LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

ENHANCEMENT IN SVD-DCT-DWT WATERMARKING TECHNIQUES TO INCREASE CLOUD DATA SECURITY

A Dissertation Submitted

By

SHAKUN GUPTA

11300100

To

Department of Computer Science & Engineering

In Partial Fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science & Engineering

Under the Guidance of

HARSIMRAN SINGH

Assistant Professor

(May 2015)

ABSTRACT

In this work, the technique of watermarking had been applied in cloud computing. The watermarking technique had provide extra security to cloud data. In this work, the work will be proceeded on image watermarking and techniques like SVD, DCT and DWT had been used to generate watermarked Image. The SVD technique had been applied first to generate watermarked image, after that DCT technique is applied to reduce MSE value of the watermarked image, to further reduce the MSE value of image DWT technique will be applied. In this work, The data will be received by the end user, the user extract the original data from the watermarked data some noisy data left behind which increase MSE value. To remove noise from that data, technique of KALMAN filter had been applied.

ACKNOWLEDGEMENT

First of all, I would like to thank my Almighty God, who has always blessed me and for giving me strength to do this work.

I wish to express my deep gratitude to my guide, Mr. Harsimran Singh, his generous guidance. His guidance and support throughout all stages of the thesis process enabled me to conduct the research. Without his support, I would not be possible to complete this program.

Then I would like to offer my sincerest gratitude to Mr. Dalwinder Singh, Head of the Department, Computer Science & Engineering, for providing all the facilities and environment.

<div align="right">

Shakun Gupta

Reg. No. 11300100

</div>

DECLARATION

I hereby declare that the dissertation entitled "**Enhancement in SVD-DCT-DWT watermarking techniques to increase cloud data security**" submission for the M.Tech degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date :   **Shakun Gupta**

                                                                                                     Reg. No. 11300100

CERTIFICATION

This is to certify that **Shakun Gupta** has prorating M.Tech dissertation **'Enhancement in SVD-DCT-DWT watermarking techniques to increase cloud data security'** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engineering.

Date :

Signature of Guide

Name: Mr. Harsimran Singh

UID-18273

TABLE OF CONTENT

LIST OF FIGURES

INTRODUCTION

1.1 Introduction of cloud computing:

Cloud computing is computing that is based on the internet, and it is most recent trend in IT world. In cloud computing shared information resources and software that are providing to computers and many other devices on demand. Email was probably first service on the "cloud". In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. Cloud is a technology based on internet that uses the internet and central remote servers to support data and applications, as:
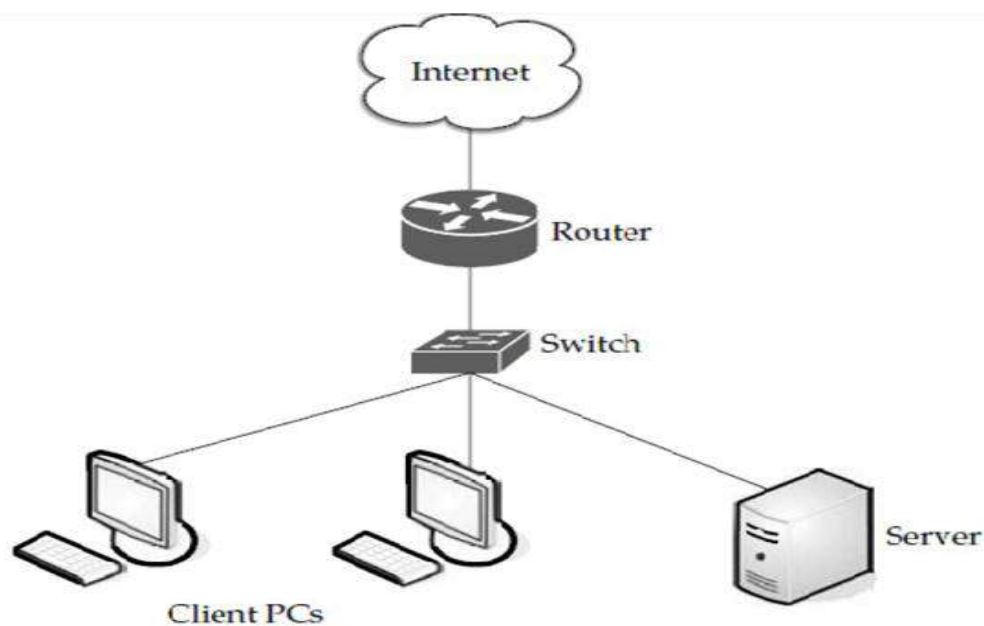
Fig 1.1: A cloud is used in network diagrams to depict the Internet

[1] By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. In Cloud computing due to network traffic and make network bandwidth more efficient introduced cloud to both infrastructure and server. With the help of Cloud Computing, users can access their databases from anywhere in the world only if they connected to the internet. Today's world depends on cloud computing to store their public data as well as personal data. That data may be required by them or others at any instant of time. As a result, data security in cloud computing has required lots of attention from the research society. Amazon played energetic role in this. IBM, google, many universities and companies adopted it [2]. Cloud Computing allows customers and businesses to access applications without installation and can access their personal files at any computer with online access. The location of physical resources and devices being accessed that are mostly not known to the user. It also provides facilities for users to develop, use and manage their applications in the cloud, which requires virtualization of resources that maintains it. [3]. Cloud computing is a particular type of computing that has some particular profits. But also it has some particular rejections as well. And it does not assist the requirements of real businesses to hear only the publicity about cloud computing – together positive as well as negative.

1.2 Service Model of Cloud Computing

- **Software as a Service (SaaS)**

In this, the consumers purchase the ability to access and use an application or service that is present in the cloud. Where applications are introduced and distributed online through a web browser proposing functionality of traditional desktop.for example Google Apps and Oracle on demand.

- **Plat1form as a Service (PaaS)**

This service models purpose the service to the consumer as both operation and development platform. The cloud provide the software platform for system for example Google App Engine and force.com.

- **Infrastructure as a Service (IaaS)**

The Consumers can use infrastructure as a service based service offering to organize their own operating system and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over the operating system and deployed applications. For example Amazon Elastic Compute Cloud and Simple Storage Service. For example Amazon Elastic Compute Cloud.

These service models have been taken together which is also known as SPI model.
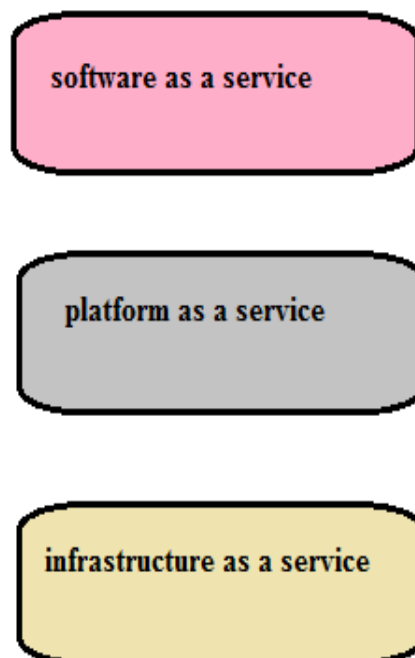
Fig 1.2: Cloud Computing Service Models

There are also several other service models such as Identity as a Service (IdaaS), Compliance as a Service (CaaS), and Storage as a Service (StaaS).

1.3 Deployment Models

These models describes about what is the purpose of the cloud and about the nature of cloud how it is located. Organizing cloud computing is rest on the changed requirements, hence it is be different as of each other. As for organizing a cloud computer, there are four models of deployment can be used. Every model has its own characteristics.

- **Private Cloud**

This cloud infrastructure is worked for the special use of an organization. The cloud may be deployed by the organization or any third party. These clouds may be either off-premises or on-premises.

- **Community Cloud**

This cloud is the one where the cloud has been deployed which assists the common function and common purpose.[1] It may be for many organizations or may be for only one organization, but mutual concerns are shared by them such as their mission, security, policies and so on.

- **Public Cloud**

This cloud infrastructure is presented for the public use instead for a large industry group and is owned by an organization selling services of cloud.

- **Hybrid Cloud**

Hybrid clouds are a grouping of public and private clouds. Hybrid clouds control the abilities of every deployment model of cloud. Every part of a hybrid cloud is linked to the other through a gateway, directing the applications and the data that flow from every part to the other part. Where private and public clouds are accomplished, maintained and located on *either* organization *or* third party provider side. The users of hybrid clouds can be considered as trusted and untrusted. Untrusted users are prevented to access the resources of the private and community parts of the hybrid cloud.

- **Special purpose clouds**

Specialized functionalities are provided e.g. by the Google App Engine which provides specific capabilities dedicated to distributed document management. Similar to general service provisioning (web based or not), it can be expected that future systems will provide even more specialized capabilities to attract individual user areas, due to competition, customer demand and available expertise.
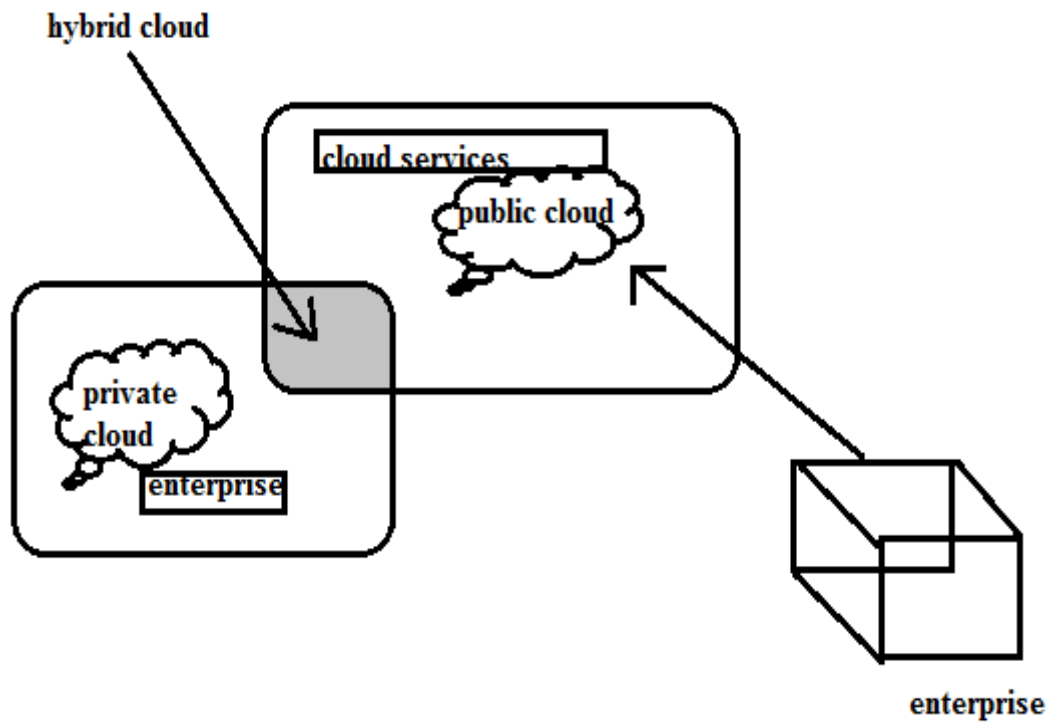
Fig 1.3: Public, Private, and Hybrid Cloud Deployment

1.4 Components of cloud computing

There are three components present in cloud computing. These are:

- Clients
- Datacenter
- Distributed servers.

In cloud computing every element in plays a definite role.
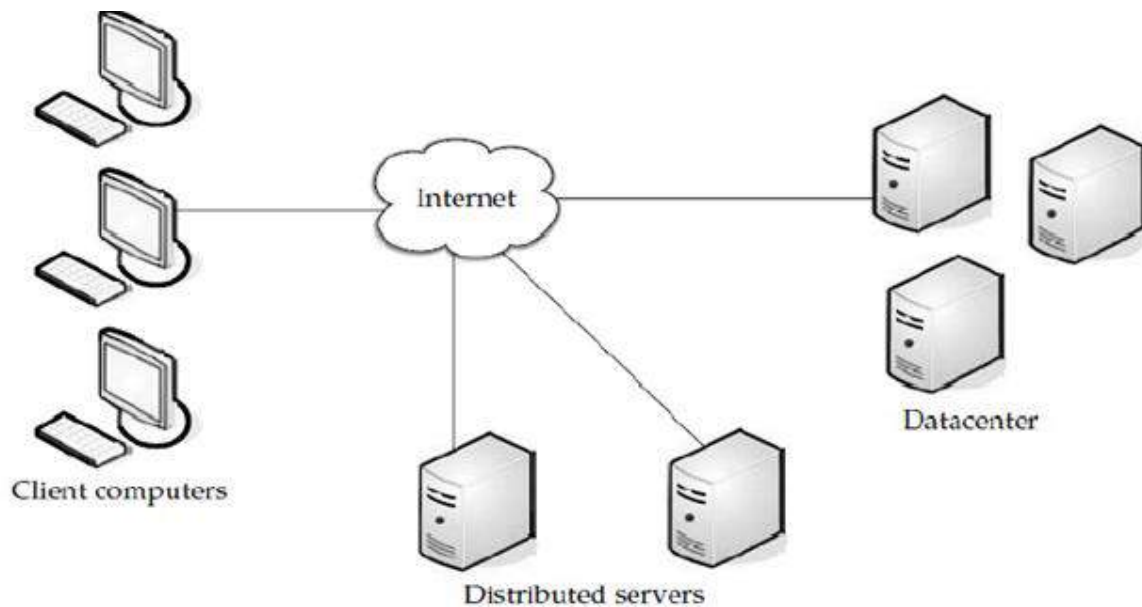
Fig 1.4: components of cloud computing

➢ **Clients** The end user managed the information in the cloud computing. They end users cooperate with the clients to manage information associated with clouds. The clients are described in three categories [4]:

➢ **Mobile Client:** First one is mobile client. These can be mobile in nature. It contains many mobile phones like windows mobile smart phone, like a Blackberry or I Phone and so on.

➢ **Thin:** Second type is Thin clients. These thin clients do not do computational work. They can use to show information. The internal memory is not present in thin clients. The servers do entirely work for the thin clients.

➢ **Thick:** The internet cloud is connected by using different browser from these clients. Internet cloud is connected by these browsers contains internet explorer, Mozilla Firefox or Google Chrome.

