TO PROPOSE FRAMEWORK FOR CLOUD DATA SECURITY

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

By

NIKITA MAHAJAN

11509912

Supervisor

MOHIT ARORA

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

April 2017

ABSTRACT

In recent years, cloud computing is being used everywhere and various frameworks has also been formed to secure the data. For cloud computing environments, secured and proper authentication is the most essential thing and due to its connection with external environment, user data is at high risk. To overcome that problem few techniques were proposed namely, Mutual Authentication and Out of Band Authentication. The problem which occurred by using these techniques were complexity, space utilization and execution time. Here, Steganography and light weight framework is proposed which will authenticate the user and also use authenticated keys for encryption of the data. According to this, the cloud has an architecture in which data is uploaded on the cloud servers after authenticating the clients. In this work the novel technique is proposed which will authenticate the user, where we will provide 2 step authentication and same authentication keys which were used for encryption of the message. This leads to reduction in encryption time and increase security. Steganography is the technique which hide sensitive information and generate final encrypted data. In the case of steganography the images are used to hide the sensitive text information. Here, LSB technique has also been applied which will access the textual features of the image to generate final stenographic image. Here, improvement in LSB technique has also been proposed which increase security, robustness and execution time of the algorithm.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled **"TO PROPOSE FRAMEWORK FOR CLOUD DATA SECURITY”** in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Mohit Arora. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University’s Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Nikita Mahajan

11509912

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**TO PROPOSE FRAMEWORK FOR CLOUD DATA SECURITY"**, submitted by **Nikita Mahajan** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

(Mohit Arora)

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: ________________

   HoD Name: ____________________

   Date: ___________________

2) **Neutral Examiners:**

   External Examiner

   Signature: _______________

   Name: __________________

   Affiliation: ______________

   Date: ___________________

   Internal Examiner

   Signature: _______________

   Name: __________________

   Date: ___________________

ACKNOWLDGEMENT

It is not until you undertake research like this one that you realize how massive the effort it really is, or how much you must rely upon the selfless efforts and goodwill of others. I want to thank them all from the core of my heart. I owe special words of thanks to my supervisor Mr. Mohit Arora for his vision, thoughtful counseling and encouragement for this research on **“TO PROPOSE FRAMEWORK FOR CLOUD DATA SECURITY”**. I am also thankful to the teachers of the department for giving me the best knowledge guidance throughout the study of this research. And last but not the least, I find no words to acknowledge the financial assistance & moral support rendered by my parents and moral support given by my friends in making the effort a success. All this has become reality because of their blessings and above all by the grace of almighty.

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

LIST OF FIGURES

Checklist for Dissertation-III Supervisor

Name: ___________________________ UID: ________ Domain: _____
Registration No: ____________Name of student: __________________

Title of Dissertation: ____

□ Front pages are as per the format.

□ Topic on the PAC form and title page are same.

□ Front page numbers are in roman and for report, it is like 1, 2, 3…….

□ TOC, List of Figures, etc. are matching with the actual page numbers in the report.

□ Font, Font Size, Margins, line Spacing, Alignment, etc. are as per the guidelines.

□ Color prints are used for images and implementation snapshots.

□ Captions and citations are provided for all the figures, tables etc. and are numbered and center aligned.

□ All the equations used in the report are numbered.

□ Citations are provided for all the references.

□ **Objectives are clearly defined.**

□ Minimum total number of pages of report is 50.

□ Minimum references in report are 30.

Here by, I declare that I had verified the above mentioned points in the final dissertation report.

Signature of Supervisor with UID

CHAPTER 1
INTRODUCTION

1.1 Cloud Computing

The outline which gives omnipresent, simple and on-request arrange access towards the mutual pool of assets is known as Cloud processing. The assets exhibit inside the pool is configurable registering assets which require negligible administration exertion from client end and furthermore don't require much correspondence with the administration gives. The development of different innovations which are assembled to manufacture an IT framework is known as distributed computing. The advances being used inside the distributed computing are not new and have been used from ages. Inside the name of distributed computing, every one of these administrations is simply to be made to use by the various clients show. In spite of the fact that, the Internet is the fundamental prerequisite for the cloud, in any case, it is not like the Internet and is a more extensive recorded when contrasted with the Internet. The use of innovation according to a prerequisite for any span is the fundamental capacity of the cloud. There is no compelling reason to introduce whatever other application on the desktop. Likewise, there is no compelling reason to pay for the application one needs to utilize. The applications required in the cloud can be either programming or framework based. Like the applications one uses the Internet, the cloud contains such IT plan which can be used by the necessity of the client. The cloud administrations are not confined to specific areas or regions. The client can get to the applications from any separation. The cloud-base administration can be gotten to by the client from anyplace. Taking after are the three different measures which help in choosing whether the given administration is a cloud-based administration or not [1].

i. The administration is open by means of a web program or web administrations API.

ii. Zero capital use is important to begin.

iii. You pay just for what you utilize.

There are different qualities of cloud which are enrolled and portrayed beneath:

1.1.1 On-Demand Self-Service

The processing abilities can be used by the administration purchaser by it selves. There is no need of any human cooperation with the specialist co-op here for getting to administrations, for example, server handling time and system stockpiling [2].

1.1.2 Broad Network Access

Different stages can without much of a stretch get to the cloud capacities which can be either equipment or programming, over the system

1.1.3 Resource Pooling

With the end goal of serving different customers with the assistance of a multi-occupant show, the different specialist co-ops' processing assets are pooled together. There is a doling out and reassigning of different physical and virtual assets in element way according to the request of the client. Inside the cloud-based application, multi-tenure is an imperative element [6]. The area autonomy highlight is critical here which empowers the client to get to the assets at different areas and not limit them. More elevated amount of reflection is to be guaranteed here amid the openness of assets at different areas [8].

1.1.4 Rapid Elasticity

There can be a speedier scaling all through the abilities and they can likewise be flexibly provisioned. There are boundless abilities to be provisioned here and at different moments they can be purchased by the client [10].

1.1.5 Measured Service

The assets are consequently controlled and advanced inside the cloud frameworks. The deliberate capacity is to be empowered here through which the assets are checked, controlled and announced. This aide in giving straightforwardness from both finishes which are the client and the specialist co-op. Just the assets that are being used by the clients are to be paid, which is an awesome preferred standpoint here [5].

1.2 Introduction To Data Security

The edge of innovation and the Internet have picked up fame in the presence of information correspondence. Correspondence is the spirit of any association and is a champion among the most basic needs of people [3].The possibility of mystery/concealed correspondence is as old as correspondence itself. It is routinely envisioned that interchanges can be made secure by using encryption strategies; however, this is less substantial by and by. Encryption gives an unquestionable approach to managing data security, and encryption projects are immediately available [4]. Regardless, encryption doubtlessly denotes a message as containing intriguing data, and the encoded message gets the opportunity to be liable to assault. In addition, all around it is alluring to send data without anyone despite seeing that data has been sent mystery data. The history shows that is favored concealing messages rather over enciphering them since it excites less doubt. This inclination perseveres in various operational settings till up this day [7]. Information security essentially goes for saving the secrecy and uprightness of information and shielding the information from unapproved clients or programmers. Various systems, for instance, advanced watermarking, cryptography and steganography were made remembering the ultimate objective to overhaul the information security. Cryptography is a workmanship or study of figures that usage science to scramble the principal content into an obviously garbled organization for others. Steganography is the craft of undetectable correspondence [9]. Its inspiration is to shroud the very nearness of correspondence by inserting messages in a way that a third individual can't recognize the nearness of the concealed message. While cryptography is a method to hide data by scrambling it to figure writings using an obscure key and transmitting it to the planned beneficiary, steganography gives advance security by concealing the consider message along with another cover medium [13]. Advanced watermarking and fingerprinting related to steganography are basically used for licensed innovation insurance. Watermarking is the act of intangible adjusting work to insert a mystery message. A computerized watermarking is a procedure of secretively installing into a commotion tolerant flag, for instance, sound or picture information. It is regularly used to recognize responsibility for copyright of such flag. The major point of computerized watermarking is to ensure the uprightness and validness of advanced media [11]. In fingerprinting; unmistakable and specific imprints are implanted in the duplicates of the work that assorted clients should get. For this circumstance, it ends up being basic for the property proprietor to find such clients who give themselves the benefit to disregard they're permitting assertion when they illegally transmit the property to various gatherings. To shroud mystery data in some other wellspring of data without leaving any obvious evidence of information change steganographic systems can be used. In today's advanced world, undetectable ink and paper have been supplanted by significantly more adaptable and common sense spreads, for instance, computerized reports, pictures, video, and sound records are used for concealing messages [12]. For whatever time span that an electronic file contains perceptually unimportant or excess data, it can be used as a cover for concealing mystery messages. Most of the conventional steganographic methods have constrained data concealing limit around 10% or less. This is in light of the fact that the standard of those procedures was either to supplant all the minimum huge bits of a multivalued picture with the mystery data or to supplant an exceptional piece of the repeat parts of the vessel picture. Information containing both the cover flag and the implanted data is known as stego information. Rarely, especially when alluding to picture Steganography, the cover picture can be called as Vessel or Container. Steganographic advances are an imperative part without limits of Internet security and protection [3].

1.3 Image Steganography

Steganography is an artistic work of concealing data in something else to enable them to pass in secret and is a bizarre piece of security that is not conventionally known, in spite of having a history that goes back a huge number of years. Steganography is ending up being progressively endless and pertinent with the presence of present day innovation and Internet. Particular sight and sound records, for instance, picture, video, and sound show intriguing computerized document designs for disguising mystery data. The development in correspondence innovation and use of open area channels, for instance, the Internet has fundamentally encouraged the exchange of information. The web applications demand secure information transmission. In view of capture attempt and despicable control by snoop, information transmission openly correspondence framework is not secure. An alluring answer for this issue is Steganography, which is the craftsmanship and exploration of composing concealed messages in a way that no one, aside from the sender and expect beneficiary, connects the presence with the message. Media records are expansive in size and encourage all the all the more inserting limit.//Taking the cover object as a picture in steganography is known as picture steganography Distinctive multimedia files, for example, picture, video and audio exhibit intriguing advanced document positions for disguising mystery data. The development in correspondence innovation and use of open area channels, for example, The Web has essentially encouraged the transfer of information. The web applications ask for secure information transmission. Due to capture attempt and improper control by meddler, information transmission out in the open correspondence framework is not secure. An appealing answer for this issue is Steganography, which is the craftsmanship and art of composing concealed messages in a way that no one, aside from the sender and expect beneficiary, relates the presence with the message. Media records are substantial in size and encourage all the all the more inserting limit. There are various criteria for characterizing steganography. One of them is grouping based on the sort of cover protest and the arrangement is as per the following.There are numerous criteria for classifying steganography. Data concealing innovation falls into three classes of steganography, watermarking, and cryptography. Steganography and watermarking everyone fall into two subclasses:

1.3.1 Fragile Steganography

Fragile technique suggests the inclusion of data in a cover in a way that adjustment of host document will pulverize full inserted data. Since it can without a lot of an extent be expelled from the calling then is not advantageous decision for copyright insurance, yet rather for instance in court cases, it can be an eyewitness of document inventiveness. Execution of delicate frameworks is less requesting than hearty ones [4]

