0.2861
Flowers.jpg	0.0149	0.1780	0.2969

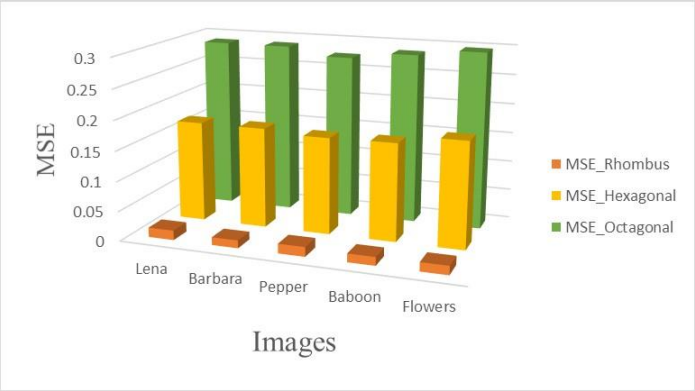

Figure 5.3: MSE for Different Cover Images

- Peak Signal to Noise Ratio The Peak Signal to Noise Ratio parameter is used to determine distortion of stego image and calculated using equation 5.3.

$$PSNR = 10 * \log \frac{255 * 255}{MSE} \tag{5.3}$$

Table 5.2: PSNR for Different Cover Images

Cover Pixels	PSNR Rhombus(db)	PSNR Hexagonal(db)	PSNR Octagonal(db)
Lena.jpg	66.0590	55.8392	53.53
Barbara.jpg	66.9506	55.8502	53.54
Pepper.jpg	66.0590	56.0099	53.74
Baboon.jpg	66.6201	55.9726	53.57
Flowers.jpg	66.4011	55.6271	53.40

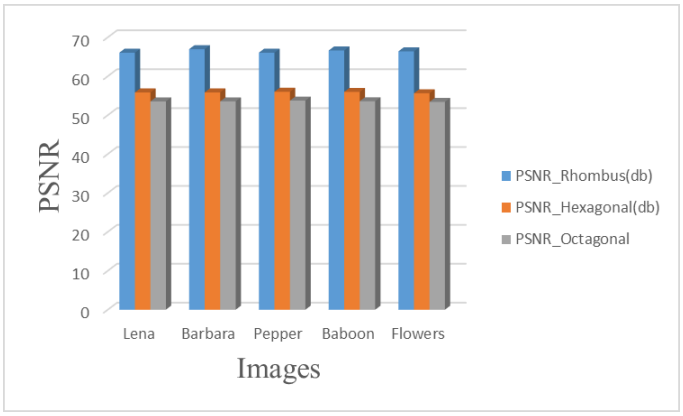

Figure 5.4: PSNR for Different Cover Images

In the Figure 5.4 for the cover image Lena.jpg the PSNR of RGB plane is calculated and founds that Rhombus shape has higher PSNR as compared to Hexagonal and Octagonal shape. And the values of MSE for different shapes as shown in Table 5.2.

- Embedding Capacity: The total number of bits are embedded in the cover image and calculated using equation 5.4.

$$EmbeddingCapacity = \frac{TotalNumberofbitsareEmbedded}{theCoverImage} \quad Sizeof \tag{5.4}$$

According to Embedding capacity, Octagonal shape has higher MSE as compared to Rhombus and Hexagonal shape wheras PSNR has decreased for octagonal shape which is shown in Figure 5.5.