- **Datacenter**

It is a group of different servers; several applications are hosted by these servers. The datacenter is connected by the end user to subscribe different applications. It exists at a huge distance from the clients. Presently, the concept which is called virtualization is used to install a software that permit several instances of virtual server applications.

- **Distributed Servers**

These servers are the parts of a cloud computing, these are existing through the Internet. various applications are hosted by these distributed servers.

6

1.5 Connecting to the Cloud

There are many ways through which clients can connect to cloud service. The following are the common ways:

- A proprietary application
- A Web browser

These applications may run on mobile device, on pc, on a server.

Here are some methods for connecting over a connection securely:

- Use a safe protocol to relocate the data such as HTTPS, FTPS to connect the cloud to a client.
- Produce a virtual private network (VPN) connection by a remote data transfer protocol such as Microsoft RDP, wherever a tunneling device threatened the data.
- If the data is interrupted, it will not be meaningful if you had encrypt the data.

1.6 Benefits of cloud computing

Cloud computing have several benefits, these benefits are based upon the services and applications of the cloud computing.

- **Scalability**

The cloud computers are scalable in nature. One can start with a little deployment and grow to a large deployment according to the needs of the companies. The companies can scale back to its initial state if necessary.

- **Flexibility**

The flexibility of cloud computing allows for using various resources, whenever the customer demands the additional features. For customer the flexibility of the resources is needed.

- C**ost Savings**

Cloud computing helps the organization to decrease their capital expenditures and resources are used for increasing their capabilities of computing.

- **Reliability**

Cloud computing is more reliable because the services used in this can support business continuity and disaster recovery.

- **Maintenance**

The cloud service providers maintain the system as well. Application installation on the PC may be done automatically. The access of the system done through APIs directly.

- **Mobile Accessible**

Users of mobile have improved productivity due to systems available in an infrastructure present from everywhere.

1.7 Challenges of cloud computing

There are some of the challenges to be faced through cloud computing.

- **Security & Privacy**

The two of more hot button may issues surrounding cloud computing to storing and securing data. The cloud computing can be monitor by the service providers [1]. These issues of the cloud computing may responsible for slowing the deployment of cloud services.

- **Lack of Standards**

In the cloud computing, clouds have documented interfaces. Hence responsible for sub-standard cloud computing. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices.

- **Continuously Evolving**

The requirements of the user are changing from time to time, hence interfaces, networking and storage requirements are increased and decreased according to the need of person. This means that a cloud does not remain constant and is also continuously changing.

- **Compliance Concerns**

The Sarbanes Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used.

1.8 Using the Communications Services in cloud computing

In a cloud the communications services can expand their capabilities or stand alone as service. It also helps to provides new interactive capabilities to current services. Cloud based communications services enable to embed capabilities into business applications, such as Enterprise Resource Planning and Customer Relationship Management systems. The services of cloud computing can be accessed from anywhere and linked into current services to extend their capabilities.

1.8.1 Accessing through Web APIs

Communications capabilities into a cloud-based environment is achieved through APIs. It allows the development of the application outside the cloud to take advantage of the communication and infrastructure within it as well.
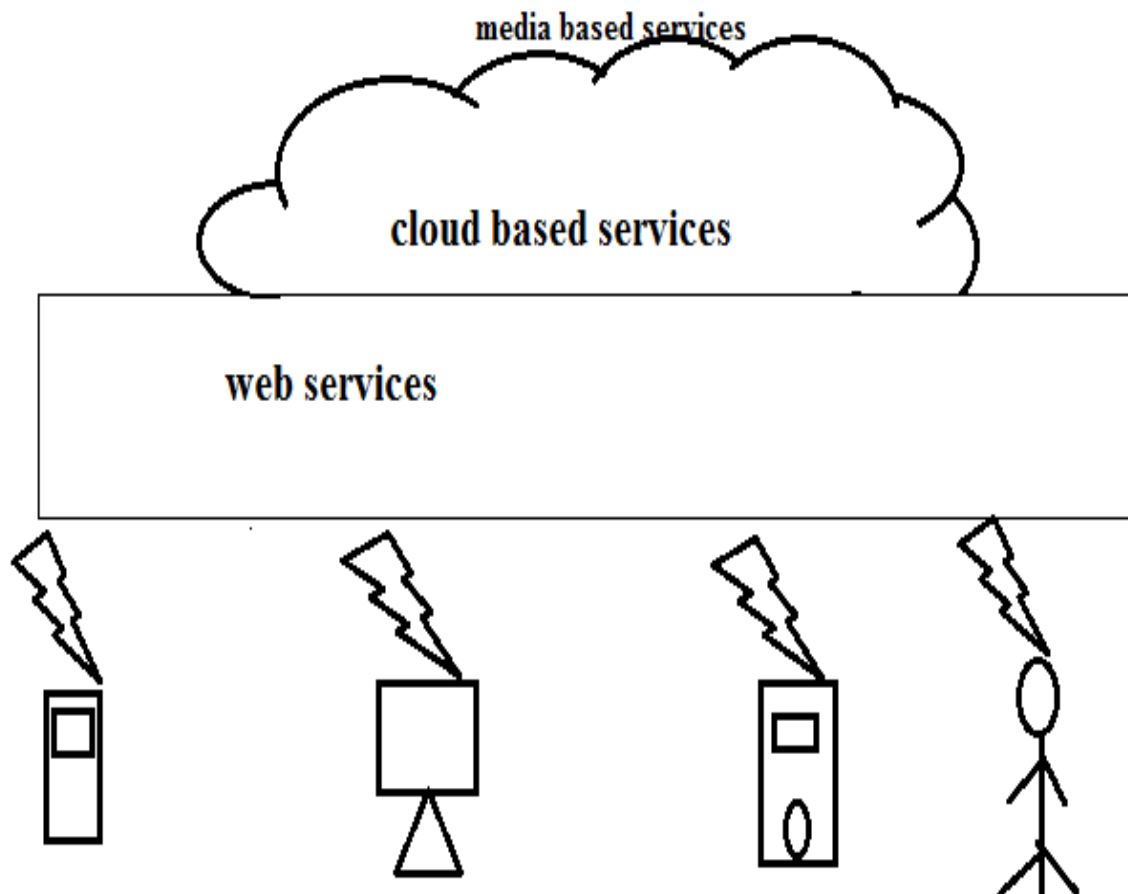
Fig1.5: Web 2.0 Interfaces to the Cloud

.1.9 Advantages of cloud computing

- **Scalability**

Cloud computing is scalable. Whenever a user needs more resources, the user can add it to anytime. It has infinite pool of resources.

- **Environment friendly**

Cloud computing makes full use of hardware as to reduce energy cost, hence it is environmental friendly too.

- **Cost efficient**

Cloud computing is cost efficient. We have to pay that much amount which we have used just like an electricity bill.

- **Up to date**

We need not to worry about the updates of the software and hardware using in the cloud. The provider updates overall process of all the components [5].

- **Improved performance**

In cloud computing high configuration resources are available on demand of user.

- **Availability**

The cloud service is distributed over multiple servers. The hosted applications nearby can be instantly between the infrastructures. In failure of server, the availability will be not be harmed.

- **Large load variations**

There are multiple servers and datacenters of the cloud computing. The cloud infrastructure can't give up, even If the applications of the cloud computing become very popular.

- **Timely and consistent updates**

The infrastructure among cloud computing needs to be fully consistent. Many customer applications are running side by side. A failure due to a patch is not something the cloud service will accept. So all servers will be very quickly and consistently updated.

- **Fast scaling out**

If your application has a great visit rate, then it wishes more servers to run on. In a cloud service it is very easy to implement a multi-server, multi-site environment.

1.10 Disadvantages of Cloud Computing

- **Custom platform**

The cloud service environment has specifics, like underlying operating system, databases, [6] application server and development platform. These are available across all over the entire cloud platform.

- **Lock in**

Once the full application is adjust to run on the particular cloud service environment, it may be problematic to transfer it to extra cloud service provider. Here the user has to readjust everything to run at the new cloud environment.

- **Isolation breach**

A breach among the control of isolation of dissimilar customers can cause access to exclusive data.

- **Data protection**

Sometimes data is very trusted in nature. Since the entire data is achieved through the service provider, incidents of loss of data, data leakages and safety breaches can completely happen.

- **Cost**

The service providers of cloud have a lot of inventive pricing devices, like pricing per I/O, Bandwidth, or their mixture. By this costs may be increased.

1.11 CLOUD SERVICE THREATS MODELS

The software cloud computing from several platforms sharing the similar platform which is maintained by the PaaS model providing by cloud systems.

Cloud provider. The cloud provider accepts the threat that the cloud infrastructure can be altered by the software which is mischievous. Outdoor malicious software can enter into the cloud and attacker can also act as service provider to corrupt the confidentiality of the cloud.[7]

Service provider once a service provider set up his software to the cloud, the one expenditure is on renting the source of cloud provider. But if malicious software act as a authentic software successively run on the similar hardware with the service providers software, it will get the chance to attack into the service provider's virtual environment. [8] For example worm virus. If it enters into the virtual environment of the service provider, it can produce several copies that lodge so abundant sources so that the service can not run accurately.

Service user when the cloud service shares with the public, the penetrating information will be increase incredibly with the growth of user's service in it user will have to submit his information for the service to applying it. Like in paypal to apply the service we have to submit about our account information.

1.12 CLOUD SUPPORT TOOLS

Such tools would cover issues related to:
A. Supporting to build up new platforms easily
B. New programming models and tools that deal with distribution and control
C. Enhanced features for provisioning, including respecting business obligations
D. Improved security and data protection
E. Efficient data management
F. Energy efficiency on all layers
G. Easy mash-ups of clouds exposing a single user interface etc.

1.13. Introduction to Water marking

Watermark technique is the technique that we use for information hiding behind the image as it stops illegitimate manipulation of the content. When the Intended node is not capable to extract the watermark from the content, it means that alteration has been done into the content. Watermarking holds a single identity that is only known by the node of source.

Images can be used to hide the data, key used to insert the data into the image is the one used for extracting the data. Data is hidden in the least significant bit of the image. It is not visible and naked eye cannot judge whether any content is hidden in the image or not. There is no difference in the original and the watermarked image.
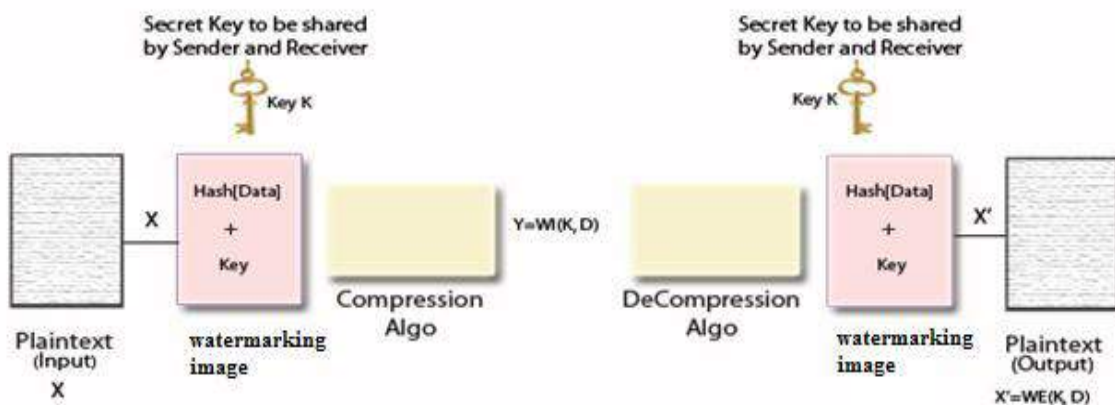
Fig :1.6 Watermarking process

At the Source End;

i.   Data is embedded into an image and a key is used to lock the content into the image.

ii.   Key is very essential as no key other than the one with which the data is locked can extract data from the image.

iii.   It will give two images as an output that seems to be identical. But in actual, one image is the original one and the other image is the watermarked image that hid the content in it.

iv.   Before the transmission of the image over the network, it is compressed as it would consume less bandwidth and other resources.

v.   Compression takes place at the sender end in which dimensions of the image are made half to its actual size. It has no effect on the content hidden in it.

vi.   Image is then transmitted over the network.

At the Destination End;

i.   Compressed image is received at the destination end.

ii.   Compressed image is then decompressed to bring the dimensions of the image back to the original size.

iii.   Key used for insertion of data in the image is used at the destination end to extract the data from the image.

1.12.1 FEATURES AND APPLICATIONS

FEATURES:

Data hiding techniques must hide the data with following restrictions and features:

- The secret data should not be embedded in the external cover rather than we have to embed data in the image itself.
- The data in the image should not be modified by anyone.
- Secret data embedded in the images when extracted should not vary from actual data.

APPLICATIONS:

There are various areas where we use watermarking

- Watermarking, Applications where the embedded data can be used as the replacement to a watermark.
- Tamper-Proofing is an application where data hiding can be used. It ensures that some modifications had been done into the embedded data.
- Feature Location, in which the data is hidden at specific location in image. It enables us to find the different content features e.g. name, Id of a person.
- Finger Print, The data set embeds a serial no which uniquely identifies the User data set. If anyone will try to copy that print it can easily be proven by extracting the finger print key.
- Copyright protection, copyright notice can be embedded into the image. If someone will try to use the image it can be easily proven by extracting watermark
- It is used in Media Database systems.
- Access control system for digital content distribution

CHAPTER 2

REVIEW OF LITERATURE

In chapter 2, we are going to present some work of research done in the field of cloud computing. In the given field of cloud computing several researchers has been work on the security of cloud computing with watermarking techniques as it is the simplest method of data hiding. Researches purposed various approaches to increase the security and the quality of the image.