1.3.2 Robust Steganography

Conversely, of delicate methodology, bits control of strong techniques won't successfully be expelled from host record. In spite of no technique can insurance that installed information is not alterable but instead if the measure of required endeavors for destructing data is amazing then it would be known as the solid procedure. To save safety of implanted data its revelation necessity be solid. Strong steganography is part into fingerprinting and watermarking. Use of fingerprinting remains set a blemish on the exact document for a specifically approved client. This exact check show which client has damaged copyright rule and scattered specific copy of the document. In the inverse side of fingerprinting which anticipated that would secure the clients, watermarking jam distinctiveness of document creator. Watermarking makes possible indictment persons who grip unlawful duplicates. In fact, watermarking will be utilized for large scale manufacturing of CDs and DVDs, although fingerprinting remains for specific duplicates. Once watermarking is not perceivable or adequately removable, it would be called vague watermarking. In any case, here is a discernible form of watermarking to display particular examples over a photo. Instance by its sort of watermarking would stay watermarks on a few certified receipts. One of them is gathering in view of the kind of cover dissent and the plan is according to the accompanying [5]

i) Image Steganography

Pictures are used as the predominant cover medium for steganography. Concealing data in the picture is known as picture steganography.in these technique pixel forces are utilized to hide the information. The cover image can be called as Vessel or Container. The picture ensuing to concealing data is called stegno-picture. A message is implanted in an advanced picture using an inserting calculation, using the mystery key. The ensuing stegno-picture is sent to the receiver.

ii) Network Steganography

The term protocol steganography refers to embedding information inside network protocols, for example, TCP/IP, UDP, and ICMP and so on. The network steganography is otherwise called protocol steganography. In the OSI organize layer show there exist incognito channels where steganography can be accomplished by concealing data in discretionary or unused header bits of TCP/IP fields [3].

iii) Video Steganography

Video Steganography is a strategy to conceal any kind of records in any information into digital video format. The video which is the mix of pictures is used as a bearer for concealed data. Video steganography utilizes video formats, for example, H.264, Mp4, MPEG, AVI, and so forth.

iv) Audio Steganography

At the point when taking audio as a transporter for data abstract it is called sound steganography. Because of the popularity of voice over IP (VOIP), the sound has transformed into a huge cover medium. Sound steganography uses advanced sound organizations, for instance, WAVE, MIDI, AVI MPEG or thus on for concealing mystery message.

v) Text Steganography

The substance steganography is a strategy for used made regular lingo to camouflage a riddle message. It can be proficient by altering the substance sorting out, or by changing certain properties of abstract parts. General strategy in substance steganography is to utilize a number of tabs, white spaces, capital letters, much the same as Morse code and so forth to finish information showing without end. After the presentation of Internet and particular sort of computerized record designs content steganography has diminished its significance. Content steganography lost its significance as a result of the way that the content documents have a little measure of excess information. Cases for coding methods are given underneath. The systems can be used either mutually or independently**.** The figure exhibits a direct representation of the brand inserting and extraction prepare in steganography. In this illustration, a mystery information is being inserted into a cover picture to make the stegno picture. A key is every now and again required in the implanting procedure. The implanting technique is done by the sender by using the right stegno key. The beneficiary can extricate the stegno cover picture with a particular ultimate objective to see the mystery information by using a similar key used by the sender. The stegno picture should look for all intents and purposes indistinguishable to the cover picture.

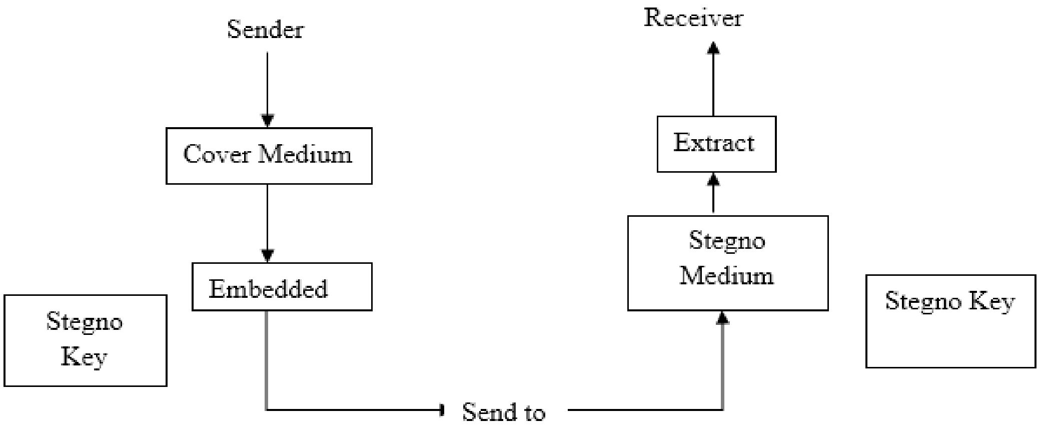


Figure 1.1: Steganography Mechanism

1.4 Steganography Measurements

1.4.1 Capacity

The limit is the most extreme measure of mystery data can be implanted in a record. Limit either can be characterized as a level out an incentive at the time of count by bits in order to specific cover either like a relative count as for fundamental bits by extra last stego document. Limit esteem depends at upon together installing capacity and cover properties. Not consistently finding implanting rate is this straightforward since some stego frameworks can install into packed spreads and along these lines, last inserting proportion would go alterable. At these sorts of matter, it’s difficult for finding a specific condition that could be precisely portray inserting limit. So another limit estimation for packed configurations is required. A bit for each non-zero DCT coefficient (BPC) is a limit metric for JPEG pictures. Pragmatic and hypothetical reviews give greater mystery information will contain more changes that measurably are more perceptible than short ones. Thusly installing rate and limit are particularly identified with the property of indistinctness.

1.4.2 Imperceptibility

Stegno address would never at keeping basic perceptual curio. The highest dedication by stegno dissent would grant superior subtlety. Its assets will be fulfilled if complexity by resulting stegno record gets non-discernable since unique cover in order to the director. Here are distinctive assessment frameworks differing steganography sorts however the primary assessment technique is PSNR. Crest Signal to Noise Ratio (PSNR) is standard for assessing the proportion in presuming greatest flag also impact in altering commotion of consistency in case of its portrayal [8].

1.4.3 Robustness

Strength is assets of seat killing mystery data by stego document. As long as identification by implanted mystery information has extensively higher significance than its expulsion, however property of strength discusses opposing against deliberate twisting of correspondence channel by techniques for an orderly interface or channel commotion intending to blacklist usage of steganography procedures. Vigor measurements of steganographic calculations are grouped in mutilation classes like geometric changes or added substance clamor. In each one of the classes twisting worth can be communicated concurring nonspecific (like commotion tool factors) or special (as PSNR) measures. Vigor by steganography techniques similarly can get examined through steganalysis assaults. Testing point by steganalysis is the discovery of nearness of the mystery information at the cover document. Nowadays different strategies vent if can lead steganalysis to uncover nearness of mystery data particularly when the cover record is modernized picture. In any case, surely understood steganalysis methodologies are:

i. recognition

ii. Histogram investigation(distinguishing agreeing first request insights)

iii. Twofold factual techniques for images by utilizing spatial connection

iv. Higher record insights (RS)

v. Scène Steganalysis of JPEG records ’ similarity

vi. Widespread visually impaired recognition techniques.

Furthermore here is additional basic component named join by qualities. Chi-squared attack breaks down proximity by PoVs to find nearness by inserted mystery data.

1.4.4 Definitions in CIA Triangle

What's all the more separated from limit, vigor, and indistinctness criteria there are more assessment measurements which fall under each side of CIA triangle. Pressure proportion, different watermarks, achievement degree, installing many-sided quality, and identification unpredictability are fundamental definitions under uprightness side. Pressure proportion few of host sorts potency be compacted as sound either picture records. The host document holding inserted information need crop an indistinct pressure proportion from the unmarked one and besides should not be tainted. Plus, the pressure procedure should not expel the installed information. Numerous watermarks further than single client need be fit for inserting watermark inside a host document. It suggests that perfect client need be equipped for implanting data without developing pre-installed one which may exist in advance. This property must be kept paying little mind to the likelihood that the calculations are not indistinguishable. Achievement rate and inserting many-sided quality assessment measurements which endeavor to decide a scaling framework for conveying pined for scale by safety and strength in order to installation at picked cover. The thoughts then factors required at classification side by CIA triangle are [9].

i. Secret Key

To secure watermarking remains not discernable or changeable the inserting estimation necessity uses cryptographic keys by shield this from the adjustment. only an aggressor have the ability to peruse the inserted information it moreover would have the ability to control this as together area and installing computation are known. So long as insurance of safety by installed information is rest on upon the mystery key then the keyspace need be adequately broad to create running savage constrain assaults illogical. The inserted information could be encoded at deuce levels in a figure key then information installing key. This exercise conveys deuce levels of safety if in most abnormal amount client won't have the ability to interpret, read, or even recognize closeness of inserted information. In another safety level gives some client by recognizing nearness of installed information, however, information an opportunity by won't be exposure deprived of taking the best possible key.

ii. Statistical Invisibility

This stuff stays expected by envisioning discovery by nearness by steganography/watermarking. Consecutively actual inspections at social affair by watermarked records must not exposure someone data neither in regard of utilized watermarking strategy nor temper by inserted information.

iii. Secrecy

It characterized like solidity by removing the inserted mystery information. This stuff may get planned by secrecy metric by encryption frameworks if applied heretofore of information implant. Computational charge or repetition remain deuce basic variables below openness party by CIA trio at the arena by steganography/watermarking.

iv. Computational Cost

The insertion also discovery period are significant considers information installing calculations. Some of the utilizations, for instance, communicate checking need consistent information handling and no deferral are worthy. In few another, as court matter adequacy is the major fundamental variable and moment could get disregarded

v. Redundancy

To enlarge vigor by inserted information this could be installed in much than single a player in host record. This could get once installed data only receive little segment by the record.

1.5 Image Steganography Techniques

Picture steganography systems can be partitioned into following.

1.5.1 Spatial Domain Methods

There are various adaptations of spatial steganography, all particularly change a couple of bits in the picture pixel values secluded from everything data. Slightest huge piece (LSB)-based steganography is one of the most straightforward methods that conceals a mystery message in the LSBs of pixel qualities without showing various noticeable contortions. Changes in the estimation of the LSB are vague for human eyes. Spatial space strategies are widely named takes after in light of the methods used for concealing data. The two important methods are a Least Significant bit (LSB), Pixel Value Differencing (PVD) [6].

1.5.2 Transform Domain Technique

This is a more mind boggling method for concealing data in a picture. The spatial area steganography strategies allow a more unmistakable measure of information to be covered up yet they are less impervious to steganalysis assaults. Change space steganography methods don't shroud the data behind picture pixels particularly rather they change the picture before veiling information. These strategies are more impervious to steganalysis assaults when contrasted with those installing rule that works in the time space. Diverse counts and changes are used on the picture to shroud data in it. The greater part of the strong Steganographic frameworks today work inside the change space. The basic approach to managing concealing data with DCT, FFT or Wavelet is to change the cover picture, change the coefficients, and after that modify the change.

1.5.3 Distortion Techniques

Distortion strategies require data of the first cover picture amid the translating method where the decoder capacities to check for contrasts between the first cover picture and the misshaped cover picture with a particular true objective to reestablish the mystery message. The encoder adds a succession of changes to the cover picture. Thusly, data is depicted as being put away by banner bending. In this method, a step image is made by applying a grouping of changes to the cover picture. This succession of adjustments is used to coordinate the mystery message required to transmit. The message is encoded at pseudoarbitrarily picked pixels. If the step image is not the same as the cover picture at the given message pixel, the message bit is a "1." by and large, the message bit is a "0." The encoder can alter the "1" esteem pixels in such a way, to the point that the actual properties of the picture are not affected. Regardless, the necessity for sending the cover picture confines the advantages of this technique.