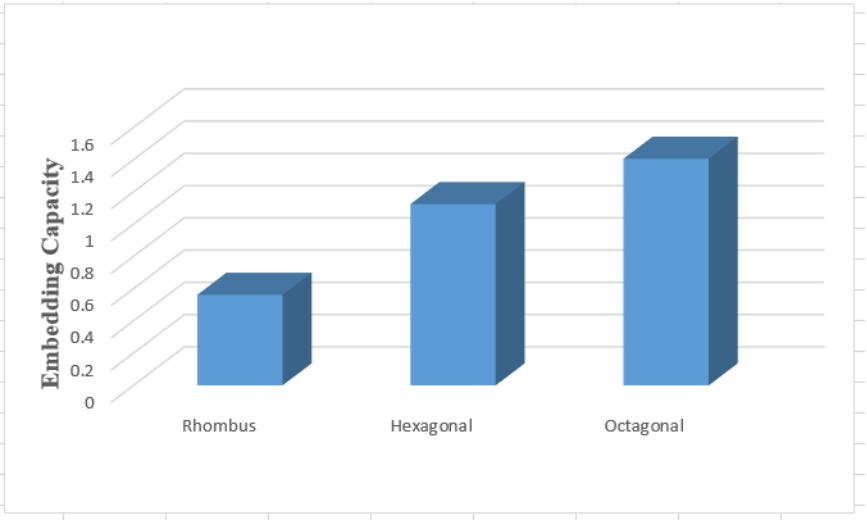

Figure 5.5: Different Shapes Vs Embedding Capacity

In the Figure 5.6 illustrates the comparitive analysis between the different images having same embedding capacity. The analysis shows that high data embedding in the cover image degrade the quality of stego image in the terms of PSNR. The 2 bit LSB technique is used in existing and proposed technique.The results show that proposed technique have higher PSNR as compared to existing one[32].

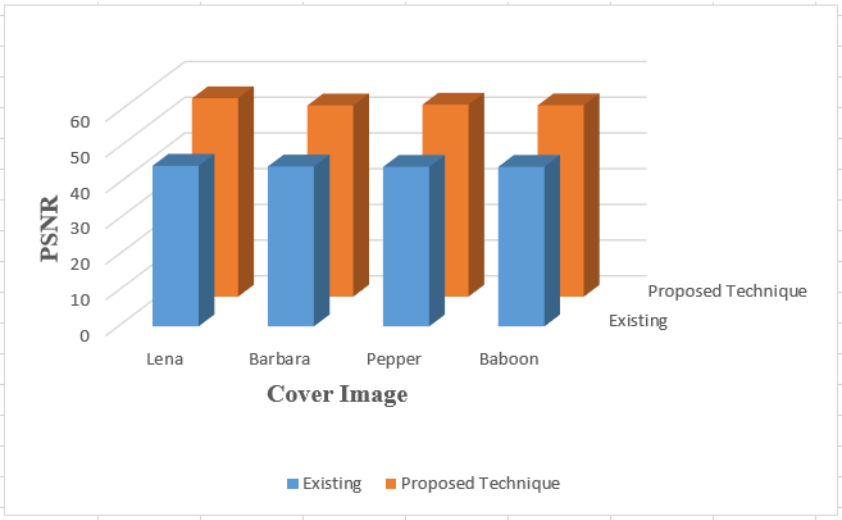

Figure 5.6: Comparative Analysis with Existing Technique[32]

Chapter 6

Conclusion and Future Work

In our work, multi-layer security system is designed for cloud computing data security. In the proposed technique, Data embedding have been used for hiding the information in an images by using the steganography and cryptography techniques in a hybrid way. The cryptography algorithms are used in steganography to achieve this target. The AES algorithm that is most suitable and preferred algorithm used for secret data encryption and its performance analysis is done in terms of avalanche effect and found that AES is provided 50% avalanche effect. Next, based on the random number generator, random symmetric shape (which includes Rhombus, Hexagonal, and Octagonal) and Nonogram puzzle is selected. The encrypted secret data is hiding in cover image using steganography algorithm. The 2-bit LSB technique is used for data hiding and improve capacity. The proposed technique performance analysis is done in terms of visual quality between cover and stego images and measures performance parameters such as Mean Square Error, Peak Signal to Noise Ratio, embedding capacity. The simulation result shows that Rhombus shape on average achieved 66dB, Hexagonal shape 55dB, and Octagonal shape 53dB PSNR. Moreover, the embedding capacity is highest in octagonal shape 1.40625bpp and lowest in Rhombus 0.5625bpp. From the analysis of PSNR and embedding capacity found that increasing embedding capacity degrade the quality in terms of PSNR.

6.1 Future Work

In steganography, Least Significant Bit(LSB) is mostly used technique which covers LSB pixels that are replaced with data bits without pre-processing in which cover pixels LSB bits are suitable for data hiding. It influences or degrades the visual quality. To improve visual quality, the optimization techniques are applied on cover pixels to search suitable pixels bits for data embedding. Next, the video will be used as cover media that improves security and capacity. Further, data hiding directly in cover pixels influence the noise. Hence, the error correction code should be added in the data bits before data embedding.