Cong Wang et.al, in the given paper, author talk over the security about cloud computing. It entails the architecture of IT enterprise. The cloud computing has numerous benefits in the field of information technology: on request self service, global network access, location librated resource pooling, fast resource elasticity, usage-based pricing and conversion of risk. [9] Cloud computing carries the fresh and inspiring security threats towards consumer's subcontracted data. For this resolution, cloud service providers are castoff. These are the distinct administrative entities. The data perfection the great matter in cloud computing. For the cloud computing, third party assessor is castoff. It customs the two formost requirements as: the third party assessor should be capable to Proffesionally review the storage of cloud data without challenging the data of local copy and the reviewing process must bring in no new liabilities to the consumers privacy of data. Here author talk about the public key based homomorphism authenticator. For this the random masking is castoff. It supports to attain the privacy preserving public cloud data auditing system, which come across wholly requirements. (Cong Wang, 2010)

Ryan K. L. Ko et.al,: in the given paper, author talks about the many schemes about cloud computing that are used in the security. Cloud computing indicates a paradigm shift from owning computing systems to buying the services of computing. In the given paper, author inspires the file centric adoption and logging mechanisms of data centric. [10] It supports in growing the accountability. The cloud computing security is a big issue. So For this drive, the cloud is accesses by the data transparency and absence of clearness in data ownership were textured. For this author purpose a fresh scheme, which supports in providing cloud computing security. This new scheme finds out the numerous

approaching trust problems and traditional security. So here the approach of data centric is use, which supports in increasing trust and cloud data security. **(Ryan K. L. Ko, 2011)**

Shuai Han et.al, In the given paper, author talks over the usages of third party auditor scheme. The technology of Cloud computing turns as architecture of next generation of IT solution. It permits the consumers to relocate their data and application software to the network that is totally different from traditional solutions. [11] Cloud computing offers the numerous services about IT, due to which it contains several tasks of security. The security of storage of data is the big cloud computing issue. In the given paper, author talks about a fresh scheme named auditor of third party. It supports in giving the trusted confirmation to consumer. (**Shuai Han, 2011)**

Jen-Sheng Wang et.al, in the given paper, author talks over the numerous approaches and processes that supports in handling the cloud computing security. The security of information is serious matter in the Internet phase. [12] The secured information is appreciated and vital. The security of information that has been made by cloud computing handling a very important and serious matter. In cloud computing the information security requires several influences. In the given paper, the significant issues of achievement are castoff. Those issues contains several parts as: first is external dimension, second is internal dimension, third is technology dimension, and other one execution dimension. A fresh scheme is purposed by those issues, which is castoff to overwhelmed the several difficulties those are associated to the security in the cloud computing. (**Jen-Sheng Wang, 2011)**

Pradeep Bhosale et.al, discuss that present world be dependent on cloud computing to stock their public as well as some private information which is required by the user themself or some additional persons. Service of cloud is that offered services to his users by cloud. As computing of cloud arises in service there are various problems such as privacy of user's data, security of user data is very significant aspects. In this paper author discuss about the enhancement of security of the data. Not only this marks researchers to make selected alterations in the current structure of the cloud, discover new model about cloud computing and much more but also there are some features of cloud computing that mark him as a super power.[13] To enhance the security in cloud computing used the 3 dimensional framework and digital signature with Encryption algorithm of RSA. In 3 Dimensional frameworks, at client side user choice the parameters reactively between CIA (Confidentiality, Integrity & Availability) and earlier actual

storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud. **(Pradeep Bhosale ,2012)**

Jasmin James et.al, converse about the security in cloud computing. Cloud computing is fast increasing area in the research computing. Through the progression of the Cloud, several different opportunities are coming into picture, like how applications can be constructed and how dissimilar services can be accessible to the end user by Virtualization. There are the providers of the cloud services who provide large scaled computing infrastructure well-defined on usage, and provide the service infrastructure in a very flexible manner. The virtualization customs the foundation of cloud technology where [14] Virtualization is an evolving IT paradigm that separates computing functions and technology implementations from physical hardware. Through virtualization, servers can be access by the user without knowing specific detail about the server. The virtualization layer will execute request of user for computing resources by accessing appropriate resources. In this paper, author firstly analyses the changed Virtual Machine (VM) load balancing algorithms. Secondly, a new VM load balancing algorithm has been proposed and executed for an IaaS framework in simulated environment of cloud computing. **(Jasmin James, 2012)**

Pengfei Dai et.al**,** in this paper author discuss about the importance of software watermark based architecture in cloud computing for its security needs. As it has now emerged as a resource sharing platform for different service providers. One must provide necessary security protection against the threats of critical data processing and e-business, a software watermark enhanced platform should be proposed to run the platform. Cloud computing also introduces significant security concerns. In this paper author proposed an architecture which employs software watermarking method to reduce the threats for security risks. In this architecture RAWS is designed to choose the proper watermarking algorithms based on the user's requirements and the JVM is customized to verify the validity of that software in the cloud. Experiments shows that the architecture is feasible for low performance slowdown. Software watermark architecture also protect more software applications such as java programs, c-c++, python etc. in the cloud.[15]

(Pengfei Dai, 2012)

Tejinder Sharma et.al, in the given paper author talks over the cloud computing. As, the computer networks are still in their initial stages, but they evolve and develop sophisticated. Cloud computing is developing as a original paradigm of large scale dispersed computing. It has stimulated computing and data away from desktop and portable PCs, into large data centers. It has the capability to connect the power of Internet and wide range area network to custom resources that are obtainable remotely.[16] There are numerous security issues in the cloud computing. In this paper, author discuss about the number of scheduling problems. One of the inspiring scheduling problems in Cloud datacenters is to take the allocation and immigration of reconfigurable virtual machines into deliberation as well as the united features of introducing physical machines. In order to select the virtual nodes for performing the task, Load balancing is a procedure to allocate workload through manifold computers. The key objective of this paper to propose efficient and improved scheduling algorithm that can preserve the load balancing and provides better upgraded strategies through effectual job scheduling and reformed resource allocation techniques.

(Tejinder Sharma, 2013)

.Sonal Guleria, Dr. Sonia Vatta et.al, In this paper, author describes that the Cloud computing is developing field because of its presentation, great obtainability, minimum cost and many others. In cloud computing, the data will be kept in storage provided by service providers. Cloud computing offers a computer consumer access to Information Technology (IT) services which comprises applications, servers, data storage, without requiring an understanding of the technology. An equivelance to an electricity computing grid is to be convenient for cloud computing. To allowing suitable and on-demand network access to a common pool of configurable computing resources are castoff for as a model of cloud computing.[17] Cloud computing can be stated as a grouping of Software-as-a-Service which denotes to a service delivery model to enabling castoff for business services of software interface and can be shared by producing fresh business services distributed using flexible networks and Platform as a Service in which Cloud systems contribution an additional construct level which delivering a virtualized infrastructure that can provide the software platform where systems should be run on and Infrastructure as a Service which Providers accomplish a large set of computing resources which is castoff for loading and handeling capacity. But still various business companies are not keen to accept cloud computing technology due to absence of appropriate security control policy and dimness in safeguard which lead to several susceptibility in cloud

computing. This paper has been written to attention on the problematic odata security. To confirm the security of consumers' data in the cloud, we recommend an actual and flexible scheme with two dissimilar algorithms .A consumer can access cloud services as a convenience service and initiate to use them almost immediately. These features that create cloud computing so flexible with the detail that services are reachable everywhere every time lead to more than a few possible risks. The significant concentrating of this research work is to explore the current security schemes and to make sure data confidentiality, integrity and authentication.

(Sonal Guleria, Dr. Sonia Vatta, 2013)

Yan Yan, Xiaohong Hao et.al, **[18]** In this paper, author talks about the privacy and security issues in mobile cloud computing. The technology of cloud computingis an important growth point of IT industry. A computer network is the collection of large number of computer resources, storage resources and software resources. Cloud computing has the many applications as it breaks the traditional one to one service. It helps to provide unlimited, scalable and easy access to the IT resources. Mobile cloud computing refers to the delivery and using patterns of infrastructure, platform, software of IT resource by mobile network according to the real demand and in a scalable way. [17]The mobile communication technology growing day by day, hence information and services from internet are needed from anywhere during the movement. (**Yan Yan, Xiaohong Hao, 2014**):

PRESENT WORK

In this chapter, we are going to present the problem of our research work, its objectives, the methodology that we used for our purposed approach and the introduction of the developed tool. In the 3.1 section we explain how we formulated our problem and what the approach we are going to use. In the 3.2 and 3.3 section the objectives and the methodology of the work done. In the methodology the flow of our work with the help of flow chart is explained.

3.1 PROBLEM FORMULATION

As cloud computing which brings many benefits when occurs as platform of resource sharing. It also hosts major security concerns. In our work the technique of watermarking had been applied in cloud computing. The watermarking technique had provide extra security to cloud data.

Watermarking is the process of hiding the data or secret message inside the cover image to protect our information from the hackers. The watermarking is the technique which will applied for providing security to cloud architecture. In our research work various techniques like singular Value (, Discrete Cosine Transformation and Discrete Wavelet Transformation(DWT) had been used to generate watermark image. The SVD technique had been applied first to generate watermarked image, after that DCT technique is applied to reduce MSE value and increase PSNR value of the watermarked image, to further reduce the MSE value and increase the PSNR value of image DWT technique will be applied.

Peak signal to noise ratio(PSNR) is used to measure the quality of the reconstruction of lossless compression for example image compression. The signal in this case is original data and noise is the error introduced by the compression. PSNR is most easily defined by the mean square error(MSE).

In this work, The data will be received by the end user, the user extract the original data from the watermarked data some noisy data left behind which increase MSE value and reduce PSNR value. In purposed work first we will apply some attacks like sharpened attack, contrast attack and salt & pepper attack on original image to check the robustness of the image. After that to remove noise from that data, technique of KALMAN filter had

been applied. The Kalman filter will help to decrease the value of MSE and increase the value of PSNR so that the quality of the watermarking image can improve. The kalman filter will help to increase the quality of the watermarking image as well maintaining its security.

3.2 OBJECTIVE

Objective function of the project is:

1) To study and explore the robustness and vulnerabilities of digital watermarking for cloud computing.

2) To implement SVD-DCT-DWT watermarking technique for cloud computing and analyze results in terms of PSNR & MSE.

3) To purpose enhancement in SVD-DCT-DWT techniques using KALMAN filter to improve PSNR & MSE value for cloud computing.

4) To implement proposed techniques and compare PSNR & MSE value with existing technique.

5) To maximize the PSNR (Peak Signal to Noise Ratio) and minimizing the MSE (Mean Square Error).

3.3 METHODOLOGY

1. To study the various watermarking techniques there are many techniques present. These various techniques are Discrete Wavelet Transformation, Discrete Cosine Transformation and singular Value Decomposition.

2. To implement the DCT-SVD technique and analysis the processing time computational power and robustness of the algorithm against security attack.

3. To calculate the PSNR value of the DCT-SVD technique.

4. The enhancement will be made in SVD-DCT-DWT technique by applying Kalman Filtering to reduce MSE value and increase robustness of the algorithm.

5. The existing DCT-SVD technique and enhanced DCT-SVD technique will be implement and results of PSNR value and robustness will be compare graphically and in tabular form.

1. **Kalman Filtering:** In radio communication systems, filtering is a desirable factor. As radio communication signals are often corrupted with noise, a good filtering algorithm is required to remove noise from electromagnetic signals while

retaining the useful information. Kalman Filtering is an effective method to filter impurities in linear systems. The Kalman filter basically consists of a set of mathematical equations that provides an efficient computational means to estimate the state of a process that minimizes the mean of the squared error. It operates recursively on streams of noisy input data to produce statistically optimal results The filter is very powerful in several aspects: it supports estimations of past, present, and even future states, and it can do so even when the precise nature of the modeled system is unknown.

2. **Gabor Filtering:** The images are filtered using the real parts of various different Gabor filter kernels. The mean and variance of the filtered images are then used as features for classification, which is based on the least squared error for simplicity.

3. **Salt and Pepper Filtering:** We consider salt-and-pepper noise, for which a certain amount of the pixels in the image are either black or white (hence the name of the noise). Salt-and-pepper noise can, e.g., be used to model defects in the CCD or in the transmission of the image. Given the probability r (with $0 \le r \le 1$) that a pixel is corrupted, we can introduce salt-and-pepper noise in an image by setting a fraction of r/2 randomly selected pixels to black, and another fraction of r/2 randomly selected pixels.

The anti process will be followed to retrieve data. User will use anti-watermarking algorithm to retrieve key then use one detection algorithm to fetch information from image and by using this key user will decrypt it.