1.5.4 Masking and Filtering

Concealing and separating systems is a Steganographic technique that receives a substitute methodology to concealing a message. These methods shroud data by indicating a picture, in an indistinct route from to paper watermarks, making markings in a picture. This can be accomplished by changing the luminance of parts of the picture. Regardless of the possibility that covering changes, the noticeable properties of a picture, it is done in a way that the human eye won't see the peculiarities. Since ceiling uses unmistakable parts of the picture, it is more vigorous than LSB change regarding pressure, trimming and different sorts of picture handling. The data is inserted in a huge ranges than basically concealing it into the commotion level, which makes it more fitting than LSB changes if misfortune pressure counts like JPEG. The concealed message is more essential to the cover picture [13]

Favorable circumstances of Masking and separating procedures are:

i. Since the data is covered up in the unmistakable parts of the picture, regarding pressure this strategy is substantially more strong than LSB substitution.

ii. Burdens of Masking and separating procedures are:

iii. Technique is just pertinent to grayscale pictures and confined to 24 bit

1.6 Criteria For Selection Of Techniques

Each of the calculations for picture steganography has unmistakable solid and powerless concentrations and guarantees that one uses the most reasonable calculation for an application. All steganographic calculations need to consent to a few crucial necessities. The most indispensable prerequisite is that a steganographic calculation must be subtle. The makers propose a course of action of criteria to additionally portray the indistinctness of a calculation. These prerequisites are according to the accompanying

1.6.1 Invisibility

The imperceptibility of a steganographic calculation is the above all necessity since the nature of steganography lies in its ability to be unnoticed by the human eye. The minute that one can see that a picture has been altered, the calculation is traded off.

1.6.2 Payload Capacity

Dissimilar to watermarking, which needs to implant only a little measure of copyright data, steganography goes for shrouded correspondence and along these lines requires an adequate inserting limit.

1.6.3 Robustness Against Statistical Attacks

Factual steganalysis is the act of distinguishing shrouded data through applying measurable tests on picture information. Various steganographic calculations leave a "signature" while installing data that can be successfully identified through measurable investigation. To have the ability to go by a superintendent without being identified, a steganographic calculation must not leave such a stamp in the picture as for be measurably huge [20].

1.6.4 Robustness Against Image Manipulation

In the correspondence of a stego picture by put stock in frameworks, the picture may experience changes by a dynamic superintendent attempting to expel concealed data. Picture control, for instance, trimming or turning, can be performed on the picture before it achieves its objective. Dependent upon the route in which the message is implanted, these controls may devastate the shrouded message. It is best for steganographic calculations to be strong against either malicious or inadvertent changes to the picture.

1.6.5 Independent of File Format

With different picture record positions used on the Internet, it might seem, by all accounts, to be suspicious that only a solitary kind of document organization is tenaciously passed on between two gatherings. The best steganographic calculations thusly have the ability to insert data into a document. This moreover takes care of the issue of not persistently having the ability to find a reasonable picture at the correct minute, in the correct configuration to use as a cover picture [30].

1.6.6 Unsuspicious Files

This prerequisite fuses all attributes of a steganographic calculation that may bring about pictures that are not used typically and may achieve doubt. Unusual document measure, for example, is one property of a picture that can bring about the further examination of the picture by a superintendent.

1.7 Applications of Steganography

There are diverse applications in steganography; it changes among the client necessities, for instance, copyright control, clandestine correspondence, shrewd ID's, printers et cetera.

i. Copyright Control

Inside a picture, mystery copyright data is installed. This is refined by Watermarking which is the perplexing structure. So that the intruder can't recognize the copyright data. There are distinctive techniques available to find the watermarking. It is refined by measurable, relationship, similitude check. Watermarking is used to guarantee the copyright data.

ii. Covert Communication

By and large, secret channel passes data by non-standard strategies. Correspondence is blurred that is unnoticed. The point of the secretive correspondence is to conceal the way that the correspondence is being happened. Incognito correspondence guarantees security. Steganography is one of the best frameworks of secret correspondence [29]

iii. Smart Id’s

In brilliant ID's the data about the individual is implanted into their picture for private data. For an affiliation, the confirmation of the assets is gotten to by the general population. So recognizing the burglary identified with the counteractive action of violations.

iv. Printers

Steganography makes use of some present printers like HP printer et cetera. In those printers, little yellow spots are embedded into all pages. Data is covered up inside the yellow spots like serial number, date and time stamp. Property is open in laser printer for watermarking the secret data [21].

CHAPTER 2

LITERATURE REVIEW

Joanne Hwan Jie Yin, et.al, (2015),"Internet of Things: Securing Data using Securing Image Steganography" suggest that Web of Things (IOT) is an ordinary thing (address) these days, which serves as a feature of our normal life exercises. Despite the fact that it benefits the private region in a few ways, diverse difficulties, for example, information classification and security are made. Genuinely, the group is concerned what data may spill out by a method for IoT. In this way, the necessities of a protected circumstance are indispensable with a particular true objective to secure the transmitting information from gadgets over the framework. Subsequently, in this paper, a protected plan is suggested on using picture steganography as an option security instrument in conjunction with a home server to secure the transmitted information from IP camera as the IoT gadget to substitute gadgets, either in LAN or WAN systems. In this paper, a plan is prescribed in perspective of the picture steganography since the IP camera with low handling and memory capacities is used as the IoT gadget to tackle the protection issues amid the transmission between shrewd gadget and home server. On account of the confinements of savvy gadgets, particularly bring down memory and computational power, the slightest critical piece strategy is being adjusted. With this method, changes minimum huge piece would not bring about any genuine debasement of value through human discernment and moreover measurable examination [14].

Nimmy K, et.al, (2014), "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography" suggest that Appropriate confirmation is a basic innovation for distributed computing situations in which associations with outer situations are normal and dangers are high. Here, another plan is proposed for shared confirmation where the client and cloud server can verify each other. The convention is planned in a manner that it utilizes steganography as an extra encryption conspire. The plan accomplishes confirmation utilizing mystery sharing. Mystery sharing permits a part of the key to being kept on both sides which when consolidated turns into the entire mystery. The mystery contains data about both sides included. Further, out of band verification has been utilized which gives extra security. The proposed convention gives common validation and session key foundation between the clients and the cloud server. Additionally, the clients have been given the adaptability to change the secret key. Moreover, solid security highlights make the convention appropriate for the cloud environment [15].

Wojciech Mazurczyk, Krzysztof Szczpiorski, et.al, (2011),” Is Cloud Computing Steganography-Proof” suggest that paper concentrates on the characterization of data concealing conceivable outcomes in Cloud Computing. After general prolog to distributed computing and its security, we move to brief portrayal of steganography. Specifically, we present order of Steganographic correspondence situations in distributed computing which depends on the area of the steganograms collector. These situations and in addition the dangers that Steganographic techniques can bring about must be considered when outlining secure distributed computing administrations [16].

Jun Feng, Yu Chen, Douglas Summerville, Wei-Summerville, (2011), ” Enhancing cloud storage against Rollback Attacks with A New Fair Multi-Party Non-Repudiation Protocol ” suggest that Alongside variation points of interest, distributed storage likewise postures new security challenges. Potential clients are hesitant to move vital and delicate information to cloud unless security challenges have been all around tended to. This paper reports our on-going endeavors to address three information security issues in distributed storage: revocation, decency, and move back assaults. We proposed a novel reasonable multi-party non-denial (MPNR) convention, which gives a reasonable non-disavowal stockpiling cloud and is fit for averting move backassaults [17].

Kazuki Murakami, Ryota Haanyu, 2014," Improvement of Security in cloud system Based on Steganography" suggest that as of late, many distributed computing frameworks have been created over the world. Notwithstanding, since there are numerous pernicious individuals who need to get to the mystery and individual data put away in cloud servers, data security is still a significant issue to understand. To cover and ensure mystery and individual data, in this paper we propose and build up a framework that can encode mystery message and implant it into a picture record by utilizing another transforming based steganography method. Regardless of the possibility that the pernicious individuals may take the picture containing the mystery data, they can't read the mystery data since this is practically incomprehensible without the stegno key. Thusly, we expect a change of security in cloud frameworks by utilizing our strategy [18].

Ankit Dhamija, et.al, 2014" A Novel Cryptographic and Steganographic Approach for secure cloud Data Migration" suggest that The adaptability to store boundless information with no stress about capacity constraints accessible available to us and the opportunity to utilize it as and when required from any place on the planet makes cloud processing the most favored innovation and stage to store and exchange information. Associations and individual clients are presently in particular agreeable to let their exceptionally vital information and programming live on the cloud servers and make themselves free from every one of the worries of capacity and security. In any case, each adaptability or advantages comes at a cost and distributed computing too is not a special case. The danger of client's protection, information classification and honesty and information security are continually approaching around. Among these, the safe exchange of information from association's premises to the cloud servers is of most extreme significance. Such a large number of encryption procedures and calculations have been proposed by scientists as of late to move information safely from their end to the servers. In this exploration paper, we propose an outline for cloud design which guarantees secure information transmission from the customer's association to the servers of the Cloud Service supplier (CSP). We have utilized a consolidated approach of cryptography and steganography since it will give a two path security to the information being transmitted on the organizing. To begin with, the information gets changed over into a coded organize through the utilization of encryption calculation and after that this coded organize information is again changed over into an unpleasant picture using steganography. In addition, steganography likewise conceals the presence of the message, accordingly guaranteeing that the odds of information being altered are negligible [19].

Bhagya Pillai, et.al, (2016), ”Image Steganography Method Using K-Means Clustering and Encryption Techniques” suggest that propose that Steganography includes covering up of content, picture or any delicate data inside another picture, video or sound in a way that an aggressor won't have the ability to distinguish its nearness. Steganography is, ordinarily, mistaken for cryptography as both the strategies are used to secure data. The distinction lays in the way that steganography shrouds the information so nothing appears out of standard while cryptography encodes the content, making it troublesome for a pariah to get anything from it paying little respect to the likelihood that they do accomplish the scrambled content. Those two are consolidated to build the security against various malevolent assaults. Picture Steganography uses a picture as the cover media to conceal the mystery message. In this paper, a picture steganography technique is proposed which bunches the picture into various portions and shrouds information in each of the section. Diverse bunching calculations can be used for picture division. The division includes an enormous plan of information as pixels, where each pixel advance has three segments to be specific red, green and blue. K-suggests grouping strategy is used to get exact outcomes. Along these lines, we use K-infers grouping method to get precise outcomes in a little day and age. A mix of cryptographic and bunching methods has been used alongside steganography. This gives extensively more noteworthy security as the encryption key is additionally obscure to the assailant. In addition, the scrambled content is covered up in each of the groups which progress reduces the likelihood of the message being found [20].

N. Jothy, et.al, (2016), ” A Secure Colour Image Steganography Using Integer Wavelet Transform” suggests that Steganography is an innovation that is used to disguise the data inside a couple challenges, for instance, picture, sound or video so no one can detect the data. Steganography technique has a few points of interest including high concealing limit and imperceptibility. The mystery substance has been covered up into the cover picture using IWT strategy. It is hard to identify the concealed data by Steganalyser since Stegno

Image and the Cover picture is all in all comparable. High PSNR (Peak Signal to Noise Ratio) esteem for the separated picture is as same as the mystery picture. This has been substantiated by contrasting systems which are comparable with IWT and the outcomes hurl light that the proposed IWT procedure is less difficult besides gives better PSNR values. In this paper, the mystery pictures can be extricated with no twisting to the first picture. Higher the PSNR esteem brings about less mutilation. This system offers the high caliber of the Stegno-picture having high PSNR values contrasted with various strategies. In any case, this technique can empower us to transmit the mystery data to the beneficiary autonomously, it is about unthinkable for any unintended gatherings to evacuate the mystery data, and recoup the first host picture when the Stegno picture is gotten to by them. Thusly, mystery data can be safely transmitted without adjusting the first cover picture [21].

