**CONTENTS**

List of Figures

Abbreviations

Abstract

**CHAPTER I**

1.1 Introduction

1.2 Problem Defination

1.3Motivation

1.4Objective

**CHAPTER II**

2.1 Literature Survey

**CHAPTER III**

3.1 System Architecture………………………………………………………………….

3.2 System Design………………………………………………………………………….

**CHAPTER IV**

4.1 Data Hiding………………………………………………………………

4.1.1 Input Image(Carrier)………………………………………………………

4.1.2 Setting protection Wall(ROI)………………………………………………………….

4.1.3 Data Hiding Algorithm………………………………………………………………

4.2 Data Extraction………………………………………………………………...

4.2.1 Resultant Image………………………………………………………………...

4.2.3 Getting ROI………………………………………………………..…

4.3Result Analysis………………………………………………………………….

4.3.1 Image Analysis

4.3.2Text Analysis………………………………………………………………..…

**CHAPTER V**

5.1 Result…………………………………………………………………………………

**CHAPTER VI**

6.1 Applications……………………………………………………………………….…

**CHAPTER VII**

7.1 Conclusion……………………………………………………………………………

7.2 Future Scope…………………………………………………….……………………

**APPENDIX**

References……………………………………………………..……………………………..

Publications………………………………………………………………………………..…

***CHAPTER I***

**1.1 Introduction**

Data or information is very crucial to any organization or any individual person. No one likes our conversation being overheard as it contains the potential of being misused. Same is the case with the data of any organization or of any person. The exchange of data among two potential parties must be in done in a secured method so as to avoid any tampering. Two types of threats exists during any information exchange. The unintended user who may try to overhear this conversation can either tamper with this information to change its original meaning or it can try to listen to the message with intention to decode it and use it to his/her advantage. Both these attacks violated the confidentiality and integrity of the message passed. Providing intended access and avoiding unintended access is a very challenging task. Information hiding has been since long time.

With the advancement of technology today communication is mostly done through internet which is open and public in nature.Due to this security and secrecy of information has always been important to people, organizations and governments. The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial.Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. The reason for this security and confidentiality is because the underlying communication network over which the transfer of sensitive information is carried out is unreliable and unsecured. Anybody with the proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations. Ideally the internet and the communication network and the routing protocols should exhibit the following the properties:

* **security:** Security is an important property of the internet. The internet should provide and preserve the confidential and sensitive information that flows through it. The security should be such that only the intended recipient of the information should gain access to it.
* **Distributed Operation**: The internet should be distributed rather than only residing on some centralized server. In the event of the crash the internet should not lose its functionality and continue performing efficiently.
* **Reliability**: Reliable communication is one of the vital properties of the internet. The internet should guarantee the reliable delivery of the information to the intended recipient.
* **Fault-Tolerance**: Fault-tolerance means the ability of the system to operate normally even in the events of failure. Internet should exhibit fault-tolerance so that it keeps on functioning even when there is failure in some part of the internet.
* **Quality of Service Support**: Quality of Service (QoS) is one of the crucial properties in terms of communication. Inter should provide QoS support to various applications and sensitive data and should prioritize them depending on the nature of the data.
* **Robustness**: Internet should be robust in the sense that it should continue functioning normally even in the presence of errors and unexpected situations like invalid input. All the above mentioned properties are ideal and cannot be practically implemented in the structure and functioning of the internet as it comprises of many networks, different infrastructures: wired, wireless, ad hoc and various mobility models. One such property that cannot be guaranteed in the internet is Security. Due to the inability to guarantee security, various vulnerabilities exist in the network that can be exploited and gives rise to several security attacks. Some of the common security attacks are listed below.
* **Impersonation or Spoofing:** The main goal of this attack is to assume the identity of the person and convince the sender that it is communicating with the intended recipient.
* **Man in the Middle attack:** In this attack, the attacker makes independent connections with the two parties across the network making them believe that they are communicating privately, when in fact the communication is controlled and intercepted by the attacker.
* **Traffic Analysis:** In this process the attacker listens to the chatter on the communication network between two parties without interacting between them and tries to learn the information that they are sharing. To mitigate these security vulnerabilities and facilitate seamless and safe transfer of data over the communication channel, techniques like cryptography, hashing, authentication, authorization, steganography are developed