References

[1] "A survey of security issues for cloud computing," *J. Netw. Comput. Appl.*, vol. 71, no. C, pp. 11–29, Aug. 2016. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2016.05.010

[2] D. F. S. Abed, "A proposed method of information hiding based on hybrid cryptography and steganography," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 4, 2013.

[3] E. Alrashed and S. S. Alroomi, "Hungarian-puzzled text with dynamic quadratic embedding steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 2, pp. 799–809, 2017.

[4] M. A. AlZain, B. Soh, and E. Pardede, "A new approach using redundancy technique to improve security in cloud computing," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*. IEEE, 2012, pp. 230–235.

[5] A. J. Amalraj and J. J. R. Jose, "A survey paper on cryptography techniques," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 8, pp. 55–59, 2016.

[6] F. N. Amir and A. R. N. Nilchi, "Steganography on rgb images based on a" matrix pattern" using random blocks," *International Journal of Modern Education and Computer Science*, vol. 5, no. 4, p. 8, 2013.

[7] R. Ashalatha, J. Agarkhed, and S. Patil, "Network virtualization system for security in cloud computing," in *Intelligent Systems and Control (ISCO), 2017 11th International Conference on*. IEEE, 2017, pp. 346–350.

[8] A. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the internet of things (iot) critical infrastructures," *Information Security Journal*, vol. 25, no. 4-6, pp. 197–212, 12 2016.

[9] A. Bhandari, A. Gupta, and D. Das, "A framework for data security and storage in cloud computing," in *Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on*. IEEE, 2016, pp. 1–7.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 1, pp. 222–233, 2014.

[11] R. Chalse, A. Selokar, and A. Katara, "A new technique of data integrity for analysis of the cloud computing security," in *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*. IEEE, 2013, pp. 469–473.

[12] C. C. Chang, Y. Liu, and T. S. Nguyen, "A novel turtle shell based scheme for data hiding," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*. IEEE, 2014, pp. 89–93.

[13] E.-J. Farn and C.-C. Chen, "Jigsaw puzzle images for steganography," *Optical Engineering*, vol. 48, no. 7, p. 077006, 2009.

[14] P. Goel, "Data hiding in digital images: a steganographic paradigm," *Indian Institute of Technology Kharagpur*, 2008.

[15] S. Goel, P. Kumar, R. Saraswat, C. N. M. Tech *et al.*, "High capacity image steganography method using lzw, iwt and modified pixel indicator technique," 2014.

[16] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168–187, 2012.

[17] M. Hariri, R. Karimi, and M. Nosrati, "An introduction to steganography methods," *World Applied Programming*, vol. 1, no. 3, pp. 191–195, 2011.

[18] W. Hong and T.-S. Chen, “A novel data embedding method using adaptive pixel pair matching,” *IEEE transactions on information forensics and security*, vol. 7, no. 1, pp. 176–184, 2012.

[19] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, “Image steganography in spatial domain: a survey,” *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[20] S. Ijeri, S. Pujeri, B. Shrikant, and B. Usha, “Image steganography using sudoku puzzle for secured data transmission,” *International Journal of Computer, Applications (0975-888)*, vol. 48, no. 17, 2012.

[21] K. Jeevan and S. Krishnakumar, “Image hiding technique using a pseudo hexagonal structure approach,” *International Journal of Computers and Applications*, pp. 1–8, 2018.

[22] Q. Jin, Z. Li, C.-C. Chang, A. Wang, and L. Liu, “Minimizing turtle-shell matrix based stego image distortion using particle swarm optimization,” *Int. J. Netw. Secur*, vol. 19, pp. 154–162, 2017.

[23] N. Jose and C. Kanmani, “Data security model enhancement in cloud environment,” *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, pp. 2278–0661, 2013.

[24] A. Joseph, R. Dr, and V. Sundaram, “Cryptography and steganography a survey.”

[25] P. S. Kale and M. M. Bartere, “Separable reversible scheme for data hiding in image,” *International Journal of Engineering Science*, vol. 5343, 2016.

[26] R. Kaur and J. Kaur, “Cloud computing security issues and its solution: A review,” in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*. IEEE, 2015, pp. 1198–1200.

[27] R. Kaur and R. P. Singh, “Enhanced cloud computing security and integrity verification via novel encryption techniques,” in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 1227–1233.