Ramandeep Kaur, et.al, (2016), " A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques" To maintain the secrecy of information different information hiding techniques are utilized. Steganography is one of them, which implies hide information inside another digital media like text, image, audio, video and so on without being detected by the human visual system (HVS). Recently Video steganography has turned into a strong tool to hide large measure of data as opposed to image steganography. This paper is proposing an idea about a hybrid approach for video steganography to achieve high capacity data and high quality of stegno video on the premise of quality metrics like PSNR, MSE, and BER. The proposed methodology is a combo pack of different techniques, for example, RSA encryption, Edge detection, Identical Match and 4LSB substitution, in which a video file will be utilized to hide text message inside in all layers of RGB colour frames of video. The experimental results are analyzed on MATLAB software on cover video of "rhinos" and text secret message is embedding the video. The resulting values demonstrate that our proposed algorithm has high imperceptibility and security and resists the visual attacks. A proposed methodology is a hybrid approach, which is the combination of edge detection, identical match, 4LSB substitution and RSA encryption algorithms [22].

Tarik Faraj Idbeaa, et.al, (2015)" An Adaptive Compressed Video Steganography Based on Pixel-Value Differencing Schemes" Late developments in both information and communication security have heightened enthusiasm for enhancing the embedding capacity for data handling techniques. Although numerous Steganographic techniques, in the literature, have been developed for this purpose, the majority of them distort the quality of the host-signal during data embedding and the progressions will be ended up visible to the human eye especially for those signals circulated by means of the Internet which must be processed by a low bit rate compression because of bandwidth limitations. Consequently, the challenge is to make a Steganographic technique that can hide acceptable measure of data without altering the quality of the host signal. In this paper, pixel-value differencing (PVD) Steganographic scheme and its two modified versions, namely, enhanced pixel-value differencing (EPVD) and tri-way pixel-value differencing (TPVD) were implemented, analyzed and compared regarding invisibility, fidelity, and impact of data hiding on the compression efficiency. Experimental results indicate that the EPVD scheme is capable of giving preferable performance over other compared schemes. The evaluations of the algorithms were analyzed and discussed in light of the main steganography issues, for example, invisibility, fidelity and the impact of data hiding on the compression efficiency. Compared to past work, the experimental results have demonstrated that the proposed EPVD gives preferred invisibility over the PVD or TPVD schemes [23]. '

Yugeshwari Kakde, et.al, (2015), " Audio-Video steganography" Steganography is the workmanship and investigation of making messages which are to hole up behind unique cover document which may be sound, video or picture. In this paper we are tackling sound video steganography which is the blend of Audio steganography and Image steganography, in this, we are using PC crime scene investigation method for confirmation reason. We understand that video is the mix of various still edges of pictures and sound. We can choose any casing of video and sound for concealing our mystery information. This paper proposed a algorithm for wrap picture in chose video sequence is a picture concealing system in perspective of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and arbitrary LSB (Least Significant Bit) sound steganography technique for concealing secret content data inside sound of the sound video document, it decrease embedding contortion of the host sound. This paper focuses the possibility of PC legal sciences procedure which is use as an instrument for verification and information security reason and its use in video steganography in security way. This strategy is using recurrence space systems which enhance security that can be used for recognizing information nearness as a piece of suspected sight and sound document [24].

CHAPTER 3

PRESENT WORK

3.1. Problem Formulation

This work is based on video stenography in which wavelet transformation domain and BCD codes. In the base technique, the wavelet based technique is applied to analyze the textural features of the input video and embed text in the video to generate final stenographical video. The text which is embedded in the video will be in the encrypted form and to generate the encrypted data technique of BCD is applied and this technique utilizes the symmetric key for encryption and decryption. In the following are the problems lies which reduce its efficiency in terms of security and accuracy.

i. The technique of wavelet transformation is used which only analyze textural features of the input video. The video has also some other features like colour features which are not used to generate stenographical video. This problem reduces the accuracy of text embedding and extraction from the input video

ii. The second problem exists which the use of BCD codes to encrypt the input text. The BCD codes use the symmetric keys for encrypting and decrypting the text. The BCD codes generated the structure of encryption which is quite complex and need much time for execution

3.2. Objectives

i. To improve the performance of mutual authentication protocol for image steganography.

ii. Implement proposed algorithm and compare with existing algorithm in the terms of various parameters like fault detection rate, accuracy, and execution time

iii. The proposed improvement will be based on secure channel establishment algorithm.

3.3 Research Methodology

In this work, improvement in the existing technique will be proposed which is based to access color features of the input image and also secure channel establishment algorithm to encrypt and decrypt the text which needs to embed in the image. To analyze colour features of the input image technique of SVD can be applied which search the colour features and embedded the text in the video. The text which needs to embed can be encrypted using RSA algorithm which is less complex than BCD and also keys for encryption and decrypts will be sent through a secure channel which will establish between source and destination. The proposed technique can be applied for the image stenography and steps described below are included in the proposed technique:-

i. The image is taken as input on which you need to apply the stenography and also images which are used to provide security to the sensitive data

ii. The technique of SVD is applied which will analyze the properties of the input image and the SVD algorithm will analyse the colour features of the image

iii. In the last step technique of LSB will be applied which will generate the final stegno image, the RSA algorithm is applied which will generate secure channel from source to destination. When the secure channel is established only then the stegno image is transmitted from source to destination

3.3.1 Algorithm to Generate Stegno Image

Step 1: Input the secret message

Step 2: Change the bits positions of the secret message by using key1.

Step 3: Convert the secret message into a 1-D array.

Step 4: Encode the secret message by using BCH (15,11) encoder.

Step 5: XOR the encoded message with 15 bits of random value by using key2.

Step 6: Input the cover image

Step 7: Decompose the image stream into a number of frames.

Step 8: Divide the frame into YUV colour space.

Step 9: Apply the 2D-DWT on each Y, U, and V frame component.

Step 10: Embed the message into middle and high frequencies (LH, HL, and HH) of YUV component.

Step 11: Apply the inverse 2D-DWT on frame components.

Step 12: Rebuild the stegno frames from the YUV stegno frame components.

Step13: Output the stegno video by reconstructing from all stegno frames.

3.3.2 Algorithm to Generate De-Stegno Image

Step 1: Input the stegno image.

Step 2: Decompose the stegno image stream into a number of frames.

Step 3: Divide each frame into YUV colour space.

Step 4: Apply 2D-DWT separately to the three Y, U and V components.

Step 5: Extract the encoded message from the middle and high frequencies (LH, HL, and HH) of each Y, U and V component.

Step 6: Segment the encoded message into 15 bits groups.

Step 7: XOR each group with the random 15 bits numbers by using key2.

Step 8: Decode the message by using BCH (15,11) decoder.

Step 9: Obtain 1-D array from the resulted groups.

Step 10: Reposition the resulted message again to the original bit order by using key1.

Step 11: Output the secret message

3.3.3 Algorithm for RSA Algorithm

Creating keys:

i. Generate (find) two large prime numbers (P and Q)

ii. Calculate N = PQ

iii. Calculate M = phi(N) = (P - 1) (Q - 1) = (Euler totient function)

iv. Ct any integer E, the rules to select E are:

   i. E is positive integer

   ii. $0 < E < M$

   iii. GCD (M, E) = 1 ... (GCD = Greater Common Divisor)

   NOTE: It is recommended to use E = 65537 (17 bits).

v. Calculate D a use Extended Euclid Theorem (mod inverse)

(E * D) = 1 (mod M)

(E * D) mod M = 1

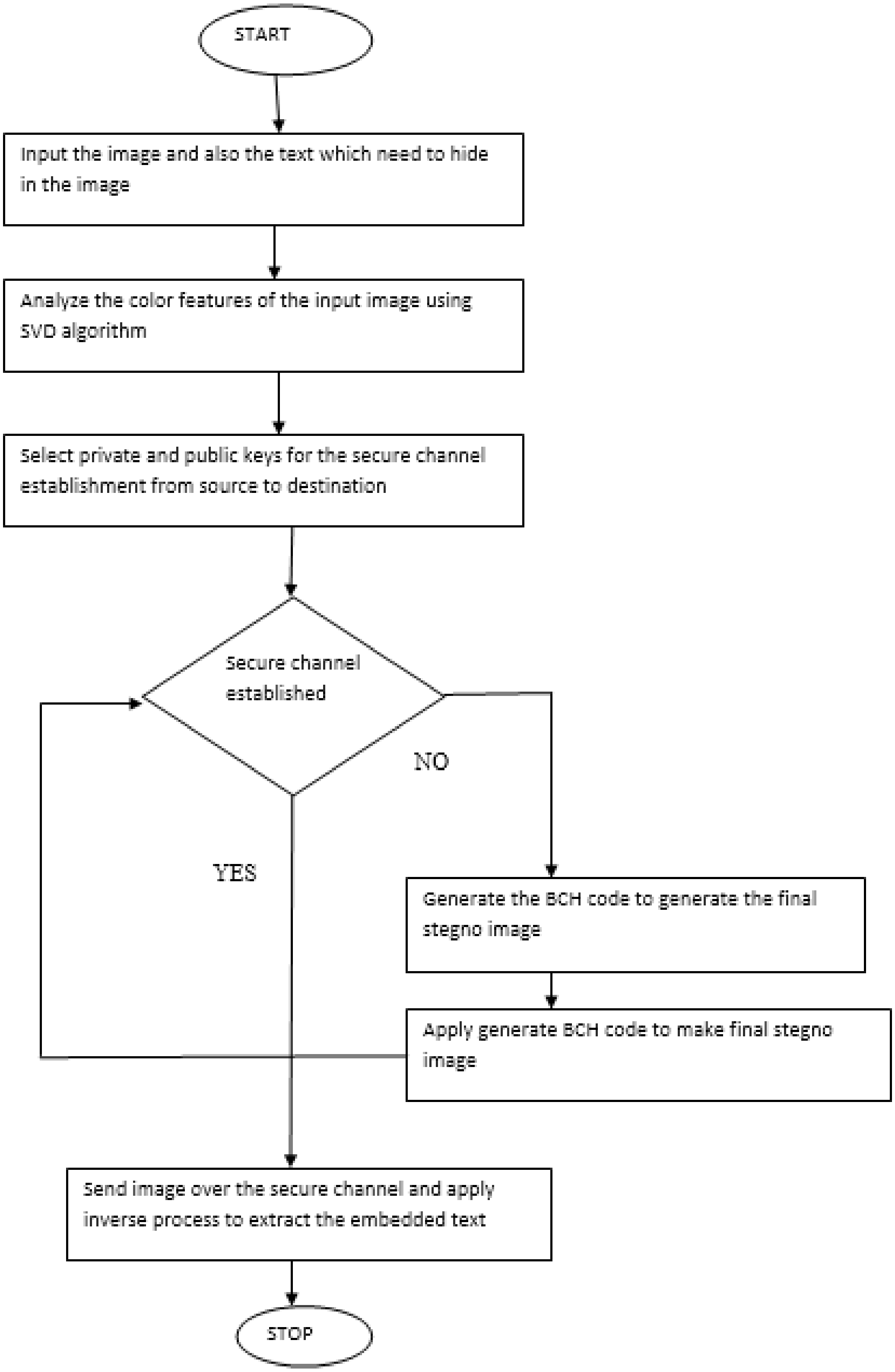
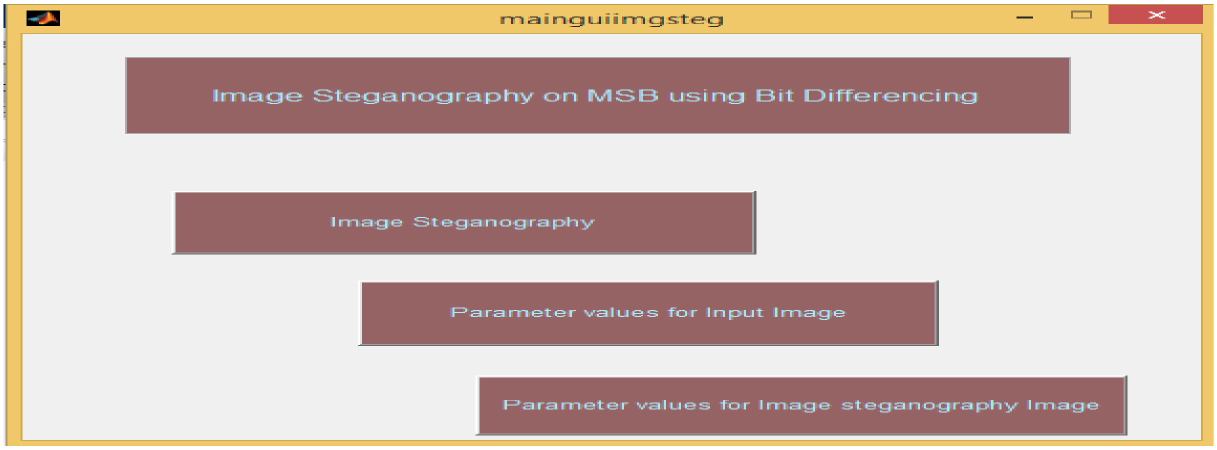