Data hiding is the transmission of a secret message hidden within an ordinary carrier without revealing its existence. The container (cover file) may be a digital still image, audio file, or media file. Once the secret message has been embedded, it may be transferred across insecure lines or posted in public places. Usually, the data rate of covert data transmission using data hiding is low in order to keep the covert data imperceptible within the cover medium. This data rate is somewhat proportional to the volume of the cover medium. For this reason, digital media is a convenient choice for data hiding. Nowadays, given the high degree of collaboration and cooperation in modern information systems such as emerging multimedia sensor networks, covert communications becomes a greater threat to forensic analysis than ever. It is imperative to investigate methods to detect and discourage covert communications such as data hiding in multimedia networks that acquire highly correlated data.

**Who Needs Security?**

* Suppliers
* System integrators
* Industrial end users
  + Chemicals
  + Petroleum
  + Automotive
* Industry analysts/venture capitalists
* Others (associations, government, media, researchers )

Thus the proposed data hiding scheme uses half toning visual cryptography to hide the data inside the carrier.Here carrier we are using is the image.The proposed data hiding scheme set digital protection wall inside the carrier anthe secrete data is encoded inside the wall.So as to provide another layer of security to the secrete data.So that even if data loss occur it wont affect the secret data.Also, the proposed technique makes the use of higher LSB for replacement with secret data,in order to make data secure from unauthorized user.

**1.2 Problem definition**

Extensive use of digital media like text, images, audio and video on the internet generated a requirement for providing traffic security. For carrying out confidential communications over public networks, it was found that simply concealing the contents of a message using cryptography was not adequate. Conventional encryption alone leaves many problem unsolved.The protection from the encryption vanishes once the is data is decoded.Also it does not guard from the vulnerability arises from poor system infrastructure.

Digital media data hiding techniques have developed a strong basis with a growing number of applications like digital privileges management, covert communications, hiding executables for access control, annotation etc. In all application scenarios given above, multimedia data hiding techniques have to satisfy three basic requirements. The best requirement is Perceptual Transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible.

The second constraint is high data rate of the embedded data. All the stego applications, besides requiring a high bit rate of the embedded data, have need of algorithms that detect and decode hidden bits without access to the original digital media sequence (Blind detection algorithm).

The third constraint is security that means providing security to the data hidden inside carrier or we can say that inability by unauthorized users to detect/access the communication channel. Information hiding in digital media can be used for such a diverse applications as proof of ownership,authenticaton,integrity, secret communication, broadcast monitoring and event annotation.

All the techniques mentioned earlier were good ways of hiding messages but even with the new twists given to them, they were still nothing compared to the types of applications developed with the invention of the computer. So,there is need to add an additional layer of security while transferring the information over wireless network.Thus this work produced new procedures for hiding the sensitive data by using digital protection wall.So that the secrecy of the information will be maintained. Thus provides good perceptual transparency, security & improves payload capacity.

**1.3 Objective**

The objectives of this work is to create an easy to use environment in which the user can provide a sample image for hiding the secrete data in it using Half toning visual cryptography & to extract data from an image using simply reverse algorithm.As today most of communication is carried out through internet which is open and public in nature data security has become important concern when dealing with confidential data.

The Main objectives of this proposed method are:-

1. To increase the Payload capacity. It refers to the amount of data that can be inserted into cover media without deteriorating its integrity.
2. To create unbreakable digitat protection wall inside the carrier so as to protect data from unauthorized user.
3. To maintain Image Perceptual quality. It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.
4. Performance evaluation of proposed algorithm in terms of embeddability
5. To compare the performance analysis of proposed scheme with existing algorithm like LSB, HLSB, Power spectrum etc
6. To provide security to hidden message from unauthorized accesses when communication is carried out over wireless medium.

**1.4Motivation**

With the progression of the digital age, digital steganography has become more practical and powerful as data is the soul of computer communication. The digital information revolution has brought about profound changes in day-to-day life. Due to the increase in exchange of data over the computer network, the security of data has become a major concern and so the confidentiality and data integrity are required for protecting against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. The attacks on information systems, cybersecurity and cyber-forensics have become a primary concern for both governments and commercial industries. For many years, data hiding have captured the attention of designers, developers and evaluators of for processing sensitive information and to establish covert channels in order to conceal sensitive information. Data hiding is a method of hiding secret data into a digital medium so that the hidden data are imperceptible to everyone except the intended recipient.Following the **Cambridge Analytica sacandal**, where the company illegally harvested the personal data of millions of Facebook users without their consent and used the data to influence there voting preference.These type of incidences resulted in increasing the global interest in data hiding technology, research and development has exploded in recent years.