3.3.1 FLOW CHART OF PURPOSED APPROACH

In this part we are presenting flow chart of purposed approach. In this purposed approach We Deploy cloud computing network with the finite number of users. Then User send credentials to upload data on cloud. After verified the credentials apply SVD-DCT-DWT technique to get the watermark image. Then apply salt-pepper, contract and sharping attack on the watermarked image to check robustness. Then Send watermarked image to the cloud. Cloud will extract watermark and original image. Apply KALMAN filter to image quality of original image. The image we obtained from the filter is the image free from noise.
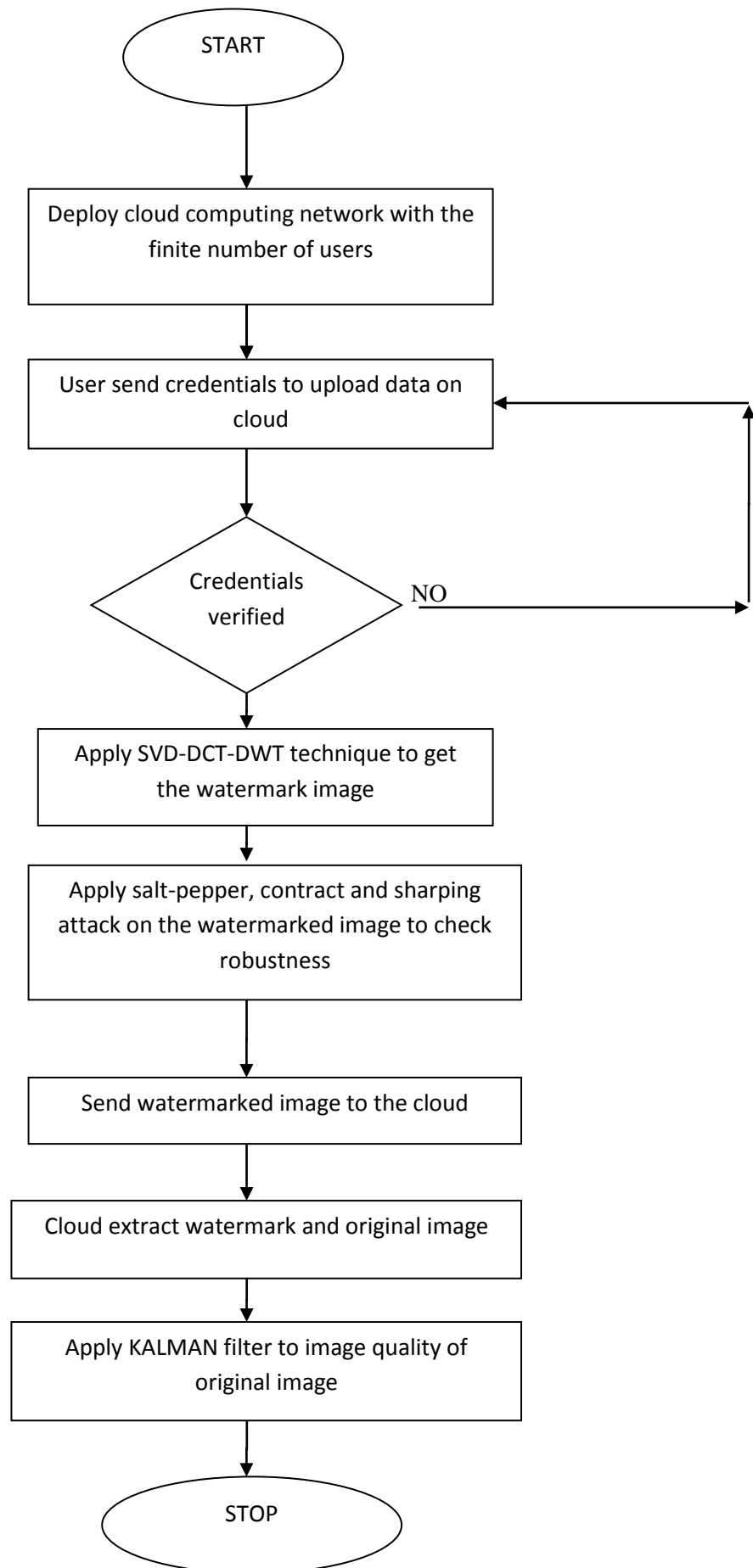
```
                    ┌─────────────┐
                    │    START    │
                    └─────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ Deploy cloud computing network with the │
        │         finite number of users         │
        └──────────────────────────────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ User send credentials to upload data on │◄──────┐
        │                 cloud                  │        │
        └──────────────────────────────────────┘        │
                           │                              │
                           ▼                              │
                    ╱─────────────╲        NO             │
                  ╱   Credentials   ╲ ─────────────────────┘
                  ╲    verified     ╱
                    ╲─────────────╱
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ Apply SVD-DCT-DWT technique to get      │
        │         the watermark image            │
        └──────────────────────────────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ Apply salt-pepper, contract and sharping │
        │ attack on the watermarked image to check │
        │               robustness               │
        └──────────────────────────────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │     Send watermarked image to the cloud │
        └──────────────────────────────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ Cloud extract watermark and original image │
        └──────────────────────────────────────┘
                           │
                           ▼
        ┌──────────────────────────────────────┐
        │ Apply KALMAN filter to image quality of │
        │            original image              │
        └──────────────────────────────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │    STOP     │
                    └─────────────┘
```

Fig: 3.1 Flow chart of purposed technique

3.4 MATLAB

MATLAB stands for **"Matrix Laboratory"**. MATLAB is a high level language. It is a program for doing numerical computation, analyzing images and data. It was originally designed for solving linear algebra type problems using matrices. Its name is derived from Matrix Laboratory. It helps us in solving the problems faster than other languages and used in various applications such as signal processing, image processing, communications, computational biology and control design. MATLAB system has following these parts:

➢ Desktop tools and development environment

➢ Mathematical function library

➢ The language

➢ Graphics

➢ External interfaces

3.4.1 FEATURES OF MATLAB:

- Environment for managing the code, files and data.
- 2-D and 3-D graphics functions for analyzing the data.
- Provide interactive tools for solving problems.
- Provide functions for integrating the MATLAB based algorithms with external applications.
- High level language.
- It helps in solving the problems faster than other languages.

3.4.2 STANDARD WINDOWS IN MATLAB:

➢ **Command Window**: - The window where you type and execute commands.

➢ **Workspace Window**: - This shows current variables and allows to edit variables by opening array editor (double click), to load variables from files and to clear variables.

> - **Current Directory window**: - this shows current directory and MATLAB files in current folder, provides with a handy way to change folders and to load files.

> - **History window**: - This shows previously executed commands. We can re-execute the Commands by double-clicking

3.4.3 MATLAB HELP

> - Help option is present on the top of the window in the right side.
> - MATLAB help is a powerful way for learning the MATLAB.
> - It not only contains the theoretical background, but also shows demos for implementation.
> - We can search any command by typing in the search box.
> - It explains the commands searched by you with examples.

In MATLAB Supported Image Format:
> - PCX
> - HDF
> - JPEG
> - TIFF
> - XWB

In MATLAB Formats Of Working:

First of all we read the image into the MATLAB if the JPEG-image is stored on the disc. We have to convert image into different formats when we start working with an image. For example when On an image to perform a wavelet transform. There are some common formats.

Formats in MATLAB:
> - Binary images or black & white images: {0, 1}
> - Intensity images or grey scale images: [0, 1] or uint8, double etc.
> - RGB images: $m \times n \times 3$
> - Multidimensional images: $m \times n \times p$ (p is the number of layers)

RESULTS AND DISCUSSIONS

In this chapter we have presented various results of the images with our purposed approach with snapshots and compared with the existing work done. We have performed various experiments on the purposed method.
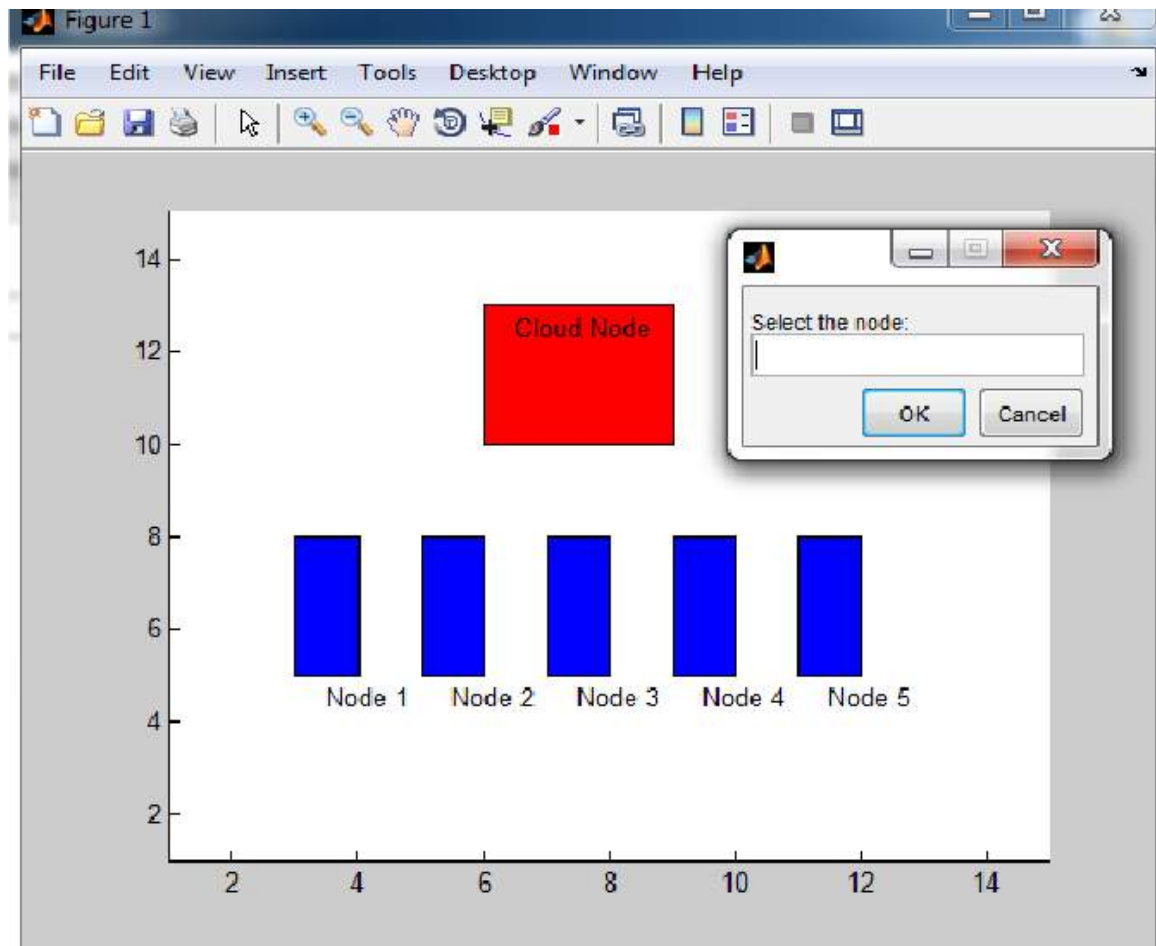
Fig. 4.1 The cloud node and user nodes are Node1, Node2, Node3, Node 4 and Node5.

In fig 4.1 First of all select the user node with which we want communicate with cloud node.
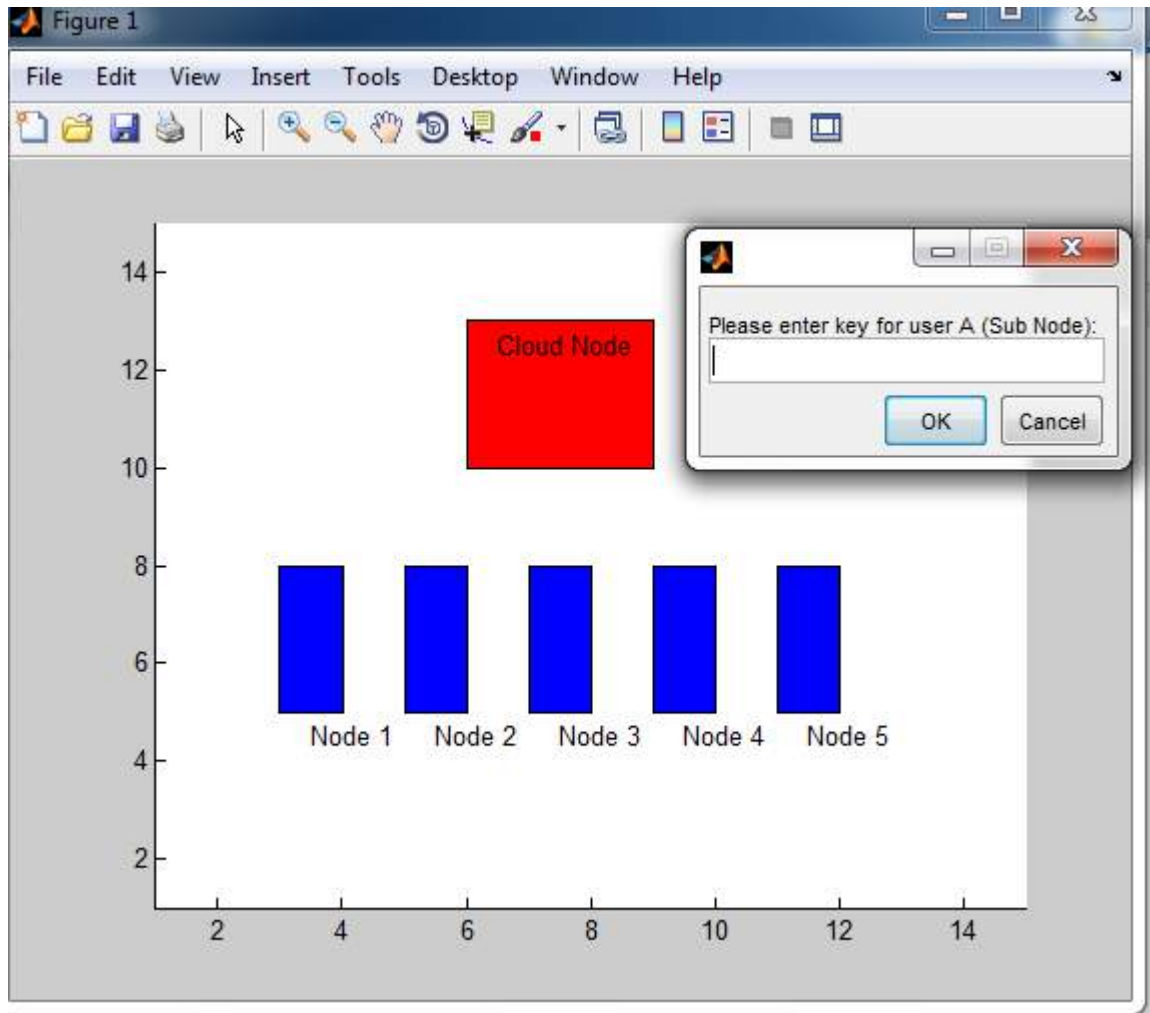
Fig 4.2 selecting sub node key for sub node