START
Input the image and also the text which need to hide in the image
Analyze the color features of the input image using SVD algorithm
Select private and public keys for the secure channel establishment from source to destination
Secure channel established
NO
YES
Generate the BCH code to generate the final stegno image
Apply generate BCH code to make final stegno image
Send image over the secure channel and apply inverse process to extract the embedded text
STOP

Figure 3.1: Flowchart of methodology

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Experimental Results



mainguiimgsteg
Image Steganography on MSB using Bit Differencing
Image Steganography
Parameter values for Input Image
Parameter values for Image steganography Image

Figure 4.1: Default interface

As shown in figure 4.1, the interface is designed in the Matlab and in the interface three buttons are plotted to execute the algorithm

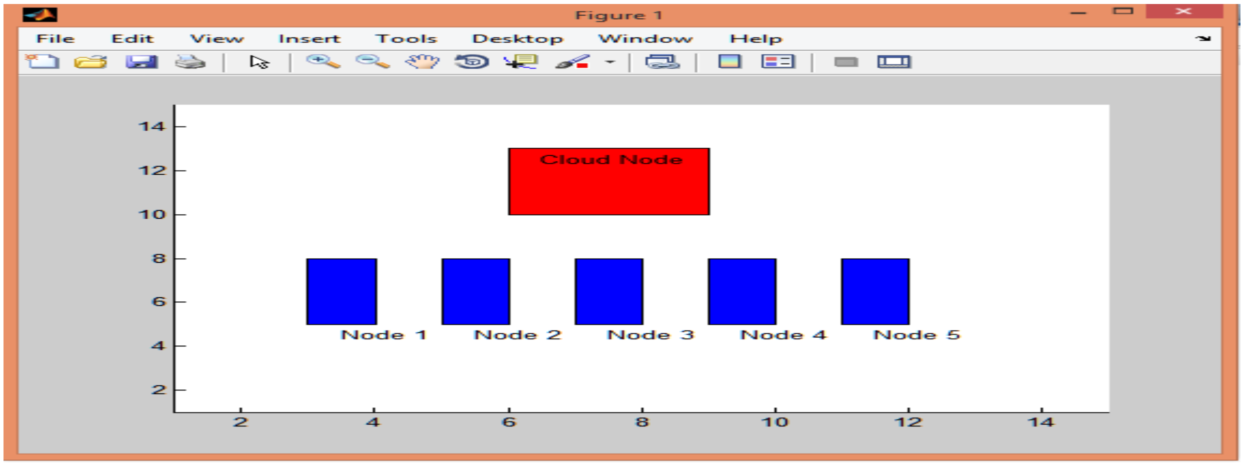
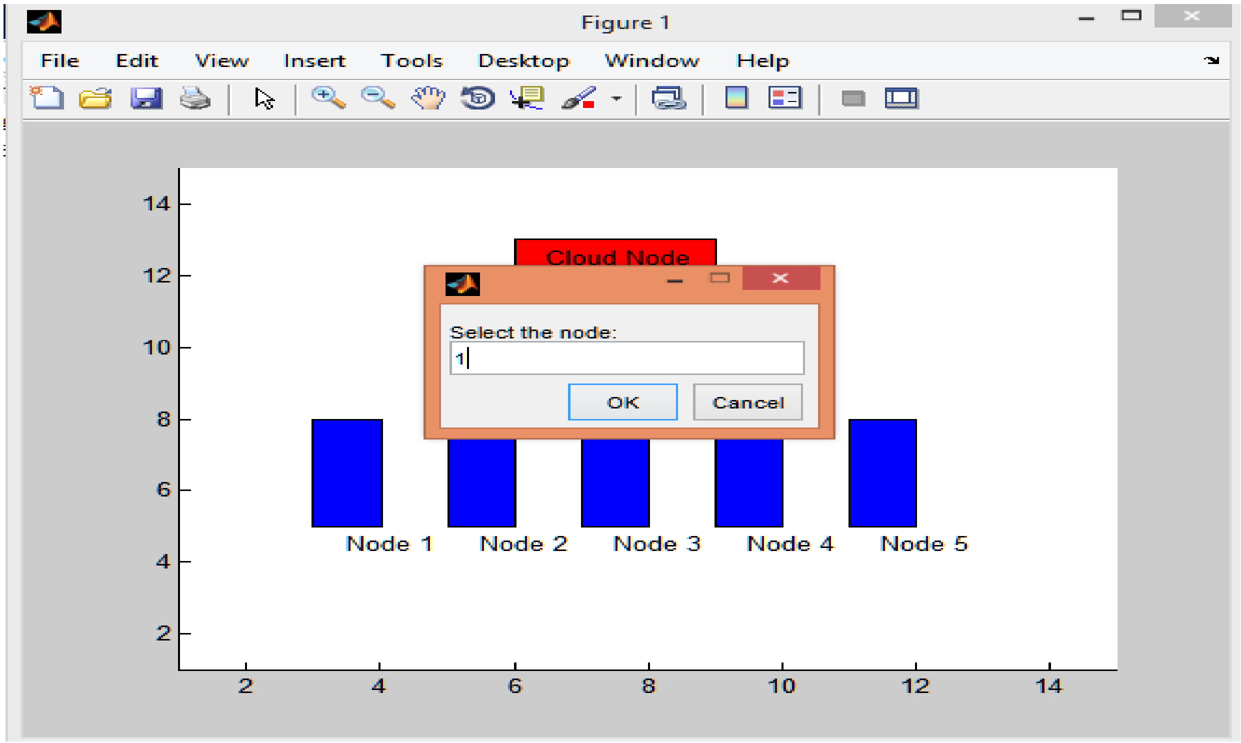


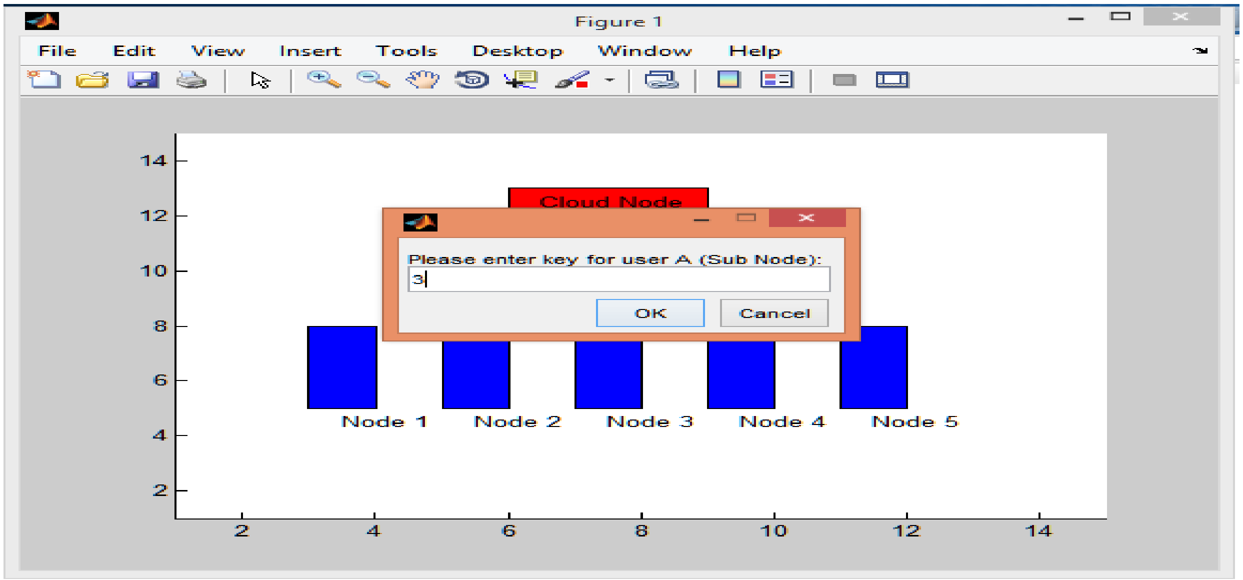
Figure 4.2 : Connection with cloud



Select the node:

1

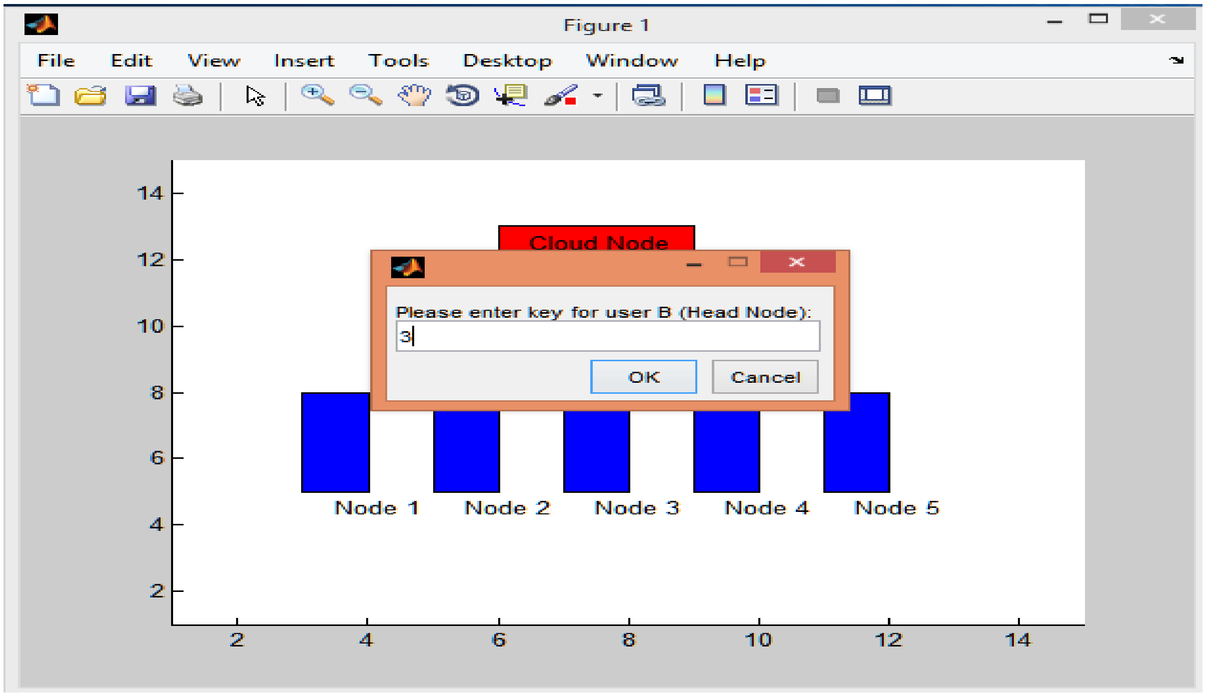
Figure 4. 3 : Select the node



Please enter key for user A (Sub Node):