This is because of the potential of digital hiding to establish covert channels for communications. With digital data hiding, it is possible to hide information inside a digital file without causing perceptual degradation. It could be done by embedding information inside a file through a technique that manipulates or modifies the unused bits of digital media and such modification is not visible. Subsequently, the receiver to whom the message is delivered can also extract the hidden information from the cover media. Methods of data hiding have existed for centuries, although with the advent of digital technology, have taken on a new form. Data hiding has a wide range of applications mainly in the security of the digital data. They are also getting attentions because of self awareness to increase security system and also after the world wide security attack. Research in hiding data inside image file using data hiding technique is a topic of great interest. Given the proliferation of digital image and given the high degree of redundancy present in its binary representation, there has been an increased interest in using image as cover-objects for the purpose of data hiding.

Internet is the fastest growing communication medium and essential part of infrastructure, nowadays. To cope with the growth of internet it has become a constant struggle to keep the secrecy of information and when profits are involved, protect the copyright of data. To provide secrecy and copyright of data many of the data hiding techniques has been developed. But each of the technique has their respective pros and cons. Where one technique lacks in payload capacity, the other lacks in robustness. So, the main motivation of proposed work is to overcome these short comings.

***CHAPTER II***

**2 . Literature Survey**

For studying the concepts of media data hiding and data hiding technique we have surveyed many latest papers. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas[2], the main requirements of any data hiding system are security, capacity and robustness. It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital media as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like media in media and picture in media as a cover image.

Ahmed Ch. Shakir [1], the confidential communications over public networks can be done using digital media like text, images, audio and media on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the author suggested the new procedures in data hiding for hiding ciphered Information inside a digital colour bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and data hiding produce immune information.

Andreas Westfeld and Gritta Wolf [3], in this work author have described a data hiding system which embeds secret messages into a media stream. Normally the compression methods are used in media conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding. In this algorithm security is established by indeterminism within the signal path.

Sherly A P and Amritha P P [14], in this paper author have proposed a new compressed media Data hiding scheme. In this scheme the data is hided in compressed domain. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed medias without degradation in visual quality.

Saurabh Singh and Gaurav Agarwal [13], have presented a novel approach of hiding image in a media. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So It is very difficult to find that image is hidden in the media of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the media. The intruder requires full media to unhide image. Authors have described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely.

S. Suma Christal Mary [12], have proposed new Real time Compressed media secure Data hiding (CVSS) algorithm using media bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity. At present we are hiding the data in media format, so in the future implementation of uncompressed formats may possible as well, so it may support MPEG4 format [15]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

Yusuf Perwej, Firoj Parwej, Asif Perwej[16] in their work describes An Adaptive Data hiding Technique for the copyright of digital images and Digital Image Protection. Authors proposing edge detection from Gabor Filter method, using data hiding by the simple LSB substitution method. In the method a set of pixels that constitute a block jointly share the bits from the watermark .The values for the mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. The results indicate the method introduces low noise and hence ensures lesser visible distortions.

Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh[17] in their work authors describes A New Digital Data hiding Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit. Author proposed a new LSB based digital data hiding scheme with the combination of LSB and inverse bit. The experimental result shows that the proposed algorithm maintains the quality of the watermarked image. When combining different positions of LSB such as the second LSB and the third LSB and fourth LSB and the combination between them. The proposed algorithm is also tested using Peak signal-to noise ratio (PSNR).Further latest paper are surveyed using different carrier and technique for data hiding has following disadvantages as shown in table:-