In fig 4.2 after selecting the user node enter any key for that user A that is sub node.
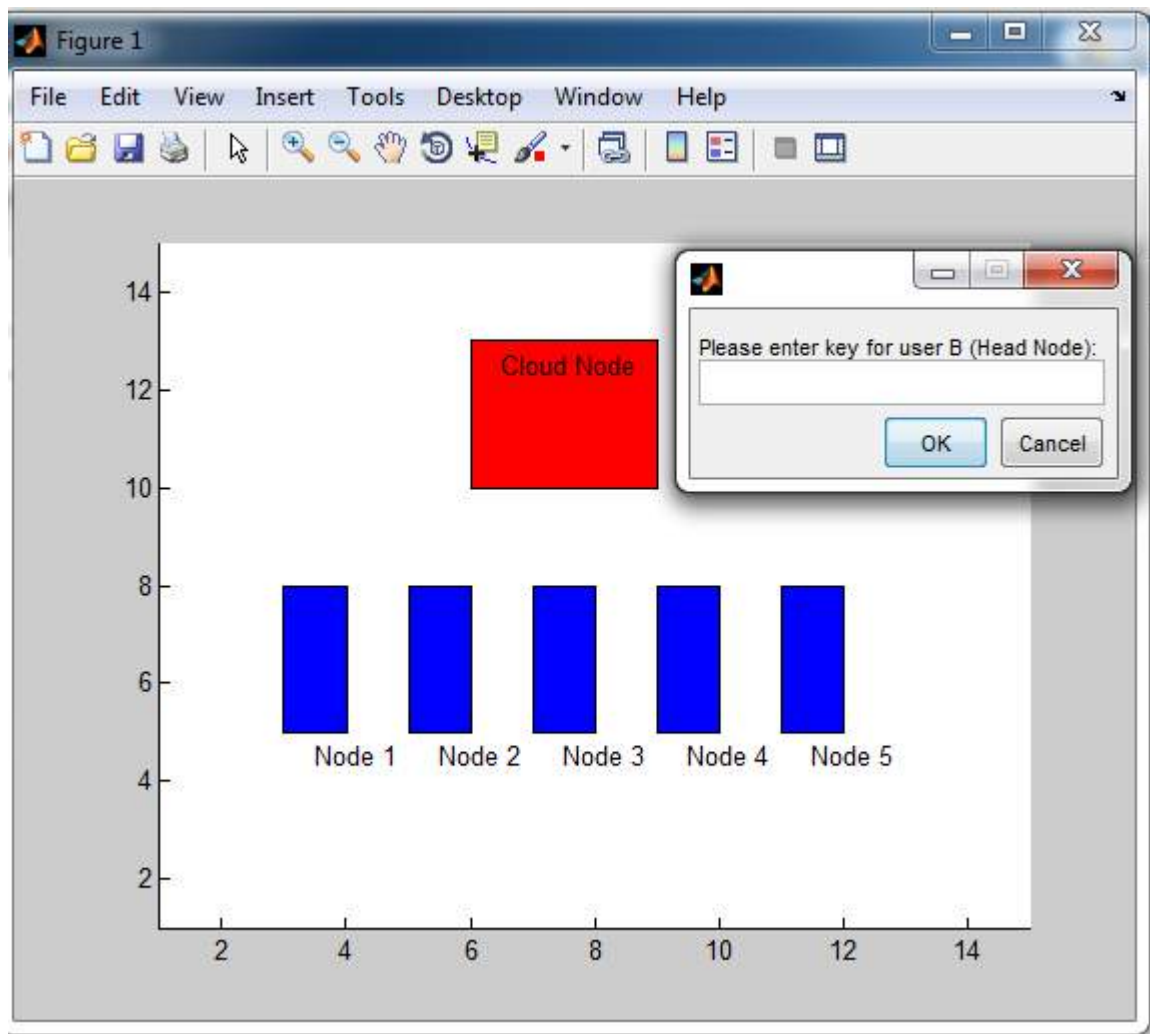
Fig. 4.3 Selecting key for head node

In fig 4.3 after entering the key for user A the same key have to be entered for user B that is Head node. And enter input number.
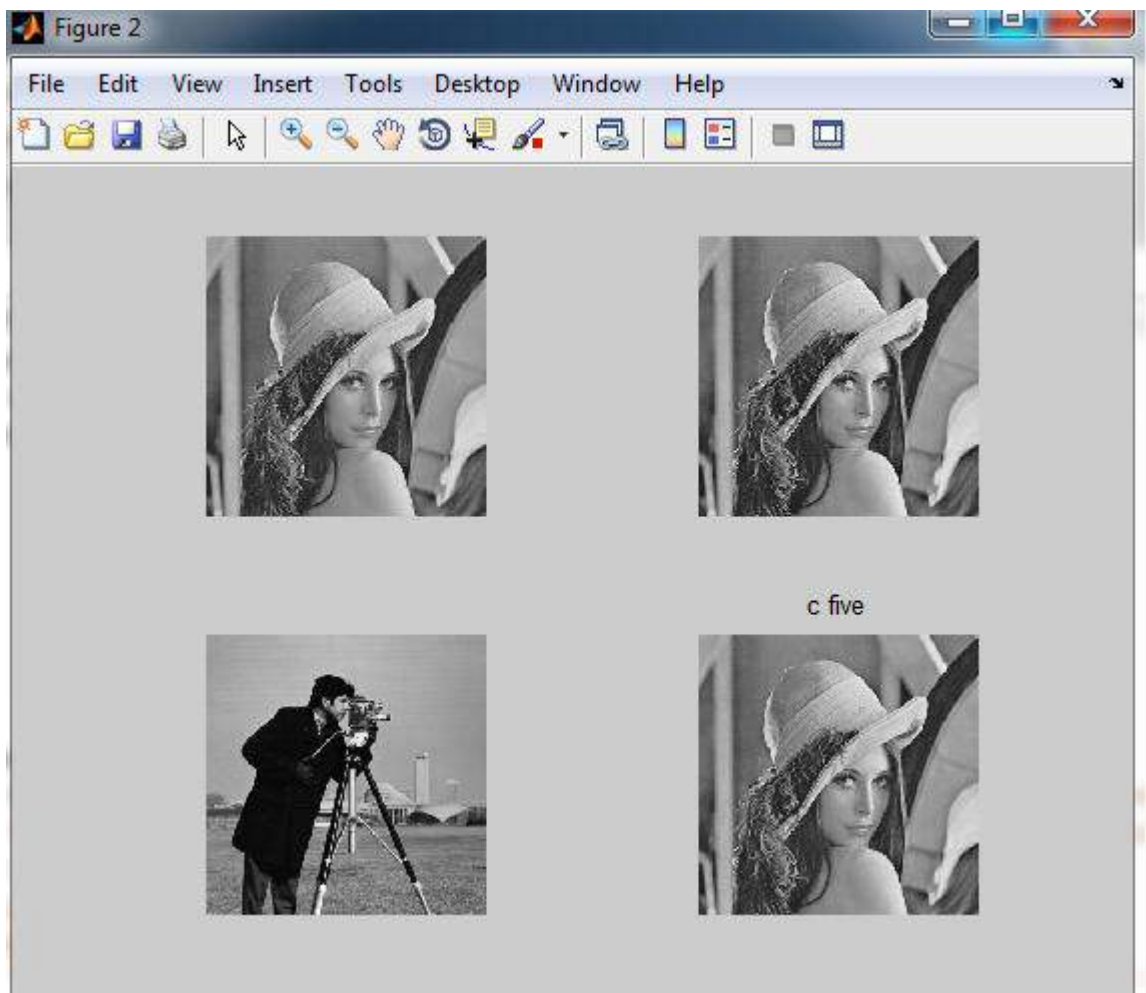
Fig. 4.4 The cover images used are Image1 , Image2 , Image3 and Image4.

In fig. 4.4 there are 4 images, image1 is original image, image2 is watermark image, image3 is input image and image4 is watermarked image.
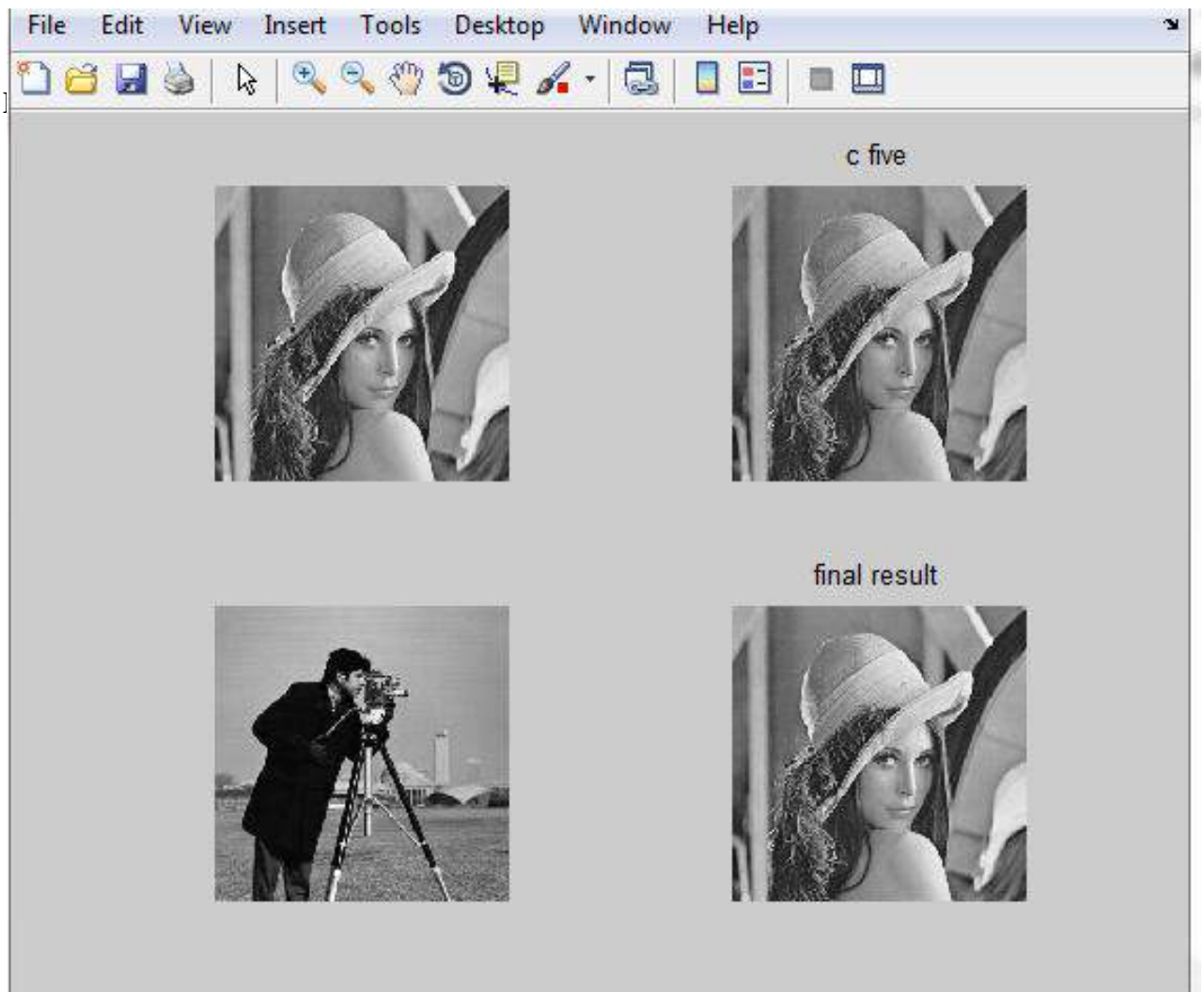
Fig 4.5 Results of purposed Approach using different images in matlab

In this section we presented the results for hybrid approach. We analyzed the four images that are image1, image2, image3, and image4.

Results for the image : Below shown fig. is the watermarked image.
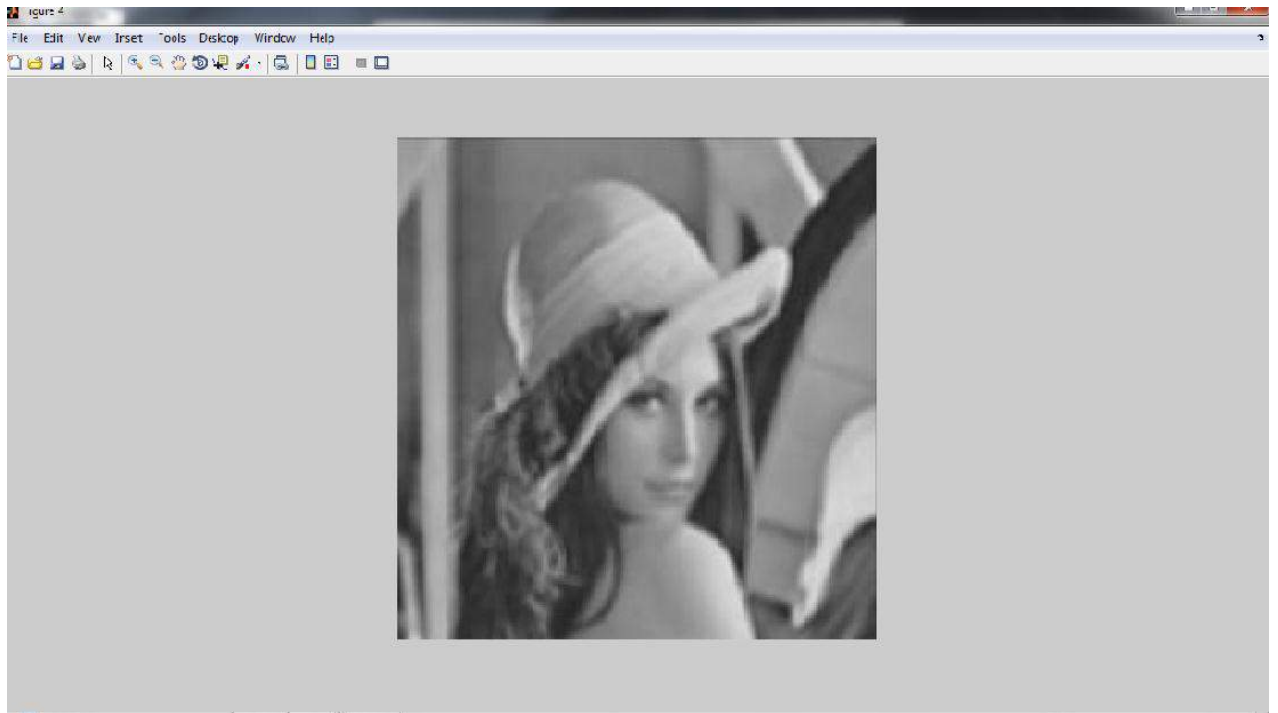
Fig. 4.6 watermarked image

We use the PSNR to evaluate the performance. Calculated PSNR values and MSE values of the Watermark image are shown in fig.4.6

Below snapshot figure of the calculation of the PSNR, MSE value of watermark image.

The mean square error is 250.95.
The PSNR of watermark image = 251.00The mean square error is 251.00.
The PSNR of watermark image = 24.17The mean square error is 24.17.
The PSNR of watermark image = 24.17

OK
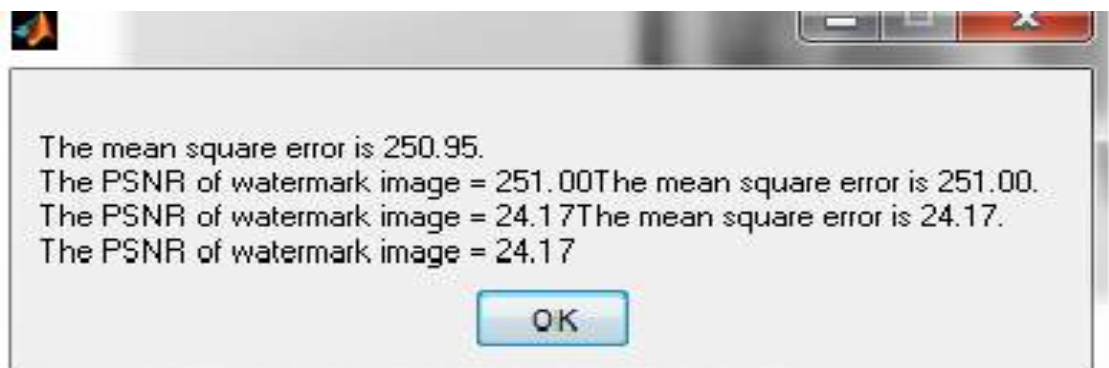
Fig. 4.7 PSNR and MSE values watermark image.