[28] S. Kaur and S. Kaur, “Comparative analysis of lightweight cryptography algorithms for smart grids,” in *Signal Processing, Computing and Control (ISPCC), 2017 4th International Conference on*. IEEE, 2017, pp. 564–567.

[29] A. Kumar and K. Pooja, “Steganography-a data hiding technique,” *International Journal of Computer Applications*, vol. 9, no. 7, pp. 19–23, 2010.

[30] S. Kurup, A. Rodrigues, and A. Bhise, “Data hiding scheme based on octagon shaped shell,” in *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*. IEEE, 2015, pp. 1982–1986.

[31] M. Kwiatkowska and L. Swierczewski. Steganography - coding and intercepting the information from encoded pictures in the absence of any initial information. [Online]. Available: https://lvee.org/en/abstracts/106

[32] C.-F. Lee and Y.-X. Wang, “An image hiding scheme based on magic square,” in *Awareness Science and Technology (iCAST), 2017 IEEE 8th International Conference on*. IEEE, 2017, pp. 301–305.

[33] J. LeJeune, C. Tunstall, K.-p. Yang, and I. Alkadi, “An algorithmic approach to improving cloud security: The mist and malachi algorithms,” in *Aerospace Conference, 2016 IEEE*. IEEE, 2016, pp. 1–7.

[34] R. J. Mstafa and K. M. Elleithy, “A video steganography algorithm based on kanade-lucas-tomasi tracking algorithm and error correcting codes,” *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10 311–10 333, 2016.

[35] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and R. J. Qureshi, “A secure cyclic steganographic technique for color images using randomization,” *arXiv preprint arXiv:1502.07808*, 2015.

[36] F. Peng, X. Li, and B. Yang, “Adaptive reversible data hiding scheme based on integer transform,” *Signal Processing*, vol. 92, no. 1, pp. 54–62, 2012.

[37] S. A. Pitchay, W. A. A. Alhiagem, F. Ridzuan, and M. M. Saudi, “A proposed system concept on enhancing the encryption and decryption method for cloud computing,” in *Modelling and Simulation (UKSim), 2015 17th UKSim-AMSS International Conference on*. IEEE, 2015, pp. 201–205.

[38] J. J. Ranjani, "Data hiding using pseudo magic squares for embedding high payload in digital images," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3715–3729, 2017.

[39] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 47–54, 2013.

[40] B. Santhi and B. Dheeptha, "A novel edge based embedding in medical images based on unique key generated using sudoku puzzle design," *SpringerPlus*, vol. 5, no. 1, p. 1670, 2016.

[41] S. Shukla and R. K. Singh, "Security of cloud computing system using object oriented technique," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*. IEEE, 2012, pp. 1–9.

[42] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[43] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer science review*, vol. 13, pp. 95–113, 2014.

[44] H. Tariq and P. Agarwal, "Secure keyword search using dual encryption in cloud: An approach," *International Journal of Computational Intelligence Research*, vol. 13, no. 5, pp. 1271–1282, 2017.

[45] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," in *Microelectronic Devices, Circuits and Systems (ICMDCS), 2017 International conference on*. IEEE, 2017, pp. 1–5.

[46] B.-B. Xia, A.-H. Wang, C.-C. Chang, and L. Liu, "An image steganography scheme using 3d-sudoku," *J Info Hiding Multimed Sign Proc*, vol. 7, no. 4, pp. 836–845, 2016.

[47] X.-Z. Xie, C.-C. Lin, and C.-C. Chang, "Data hiding based on a two-layer turtle shell matrix," *Symmetry*, vol. 10, no. 2, p. 47, 2018.

[48] G. S. Yadav and A. Ojha, “Secure data hiding scheme using shape generation algorithm: a key based approach,” *Multimedia Tools and Applications*, pp. 1–27, 2017.

List of Publications

International Journal

1. Surbhi singla, Anju Bala, *"Nonogram Puzzle using Symmetric Shape based Data Embedding Technique for Image Steganography"*, International Journal of Computer Science and Information Security(IJCSIS)[Accepted]

International Conference

1. Surbhi singla, Anju Bala, *"A Review: Cryptography and Steganography Algorithm for Cloud Computing"*, 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)[In Press]