|  |  |  |  |
| --- | --- | --- | --- |
| Sr.No. | Paper title | Focus on | Disadvantages |
| 1. | New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams | Data Hiding + Visual Cryptography on JPEG Carrier | * Data Loss * Change in Carrier * Less Security * Practically Not feasible for cloud storage. * Unsecure as sensitive information carrier. |
| 2. | Enabling Identity-Based Integrity Auditing and Data  Sharing with Sensitive Information Hiding for  Secure Cloud Storage | Data Auditing, Data Integrity, Hash Code Generation | * Show Existence of Sensitive information on carrier. * need frequent hash code calculation. |
| 3. | Reversible Data Hiding in Color Image with  Grayscale Invariance | Data Conceal in R & B Channel and G Channel value adjusted to maintain carrier originality | * Disturb carrier media after data concealing. * G Channel not used for data hiding. * Less data security. * All Carrier channels are not utilized. |
| 4. | Toward Construction-Based Data Hiding:  From Secrets to Fingerprint Images | Secrete Message is converted into Finger print image | * Major challenge is to map Secrete Message Character with ASCII from 1 to 254 to image pixels. |

For hiding secret data in digital media, large varieties of techniques are discussed above which are more complex than others and all of them have their respective pros & cons.

***CHAPTER III***

**System Architecture**

**SSENDER**

**SENDER SIDE**

Set Protection Wall

Input Carrier Media

Start

Wireless media

Embed the secrete Data

Extract the Region Of Interest

**RECEIVER SIDE**

Extract Transmission Data

Comparision by parameter

**Two tier Architecture of Proposed System**

The two tier architecture of proposed system is as shown.From which it is clear that systems deals with processing of data at two side i.e. at the sender and at the receiver side.

* **Sender Side-**

**3.1 Algorithm- Sender Side**

1. Start
2. Input carrier media.
3. Select secrete data.
4. Convert secrete data to binary format.
5. Select protection region of carrier media.
6. If (Size (Protection Region [PR] < Size (Secrete Binary data) then go to step 7.
7. Embed secrete binary data into PR region of carrier media.
8. Stop

At the sender side, the user has to select carrier in which secrete data is to be carried out.The carrier used here is an Image.We can also used video or audio stream for the purpose of data hiding but problem with these media that it is very easy to detect small change done with these carriers so here image is used as carrier.At the sender side,after selecting appropriate carrier, the digital protection wall limits are set.

The limits of digital protection wall are choosen in rectangular frame.We can also set the limits of protection wall in square or circular frame but problem with thses frames is that they will require more parameters to define particular shape.Hence here rectangular frame is taken into consideration so that only two parameters are required the top rightmost and the bottom leftmost.After setting the required limits of wall the region inside that limit is now the our Region Of Interest(ROI).

In order to hide the data inside this ROI it is necessary to fetch the pixels within this region.After fetching component within this region, the secrete data which we want to hide is then converted into binary form.Then the position of bit which we want to replace by secrete dat is choosen.After choosing appropriate position of bit the corresponding bit of RGB component is replaced with secrete data bit.In this way embedding of confidential data inside the carrier having protection wall is carried out.Thus using this methodology it adds an extra layer of security to the confidential data inside the carrier rather than only just embedding the secrete data inside the carrier and transferring over it wireless media.This methodology protects the secret data when it is transferred over wires network by digital protection wall such that even if the data loss occurs it wont affect the data within the limits of protection wall.

* **Receiver side** -

**3.2 Algorithm- Receiver Side**

1. Start
2. Input carrier media
3. Select Protection region from carrier media.
4. Extract Secrete binary data from protection region.
5. Convert secrete binary data to ASCII format.
6. Stop

**3.2Software used**

**3.1 Overview of the .NET Framework**

The .NET Framework is a technology that supports building and running the next generation of apps and XML Web services. The .NET Framework is designed to fulfill the following objectives:

To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely.

To provide a code-execution environment that minimizes software deployment and versioning conflicts.

To provide a code-execution environment that promotes safe execution of code, including code created by an unknown or semi-trusted third party.

To provide a code-execution environment that eliminates the performance problems of scripted or interpreted environments.

To make the developer experience consistent across widely varying types of apps, such as Windows-based apps and Web-based apps.

To build all communication on industry standards to ensure that code based on the .NET Framework integrates with any other code.