3

Figure 4.4: Enter key for user



Please enter key for user B (Head Node):

3

Figure 4.5 : Enter key for user B

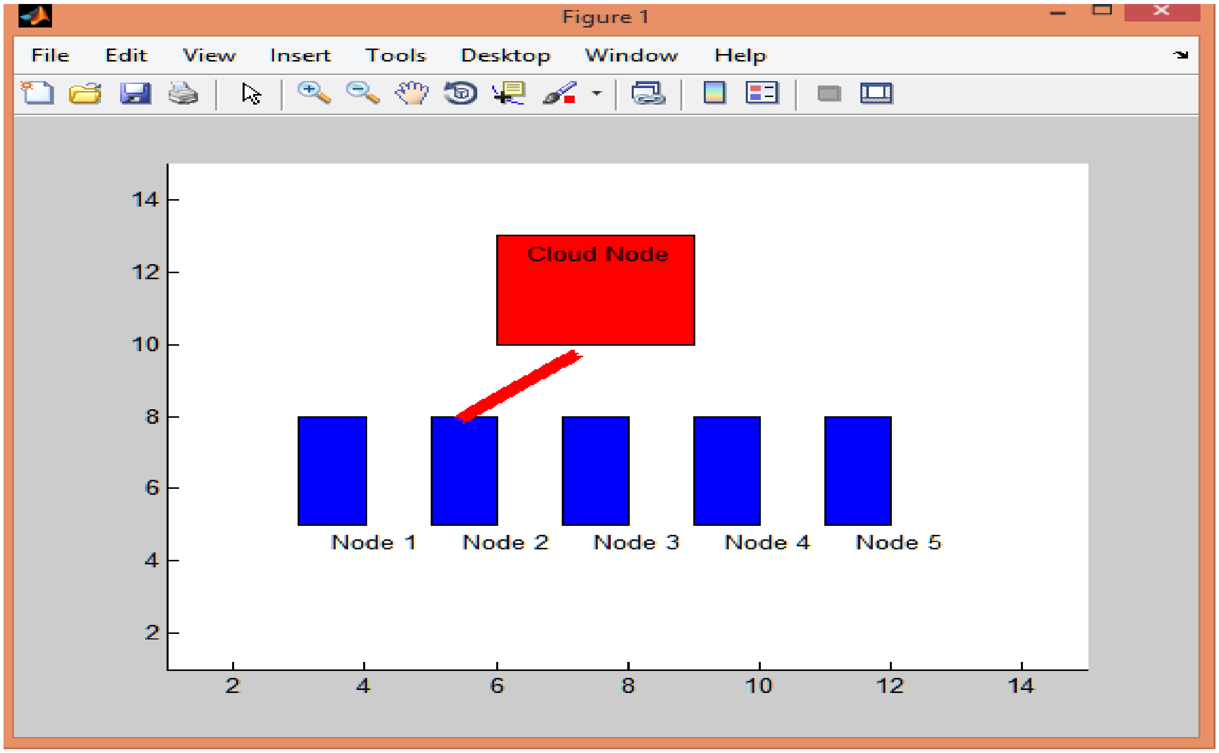


Figure 4.6 : Connection Establishment

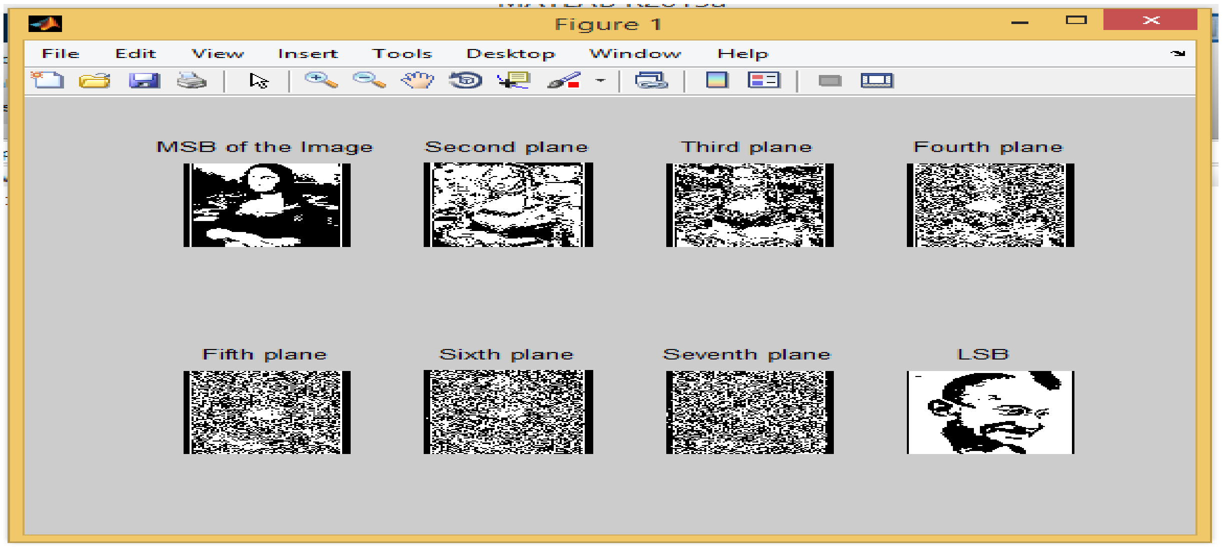


Figure 4.7: LSB technique to generate stegno image

As shown in figure 4.7, the technique of LSB technique is applied which will generate the stegno image and to generate the stegno image the seven planes are accessed.

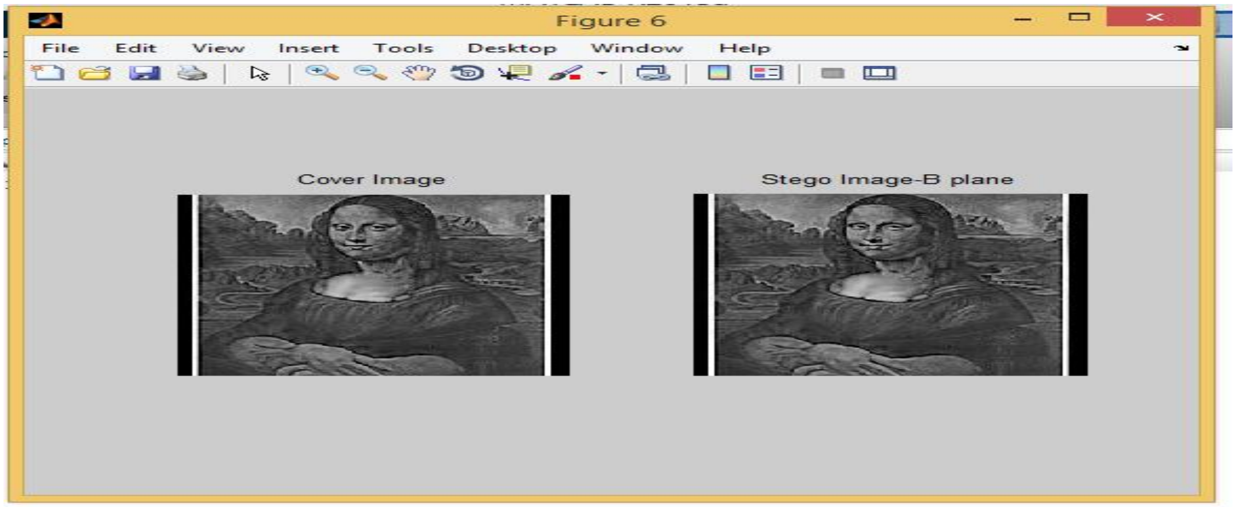


Figure 4.8: Stegno image for R plane

As shown in figure 4.8, the cover image is breaked into the seven planes and final stegno image is generated for the B image as shown in the figure

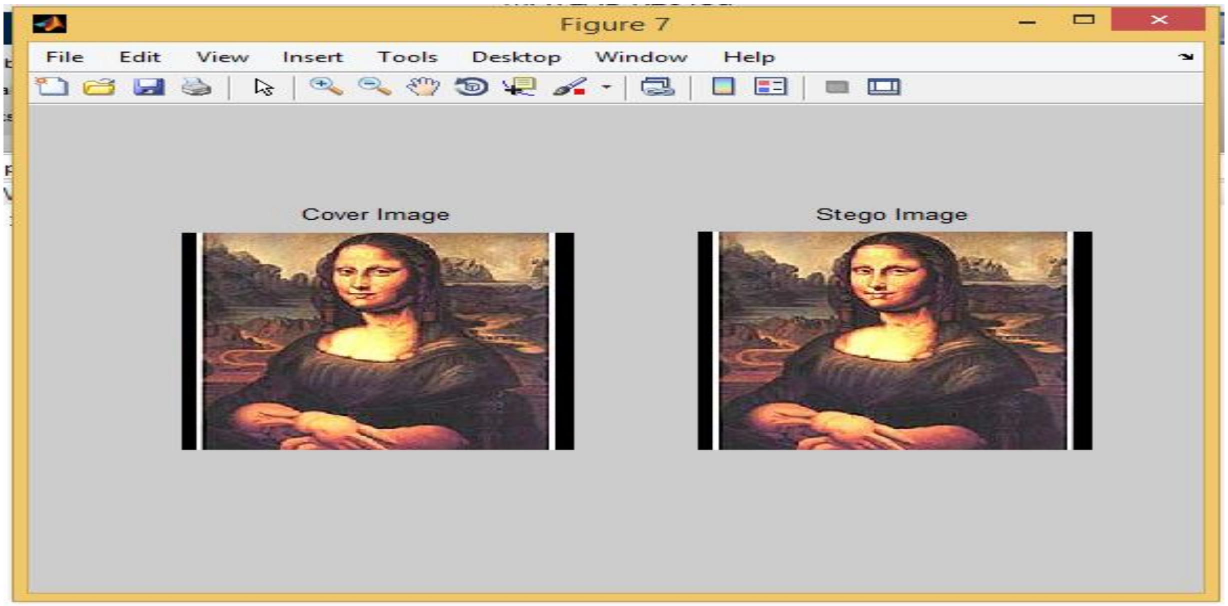


Figure 4.9: Generation of final RGB stegno image

As shown in the figure4.9, the final stegno image is generated from the cover image by embedding the text in the cover image

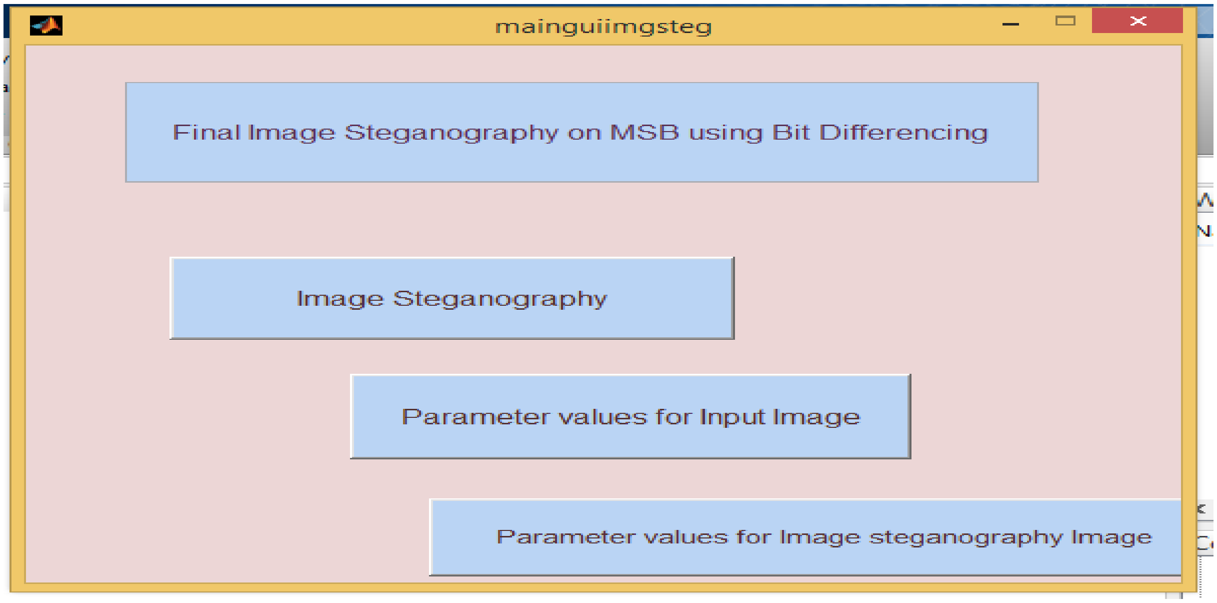

mainguiimgsteg
Final Image Steganography on MSB using Bit Differencing
Image Steganography
Parameter values for Input Image
Parameter values for Image steganography Image