Below shown figure showing the filter of the image.
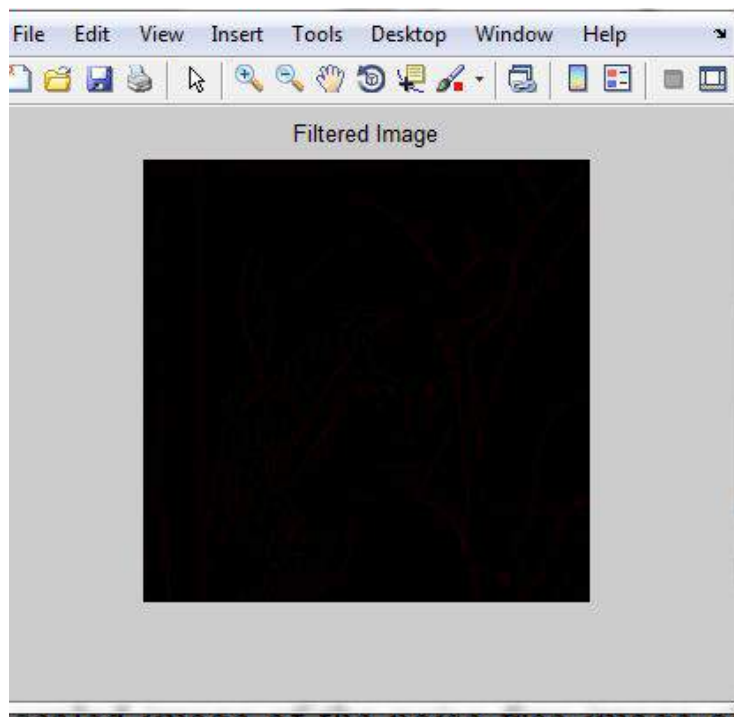
Fig. 4.8 filtered image

Below shown figure is showing the noise free image that we obtain after passing the cover image from the filter.
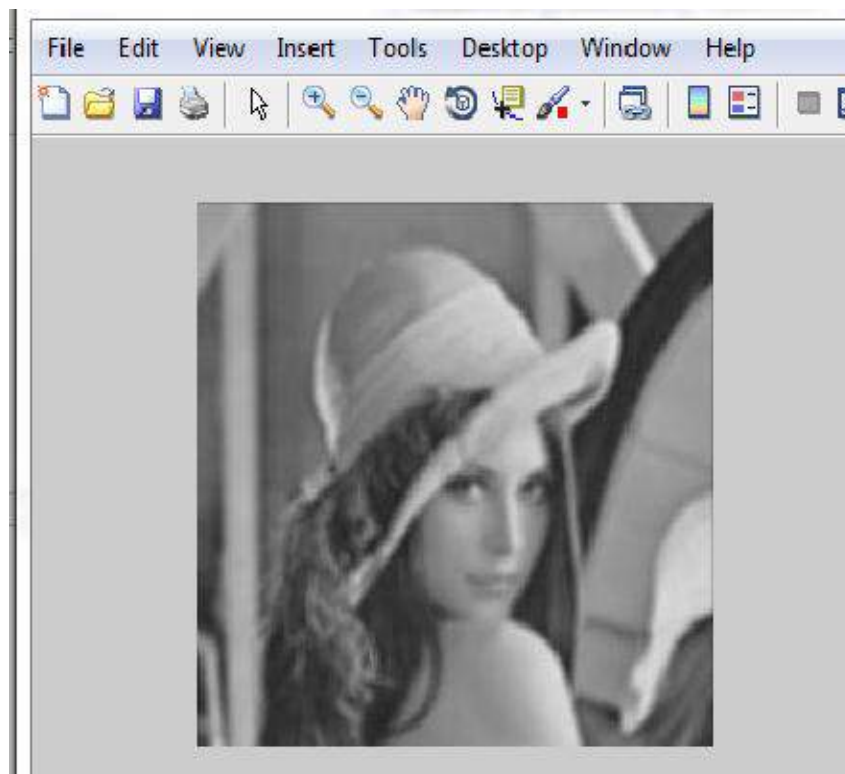
Fig. 4.9 Noise free image passed through the filter

Below shown figure is showing the original image that we passed through the sharpened attack.
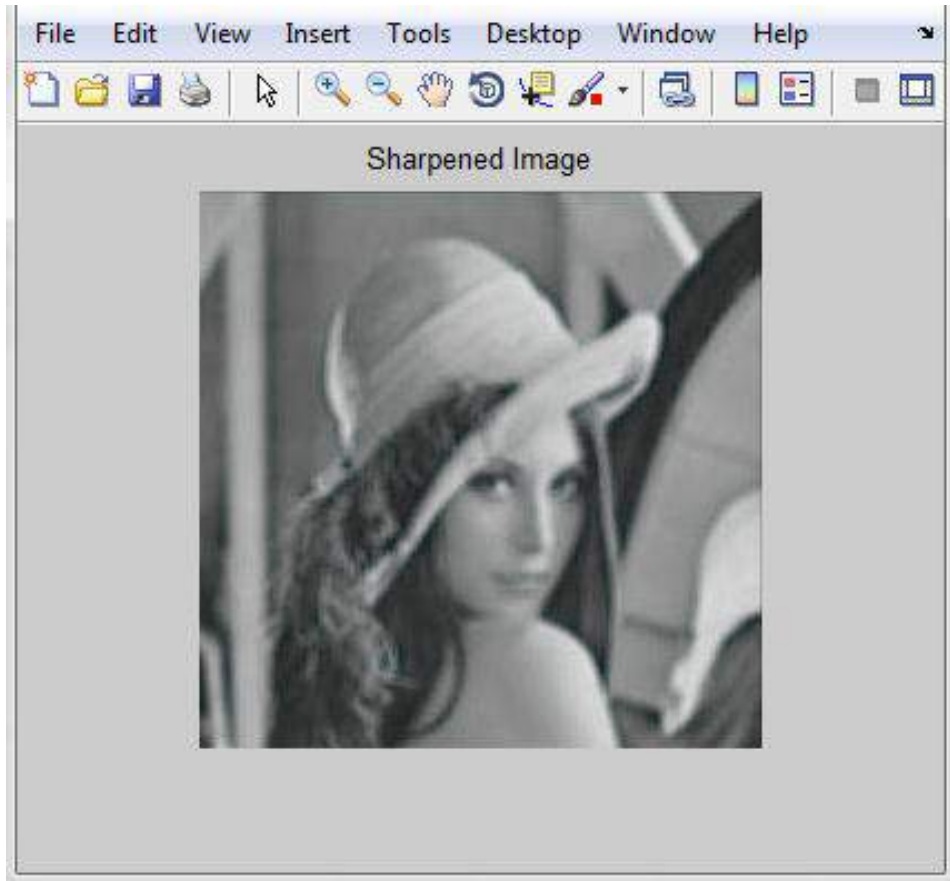
Fig. 4.10 sharpened image

In fig. 4.10 we will apply sharpened attack on the original image to check the robustness of the image**.**

Below snapshot figure of the calculation of the PSNR, MSE value of sharpened image.

The mean square error is 65.49.
The PSNR of sharppen image = 64.86The mean square error is 65.32.
The PSNR of sharppen image = 30.00The mean square error is 30.04.
The PSNR of sharppen image = 30.01

OK
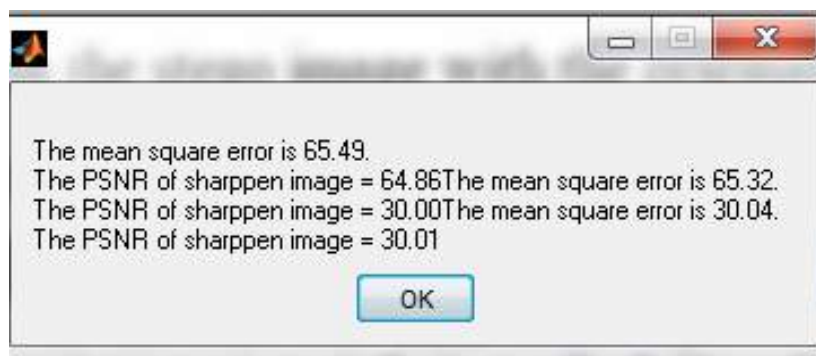
Fig.4.11 PSNR and MSE values of sharpened image

Below shown figure is showing the contrast image after applying contrast attack to the original image.
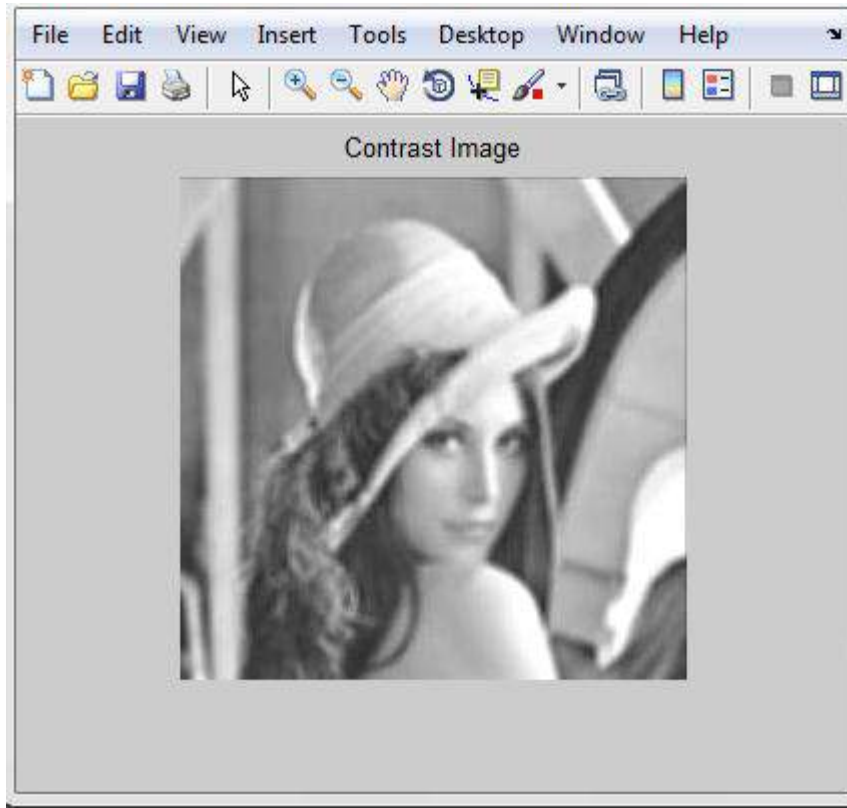
Fig. 4.12 contrast image

As shown In fig. 4.12 we apply contrast attack on original image again check the robustness of the image.

Below snapshot figure of the calculation of the PSNR, MSE value of contrast image.
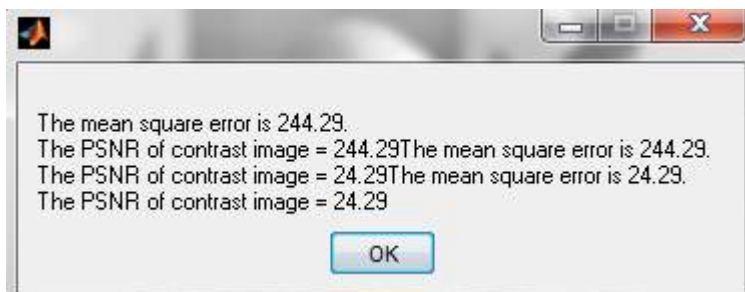
Fig. 4.13 PSNR and MSE values of contrast image

Extracted two images watermark and original image after applying contrast attack
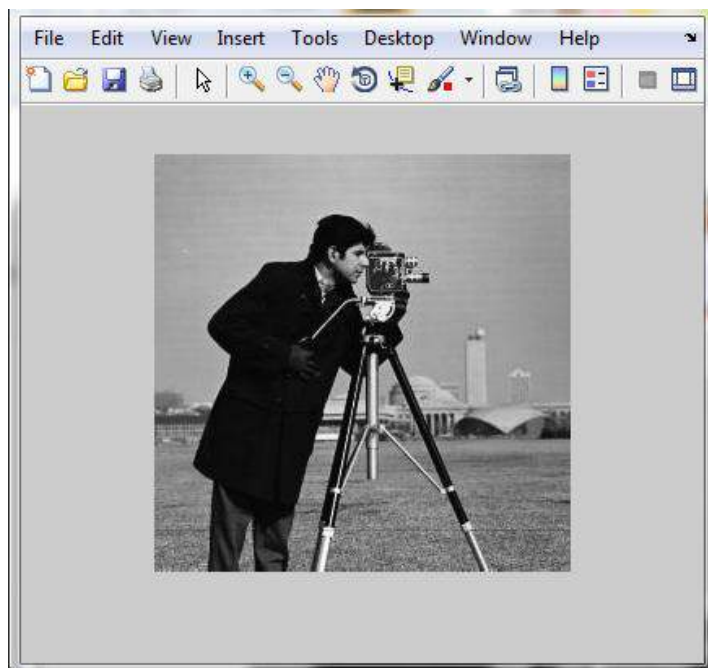
Fig. 4.14 extracted watermark image
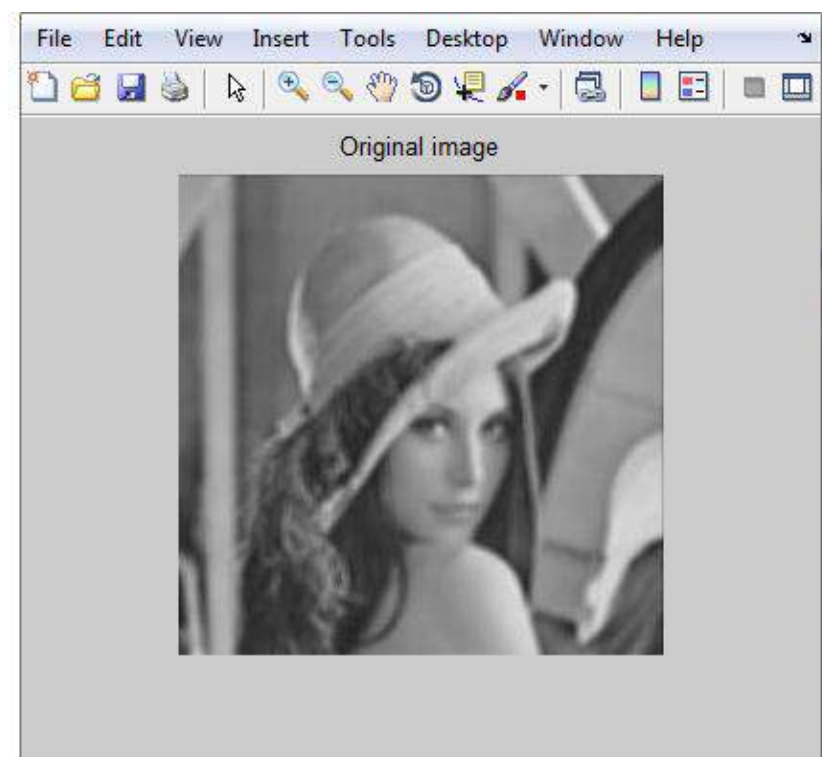
Fig.4.15 extracted original image

In fig. 4.15 after applying contrast attack we will extract two images one is watermarked image another one is original image which is given below**.**

Below shown figure is showing the watermarked image after applying the salt and pepper attack.

watermark image after Salt and Pepper attack

Fig. 4.16 watermark image after salt and pepper attack.