The .NET Framework consists of the common language runtime (CLR) and the .NET Framework class library. The common language runtime is the foundation of the .NET Framework. Think of the runtime as an agent that manages code at execution time, providing core services such as memory management, thread management, and remoting, while also enforcing strict type safety and other forms of code accuracy that promote security and robustness. In fact, the concept of code management is a fundamental principle of the runtime. Code that targets the runtime is known as managed code, while code that doesn't target the runtime is known as unmanaged code. The class library is a comprehensive, object-oriented collection of reusable types that you use to develop apps ranging from traditional command-line or graphical user interface (GUI) apps to apps based on the latest innovations provided by ASP.NET, such as Web Forms and XML Web services.

The .NET Framework can be hosted by unmanaged components that load the common language runtime into their processes and initiate the execution of managed code, thereby creating a software environment that exploits both managed and unmanaged features. The .NET Framework not only provides several runtime hosts but also supports the development of third-party runtime hosts.

For example, ASP.NET hosts the runtime to provide a scalable, server-side environment for managed code. ASP.NET works directly with the runtime to enable ASP.NET apps and XML Web services, both of which are discussed later in this topic.

Internet Explorer is an example of an unmanaged app that hosts the runtime (in the form of a MIME type extension). Using Internet Explorer to host the runtime enables you to embed managed components or Windows Forms controls in HTML documents. Hosting the runtime in this way makes managed mobile code possible, but with significant improvements that only managed code offers, such as semi-trusted execution and isolated file storage.

The following illustration shows the relationship of the common language runtime and the class library to your apps and to the overall system. The illustration also shows how managed code operates within a larger architecture.

**.NET Framework class library**

The .NET Framework class library is a collection of reusable types that tightly integrate with the common language runtime. The class library is object oriented, providing types from which your own managed code derives functionality. This not only makes the .NET Framework types easy to use but also reduces the time associated with learning new features of the .NET Framework. In addition, third-party components integrate seamlessly with classes in the .NET Framework.

**4.2 C#**

C# is a simple, modern, general-purpose, object-oriented programming language developed by Microsoft within its .NET initiative led by Anders Hejlsberg. This tutorial will teach you basic C# programming and will also take you through various advanced concepts related to C# programming language.

C# is a modern, general-purpose, object-oriented programming language developed by Microsoft and approved by European Computer Manufacturers Association (ECMA) and International Standards Organization (ISO).

C# was developed by Anders Hejlsberg and his team during the development of .Net Framework.

C# is designed for Common Language Infrastructure (CLI), which consists of the executable code and runtime environment that allows use of various high-level languages on different computer platforms and architectures.

**Integrated Development Environment (IDE) for C#**

Microsoft provides the following development tools for C# programming −

Visual Studio 2010 (VS)

Visual C# 2010 Express (VCE)

Visual Web Developer

The last two are freely available from Microsoft official website. Using these tools, you can write all kinds of C# programs from simple command-line applications to more complex applications. You can also write C# source code files using a basic text editor, like Notepad, and compile the code into assemblies using the command-line compiler, which is again a part of the .NET Framework.

Visual C# Express and Visual Web Developer Express edition are trimmed down versions of Visual Studio and has the same appearance. They retain most features of Visual Studio. In this tutorial, we have used Visual C# 2010 Express.

**4.3 Visual Studio**

**Introduction to Visual Studio**

Visual Studio is a Integrated Development Environment (IDE) developed by Microsoft to develop GUI(Graphical User Interface), console, Web applications, web apps, mobile apps, cloud, and web services etc. With the help of this IDE, you can create managed code as well as native code. It uses the various platforms of Microsoft software development software like Windows store, Microsoft Silver light, and Windows API etc. It is not a language specific IDE as you can use this to write code in C#, C++, VB(Visual Basic), Python, JavaScript, and many more languages. It provides support for 36 different programming languages. It is available for Windows as well as for macOS.

Evolution of Visual Studio: The first version of VS (Visual Studio) was released in 1997, named as Visual Studio 97 having version number 5.0. The latest version of Visual Studio is 15.0 which was released on March 7, 2017. It is also termed as Visual Studio 2017. The supported .Net Framework Versions in latest Visual Studio is 3.5 to 4.7. Java was supported in old versions of Visual Studio but in latest version doesn’t provide any support for Java language.

***CHAPTER IV***

**4.1 PROPOSED WORK**

**4.1Basic Idea :-**

The basics of data rely on three different facts i.e. capacity, security, and robustness. Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place.