Figure 4.10: Interface for the proposed technique

As shown in the figure 4.10, the interface is designed to implement proposed technique. In the proposed technique RSA algorithm is applied to generate final stegno image

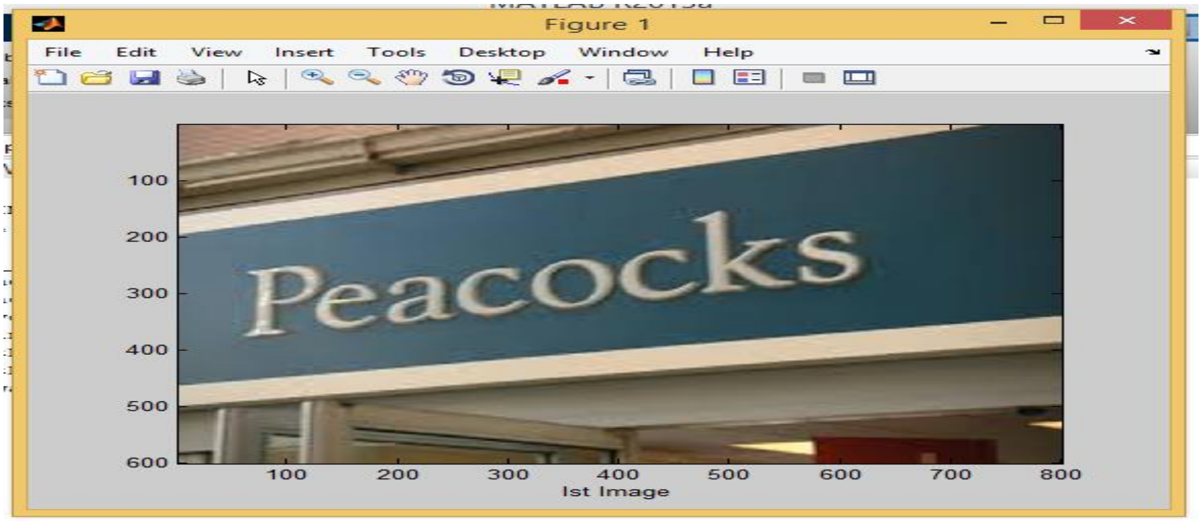


Figure 4.11: Input image to generate final image

As shown in the figure 4.11, the image is taken as input from which the final stegno image is generated. The input image is analyzed in terms of their colour features to generate final image.

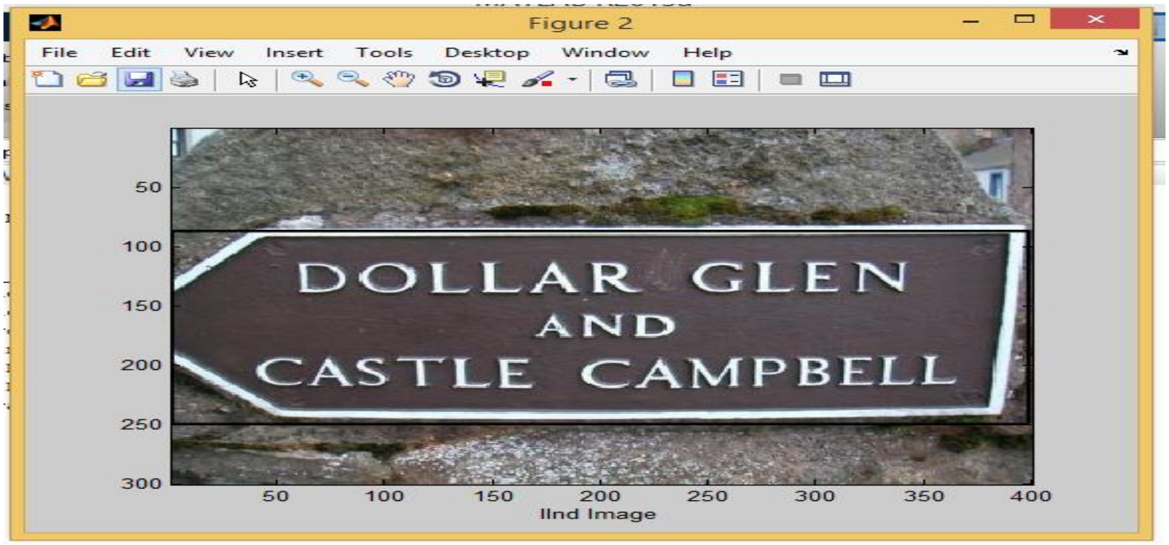


Figure 4.12: Sensitive image

As shown in the figure 4.12, this image is taken as input and technique of BCH codes is applied which will hide the sensitive image into the input image

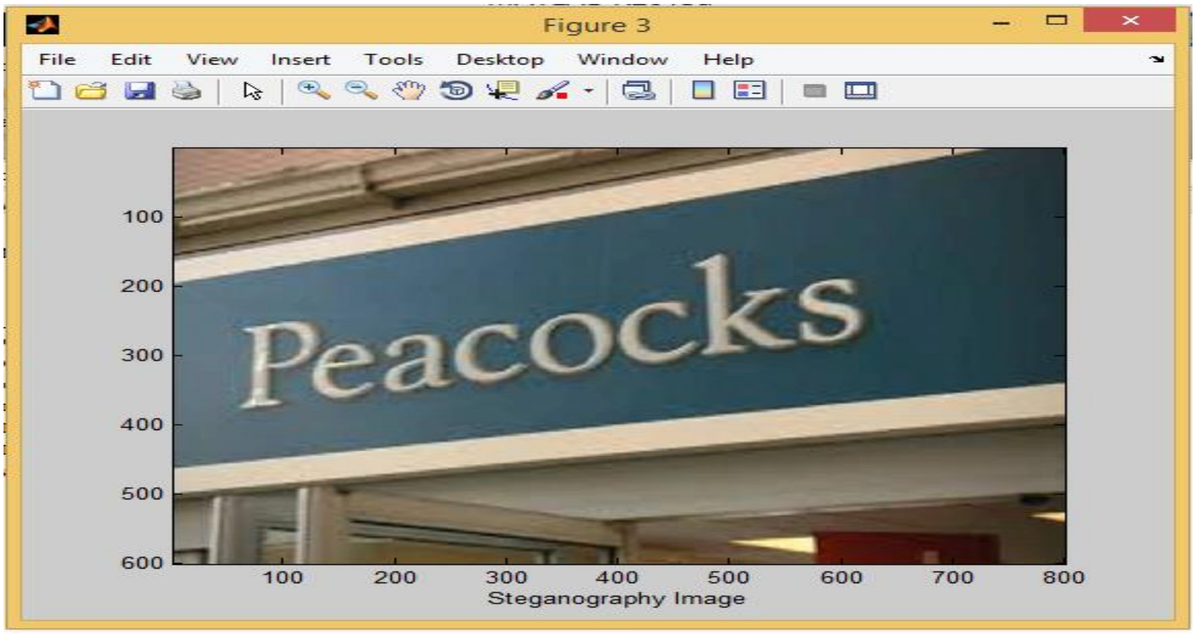


Figure 4.13: Final stegno image

As shown in the figure 4.13, the technique of LSB and technique of RSA is also applied which will generate final stegno image