Below snapshot figure of the calculation of the PSNR, MSE value of watermark image.

after salt and pepper attack

The mean square error is 64.87.
The PSNR of salt&pepper = 64.83The mean square error is 64.89.
The PSNR of salt&pepper = 30.04The mean square error is 30.05.
The PSNR of salt&pepper = 30.04

OK
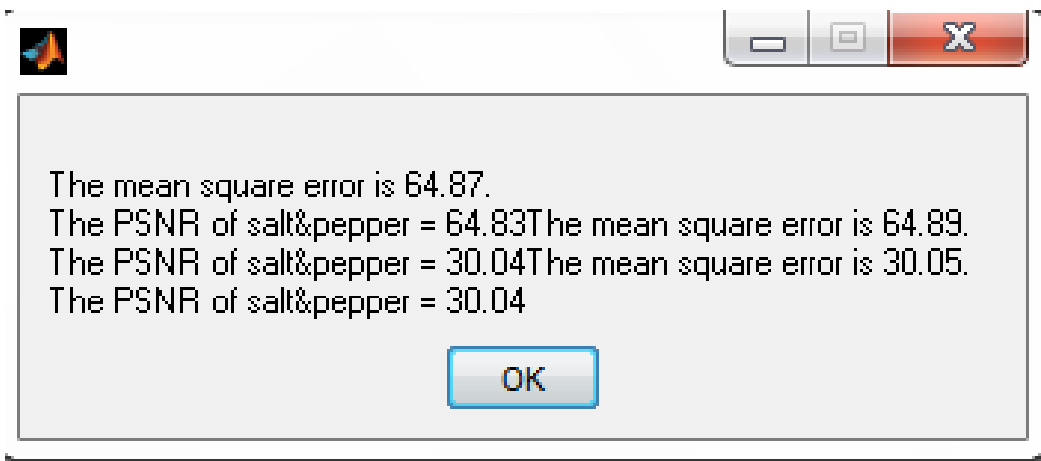
Fig.4.17 PSNR and MSE values of watermark image with salt and pepper attack.

Below shown figure is showing the final watermarked image.
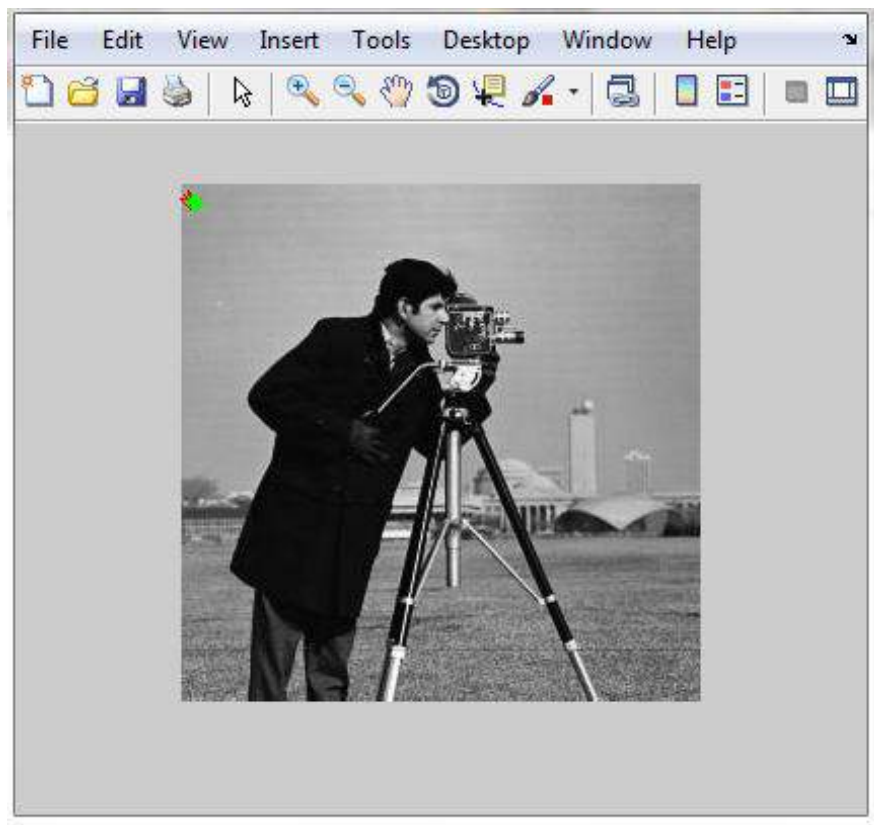
Fig. 4.18 watermarked image.

Below shown figure is showing the filtered image that we passed through the kalman filter.
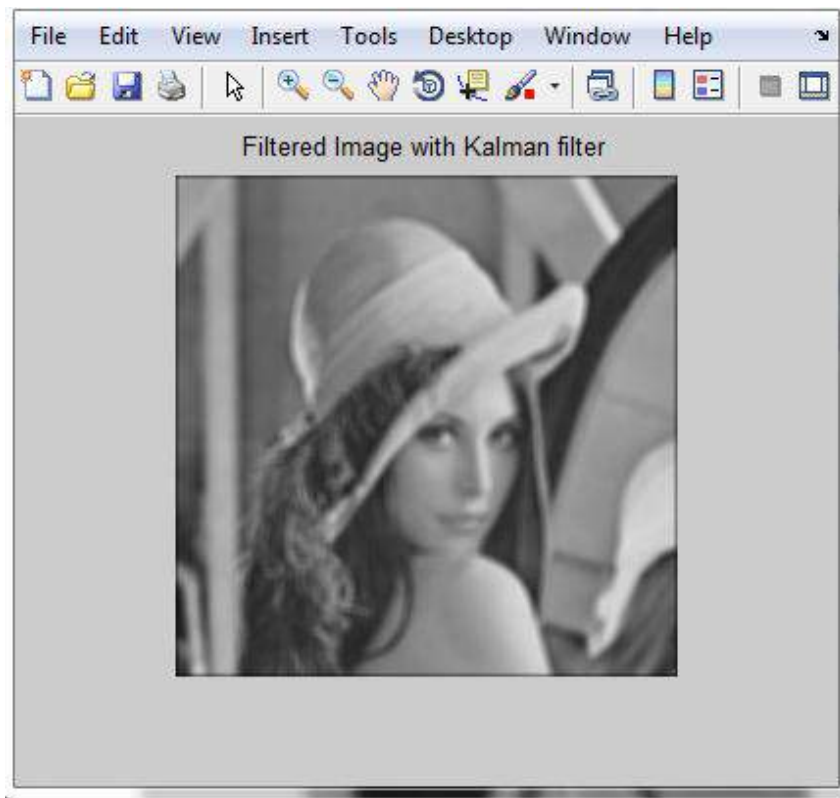
Fig. 4.19 filtered image with kalman filter.

Below snapshot figure of the calculation of the PSNR, MSE value of watermark image after applying kalman filter/one dimesion.
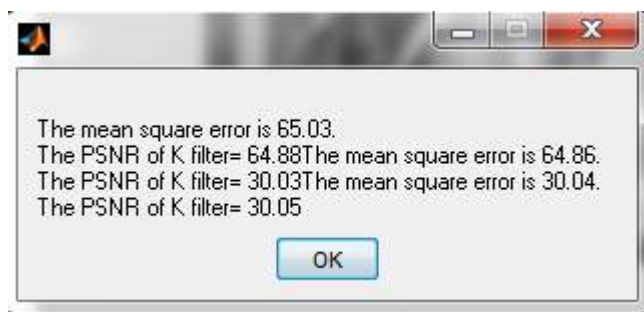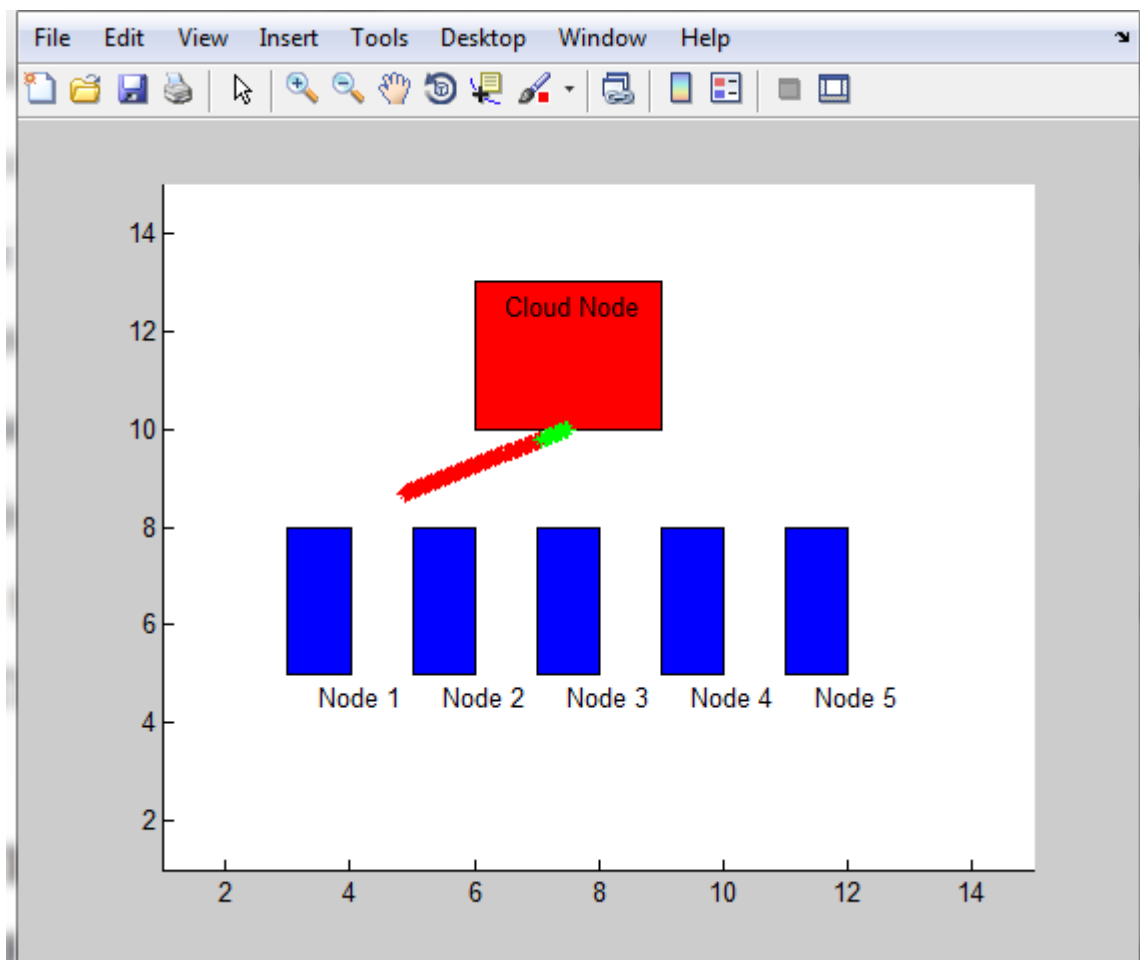

Fig. 4.20 PSNR and MSE values of kalman filter/one dimension.

Below snapshot figure of the calculation of the PSNR, MSE value of watermark image after applying kalman filter/two dimesion

The mean square error is 32.72.
The PSNR of Kalman filter = 32.72The mean square error is 32.72.
The PSNR of Kalman filter = 33.02The mean square error is 33.02.
The PSNR of Kalman filter = 33.02
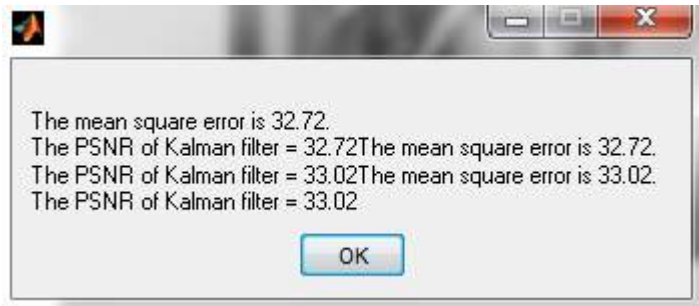
Table 4.21 PSNR and MSE values of kalman filter/two dimension.