4.2 Comparison with Existing Technique:

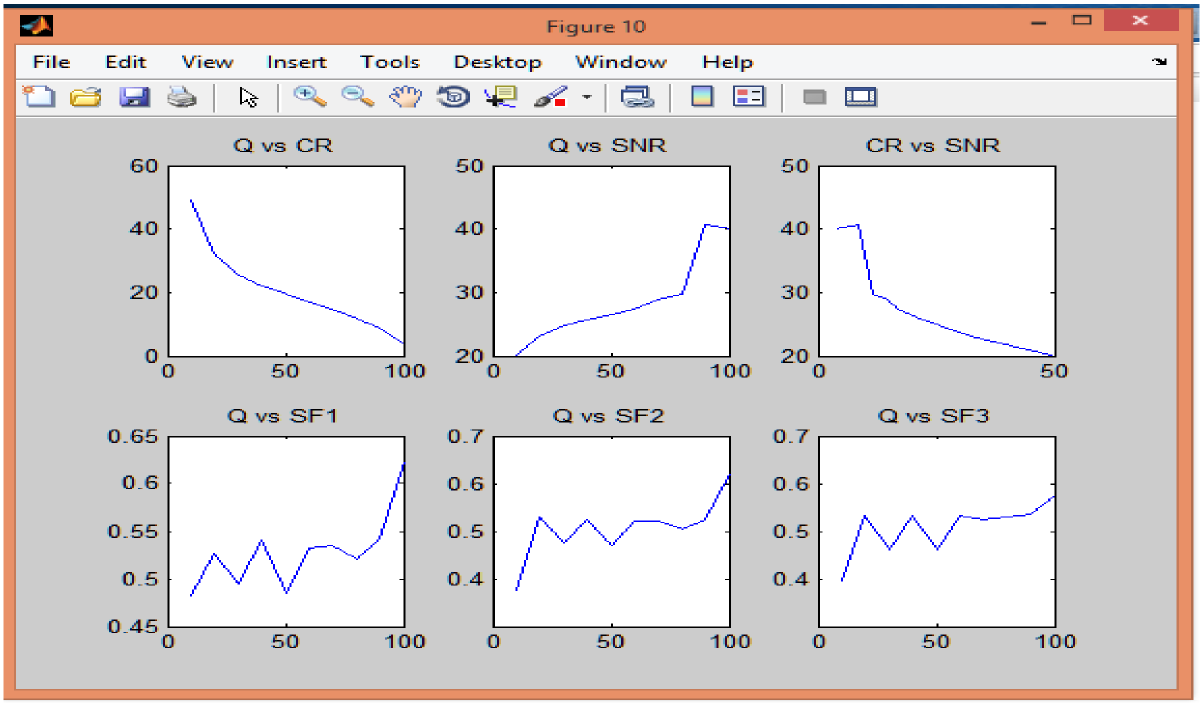
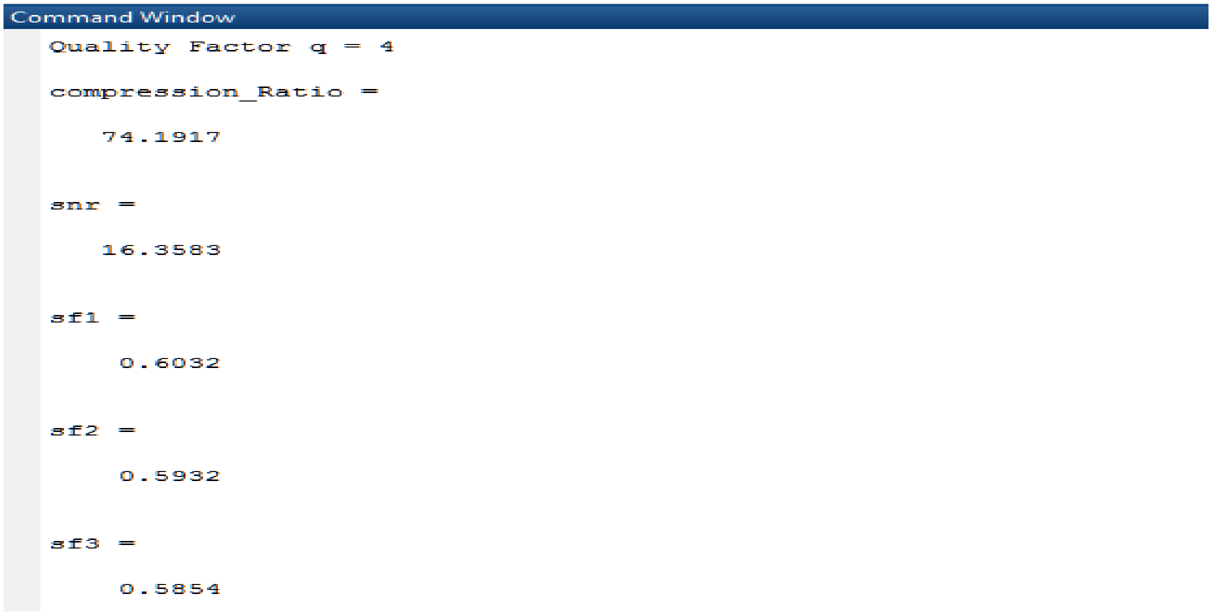
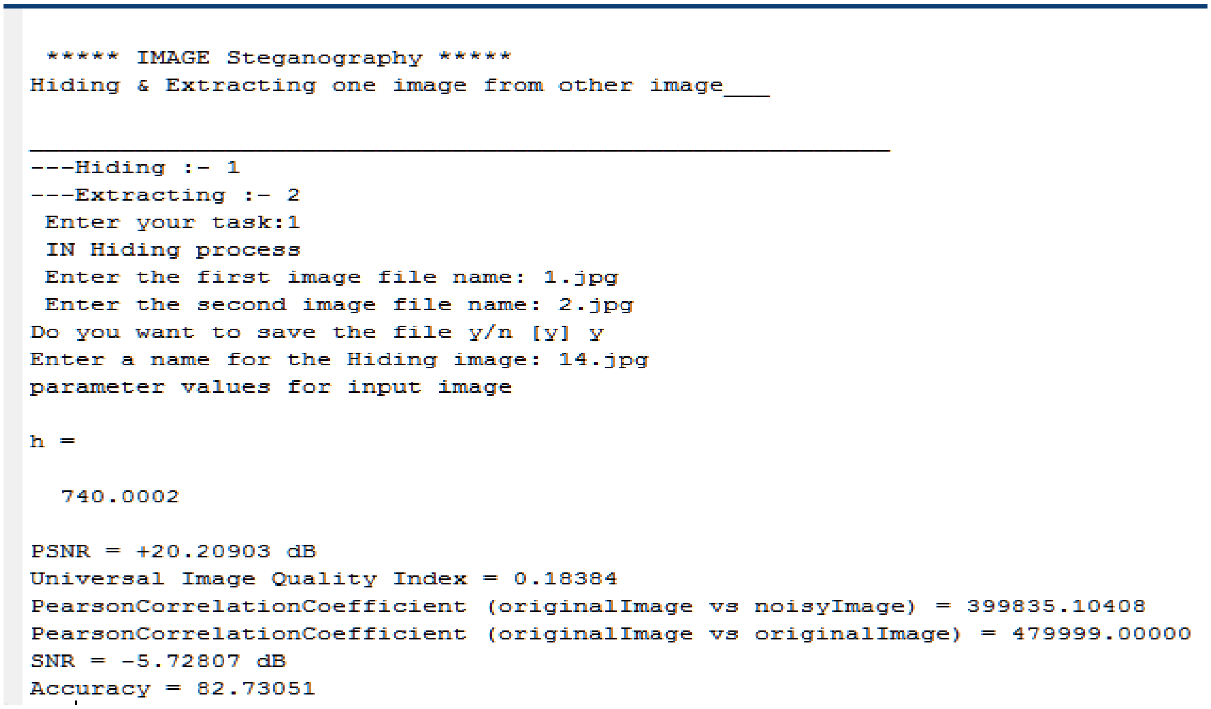


Figure 4.2.1: COMPARITIVE ANALYSIS



```
Quality Factor q = 4

compression_Ratio =

   74.1917


snr =

   16.3583


sf1 =

    0.6032


sf2 =

    0.5932


sf3 =

    0.5854
```

Figure 4.2.2: COMPARISON OF RESULTS



```
 ***** IMAGE Steganography *****
Hiding & Extracting one image from other image___

_________________________________________________________
---Hiding :- 1
---Extracting :- 2
 Enter your task:1
 IN Hiding process
 Enter the first image file name: 1.jpg
 Enter the second image file name: 2.jpg
Do you want to save the file y/n [y] y
Enter a name for the Hiding image: 14.jpg
parameter values for input image

h =

  740.0002

PSNR = +20.20903 dB
Universal Image Quality Index = 0.18384
PearsonCorrelationCoefficient (originalImage vs noisyImage) = 399835.10408
PearsonCorrelationCoefficient (originalImage vs originalImage) = 479999.00000
SNR = -5.72807 dB
Accuracy = 82.73051
```

Figure 4.2.3 IMPLIMENTATION RESULT

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In this work, it is being concluded that due to various attacks are possible in cloud computing architecture. Due to various vulnerabilities in the network data security need to be considered which provide security to the text and image data. The technique of stenography will be applied which provide security to the text and image data. In the technique of stenography, the sensitive text data will be hidden under the image data. The technique of LSB can be improved which increase the security of the stenography in cloud computing. When the LSB technique of stenography is improved it leads to reduction in chances of attack in the network and also reduce data transmission time of the network

5.2 Future Scope

i. In future technique will be proposed which increase the security of the network.

ii. The technique of access rights will be applied which gave extra security to the network.

REFERENCES

[1] Ross J. Anderson and Fabien A. P. Petit colas," On the Limits of Steganography", 1998, *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, VOL. 16, NO.

[2]R. Tavares and F. Madeira," Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel", 2016, *IEEE LATIN AMERICA TRANSACTIONS*, VOL. 14, NO. 2

[3]Udit Budhia, Deepa Kundur, and Takis Zourntos," Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain", 2006, *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* Vol. 1, No. 4

[4]Yun Cao, Xianfeng Zhao, and Dengguo Feng," Video Steganalysis Exploiting Motion Vector Reversion-Based Features", 2012, *IEEE SIGNAL PROCESSING LETTERS*, VOL. 19, NO. 1

[5]Yun Cao, Hong Zhang, Xianfeng Zhao and Haibo Yu," Covert Communication by Compressed Videos Exploiting the Uncertainty of Motion Estimation", 2013, *IEEE, 1089-7798*

[6]Qiang Cheng and Thomas S. Huang," An Additive Approach to Transform-Domain Information Hiding and Optimum Detection Structure", 2001, *IEEE TRANSACTIONS ON MULTIMEDIA, Vol. 3, No. 3*

[7]Sorina Dumitrescu, and Xiaolin Wu," A New Framework of LSB Steganalysis of Digital Media", 2005, *IEEE TRANSACTIONS ON SIGNAL PROCESSING,* Vol. 53, No. 10

[8]Klimis Ntalianis, and Nicolas Tsapatsoulis," Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks", 2015, *IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING,* Vol 5, No. 7

[9]Chuan Qin, Chin-Chen Chang, Ying-Hsuan Huang, and Li-Ting Liao,” An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism”, 2013,*IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*,Vol.23,No.

[10]Kasim Tasdemir, Fatih Kurugollu, and Sakir Sezer,” Spatio-Temporal Rich Model-Based Video Steganalysis on Cross Sections of Motion Vector Planes”, 2016, *IEEE TRANSACTIONS ON IMAGE PROCESSING*, Vol. 25, No. 7

[11]Keren Wang, Hong Zhao, and Hongxia Wang,” Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value”, 2014,*IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Vol. 9, No. 5

[12] Nematollah Zarmehi, Mohammad Ali Akhaee,” Digital video steganalysis toward spread spectrum data hiding”, 2015, *IET Image Process.*, pp. 1–8

[13]C. Zhang, Y. Su and C. Zhang,” Video steganalysis based on aliasing detection”, 2008,*IEEE, Vol. 44 No. 13*

[14] Joanne Hwan Jie Yin, Gan May Fen, Fiza Mughal, Vahab Iranmanesh,” Internet of Things: Securing Data using Image Steganography”, 2015, *IEEE, 978-1-4673-8675-3*

[15]Nimmy K, M. Sethumadhavan,” Novel Mutual Authentication Protocol for Cloud Computing Using Secret Sharing and Steganography”,2014, IEEE,978-1-4799-2259-14/$31.00

[16]Wojciech Mazurczyk, Krzysztof Szczypiorski “Is Cloud Computing Steganography-Proof?”, 2011, IEEE ,978-0-7695-2/11$26.00©2011©2014

[17] Jun Feng, Yu Chen, Douglas Summerville, Wei-Shinn Ku, Zhou Su “Enhancing Cloud Storage Security Against Roll-back Attacks with A New Fair Multi-Party Non-Repudiation Protocol” 2011, IEEE,978-1-4244-8790-5/11/$26.00©2011

[18]Kazuki Murakami, Ryota Hany, Qiangfu Zhao and Yuya Kaneda “Improvement of Security in cloud system Based on Steganography” IEEE,965-8580

[19]Vijay Dhaka, “A Novel Cryptogphic and Steganographic Approach for Secure Cloud Data Migration”2015, IEEE,978-1-4673-7910-6/15/$31.00©2015 IEEE*45*

[20]Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram,” Image Steganography Method Using K-Means Clustering and Encryption Techniques”, 2016, *IEEE, 978-1-5090-2029-4*

[21]N. Jothy, S. Anusuyya,” A Secure Color Image Steganography Using Integer Wavelet Transform”, 2016, *IEEE, 97698542-3234-346-7*

[22] Ramandeep Kaur, Pooja, Varsha,” A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques”, 2016, *IEEE, 978-1-4673-9338-6*

*[23]*Tarik Faraj Idbeaa, Salina Abdul Samad, Hafizah Husain,” An Adaptive Compressed Video Steganography Based on Pixel-Value Differencing Schemes”, 2015, *IEEE, 978-1-4673-8374-5*

[24]Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale,” Audio-Video steganography”, 2015, *IEEE, 978-1-4799-6818-3*

[25]Diksy M. Firmansyah, Tohari Ahmad,” An Improved Neighbouring Similarity Method for Video Steganography”, 2016, *IEEE, 35365-7455-67*

[26]C. Lalengmawia, A. Bhattacharya, and A. Datta,” Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data”, 2016, *IEEE, 978-1-4673-9802-2*

[27]Mehdi Sharifzadeh1 and Dan Schonfeld,” Statistical and Information-Theoretic Optimization and Performance Bounds of Video Steganography”, 2015, *IEEE, 978-1-5090-1824-6*

[28]Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi," Stochastic Local Search Combined with LSB Technique for Image Steganography", 2016, *IEEE, 9587965-3489-5765-*

[29] Saakshi Narula, Arushi Jain and MS. Prachi "Cloud Computing Security",2015, IEEE,2327-0659

[30] S. Suganya and P.Damodharan " Enhancing Security For Storage Services In Cloud Computing"2013,IEEE,9687865-3589-57