Final outcome

**Fig.4.22 Transfer of data from cloud node to expected node.**

TABULAR FORM OF PSNR AND MSE VALUES

VARIATIONS	PSNR	MSE
SVD-DWT-DCT	30.05	65.05
SHARPENED ATTACK	30.01	65.49
CONTRAST ATTACK	24.09	244.29
SALT & PEPPER ATTACK	30.04	64.87
KALMAN FILTER/ONE DIMENSION	30.05	65.03
KALMAN FILTER/TWO DIMENSION	33.02	32.72

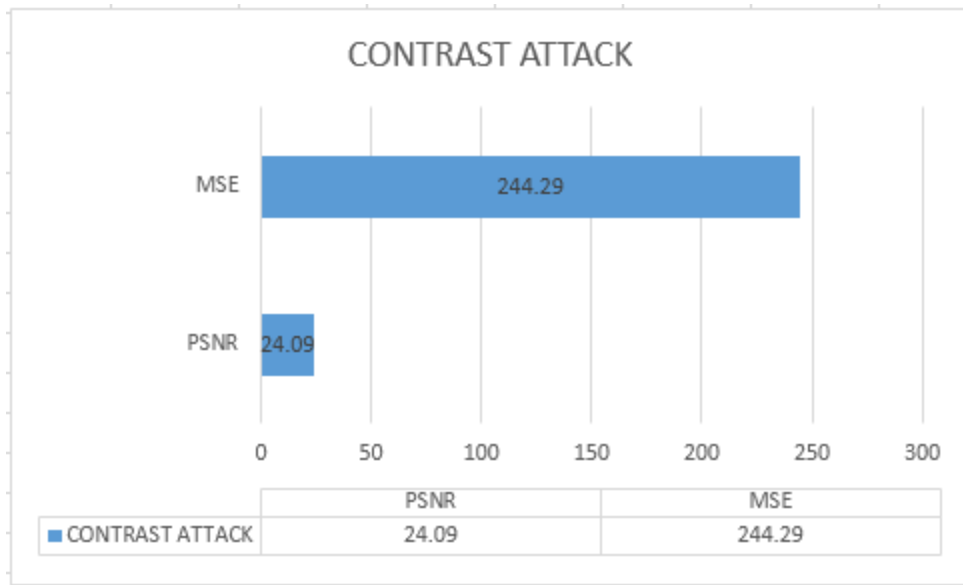**Table 4.1 Comparison of PSNR AND MSE values of existing approach with these images.**
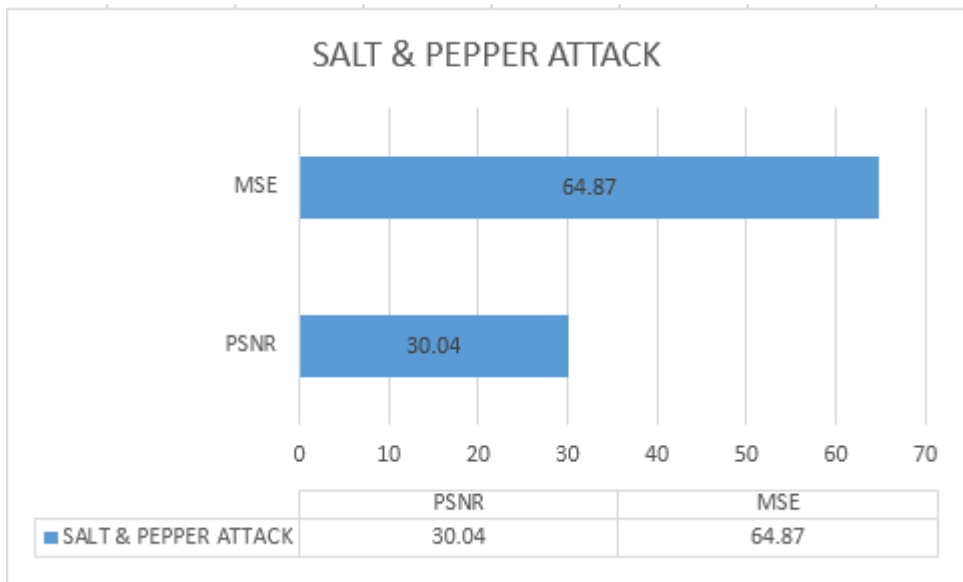
Graphical analysis of results above
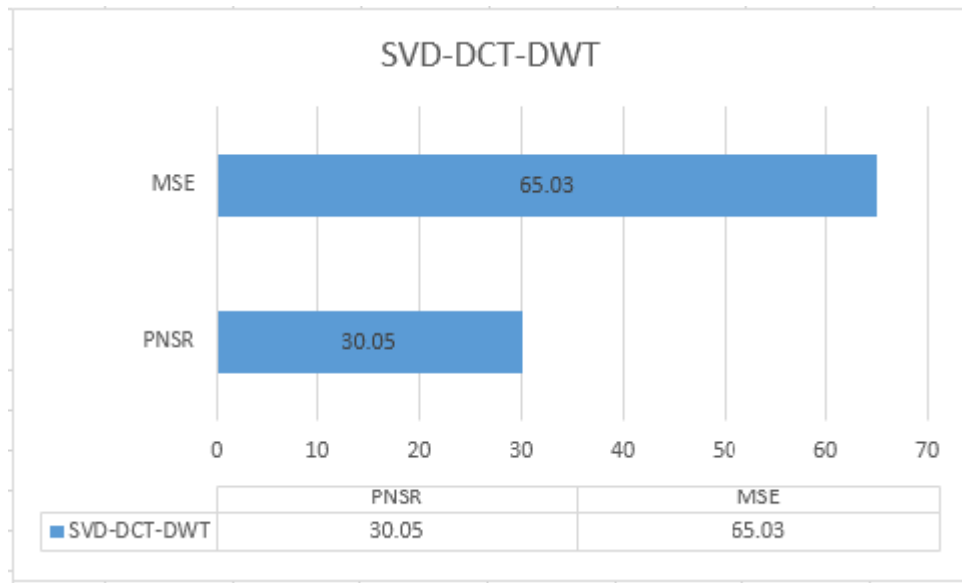
Fig. 4.23 PSNR and MSE value of existing SVD-DCT-DWT technique
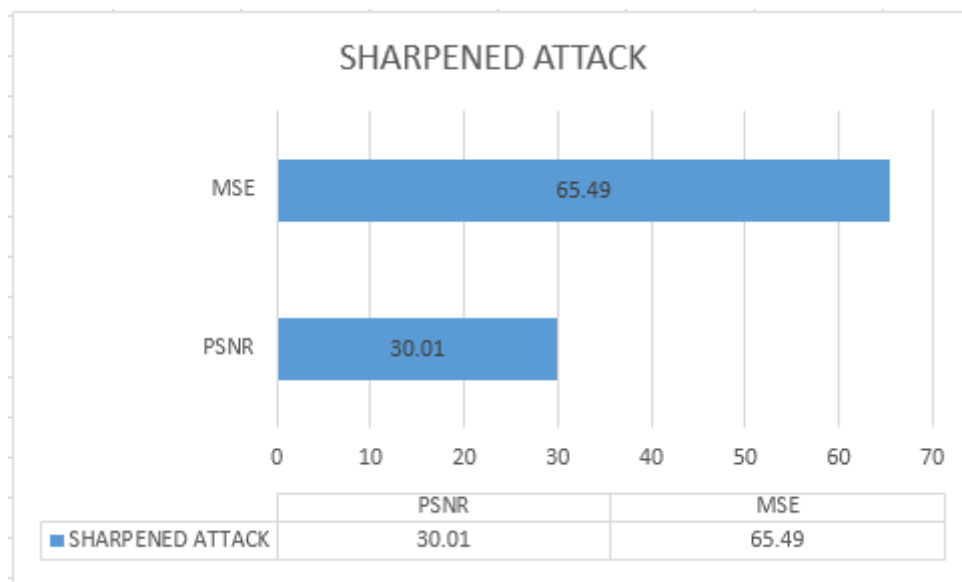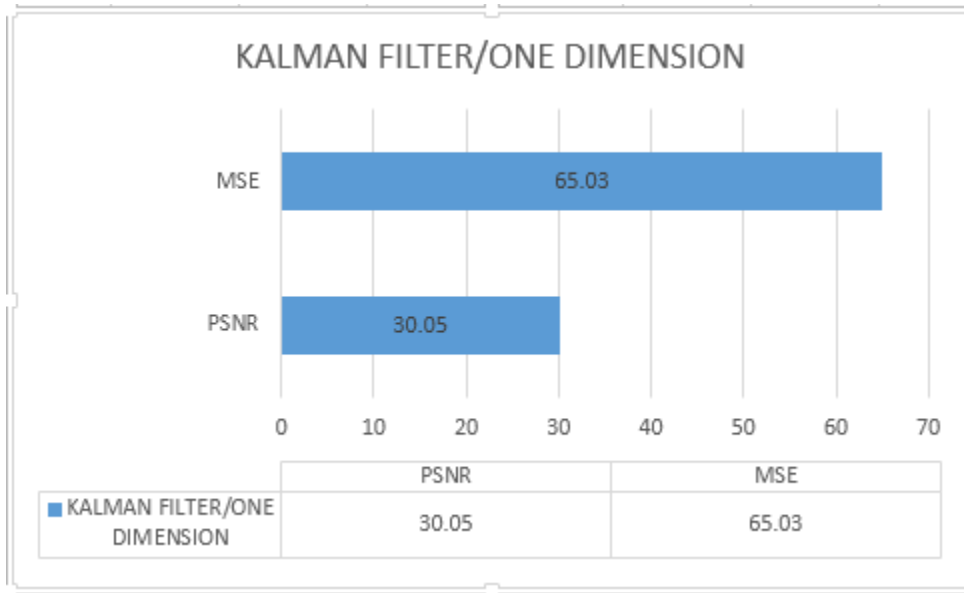

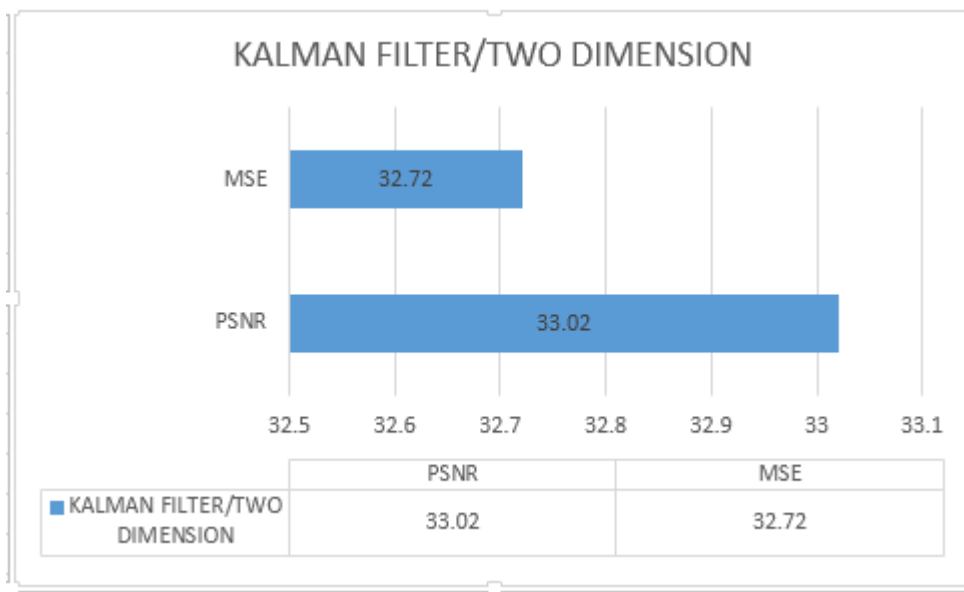**Fig. 4.24 PSNR and MSE value of sharpened image.**

Fig.4.25 PSNR and MSE value of contrast image

Fig.4.26 PSNR and MSE value of image after applying SALT & PEPPER attack

Fig.4.27 PSNR and MSE value of the extracted image in watermarking after implemented KALMAN filter with one dimension.

Fig. 4.28 PSNR and MSE value of the extracted image in watermarking after implemented KALMAN filter with two dimension.

CONCLUSION AND FUTURE SCOPE

CONCLUSION

In this work cloud computing architecture has been implemented with certain number of users. The users can present their credentials to the cloud services provider and cloud service provide access to users. In this work, watermarking technique has been implemented to provide data security. To implemented technique of watermarking SVD-DCT-DWT techniques has been implemented on cloud architecture. To check robustness of the watermarked data, sharpened attack, contrast attack and salt-pepper attack has been triggered and performance is analyzed with PSNR and MSE value. In proposed technique, KALMAN filter is implemented with SVD-DCT-DWT technique to improve PSNR and MSE value of the extracted image in watermarking.

FUTURE WORK

As mentioned above, we tried to improve quality of the image by using KALMAN filter with SVD-DCT-DWT technique to improve PSNR and MSE value of the extracted image in watermarking. In future other filtering techniques like Gabor filter has been implemented with KALMAN filter to further improve PSNR and MSE value.

REFRENCES:

[1]   Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE

[2]   Cloud Computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com

[3]   S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service deliverymodels of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul.,2010.

[4]   Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing A Practical Approach, TATA McGRAW-HILL Edition 2010.

[5]   http://en.wikipedia.org/wiki/Cloud_computing

[6]   http://www.infosecisland.com/blogview/14755-The-Cloud-Time-for-Some Serious consideration.html

[7]   Blumenthal, M.S.: Hide and seek in the cloud. IEEE Security & Privacy 8(2), 57-58 (2010)

[8]   Cloud Security Alliance (March 2010)

[9]   Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE

[10]   Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee , From System-centric to Data-centric Logging Accountability, Trust & Security in Cloud Computing

[11]   Shuai Han, Jianchuan Xing, ensuring data storage security through a novel third party auditor scheme in cloud computing, Proceedings of IEEE CCIS2011

[12]   Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing

[13]   Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012

[14]   Jasmin James, Dr. Bhupendra Verma, efficient VM load balancing algorithm for a cloud computing environment, Jasmin James et al. International Journal on Computer Science and Engineering (IJCSE)

[15] Pengfei Dai et.al, A Software Watermark Based Architecture for Cloud Security, 2012

[16] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[17] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013

[18] Yan Yan, Xiaohong Hao, privacy security issue under mobile cloud computing mode (CCIT-14) ISBN: 978-90786-77-97-0, January 2014

LIST OF ABBREVIATIONS

CSPs: - Cloud Service Providers

SVD: - Single Value Decomposition

DCT: - Discrete Cosine Transform

DWT: - Discrete Wavelet Transform

PSNR: - Peak Signal to noise ratio

MSE: - Mean Square Error

HTTPS: - Hyper Text Transfer Protocols

FTPS: - File Transfer Protocols

VPN: - Virtual Private Network