**4.2 Methodology:-**

Proposed Methodology has been divided in 2 Phases:-

1) Data Hiding

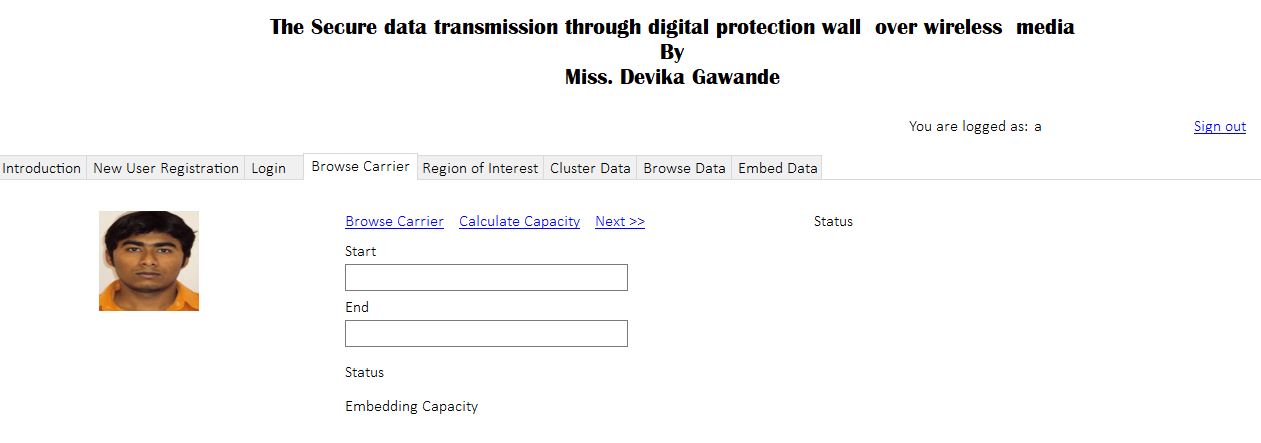
2) Data Extraction

**4.2. 1 Data Hiding**

This phase is further divided into no. steps as data hiding is carried by first selecting an appropriate carrier then setting of protection wall limits,extracting the corresponding RGB component of that ROI,and then classification of bits according to classes and finally embedding the data.All these steps are discussed in detail as follows-

**4.2.1.1 Input Image (Carrier)**

For the purpose of data hiding appropriate carrier is selected in order to transfer the secrete data over wireless media.This carrier is nothing but an image. Image basically made up of number of pixels. Any work that is related with the image can be done on the basis of number of pixels in an image, size of the image, color intensity of the image and the shape of the image.While working with an image there are different model available such as pixel model,RGB color model etc.Here we are considering RGB color madel for the purpose of data hiding.The carrier is selected from the gallery/collection and van be of users choice.The length of data and the embedding capacity of carrier must be relared.If we want to hide larger amount of data the carrier should laso be large enough to accommodate that amount of data within the region of protection wall.

****

Size(carrier) >Secrete Data(Sd)

## Embeding capacity

The embedding capacity of the carrier plays important role as it provides information to user that how much data can be embedded within the single carrier.

Consider a carrier of height ‘H’ and width ‘W’ then the embedding capacity can be calculated as simply

I(size)=H\*W

Where I(Size) represents the carrier capacity

W

H

CARRIER

**4.2.1.2 To Set Digital Protection Wall**

The main purpose of work is to set protection wall within the carrier in order to provide another layer of security.The protection wall frame used in the work is rectangular one so that only two parameter will be needed to set the wall.Other shape such as circle or square can not be used.Beacause using these frames as wall to protect data can increase complexity of the system.If we use circular shape wall it requires parameter such radius, centre or area of circle.This will make the calculation of ROI much more complex same is the case for square frame.

ROI

From above it is clear that the protection wall acts as barrier between the original carrier and secrete data.The secrete data is embedded with in the ROI.The protection wall limits can be choosen according to the users need and where user want to hide the data.Thus system is that much flexible for choosing the limits of protection wall. While setting protection wall the system needs two co-ordinate points as (x1,y1) and (x2,y2) such that the protection wall is set with in the rectangular frame.

But there are few conditions while selecting these coordinate points so that the secrete data remain intact and less quantization error occurs.

These conditions are given as

P1={x1,y1}

P2={x2,y2}

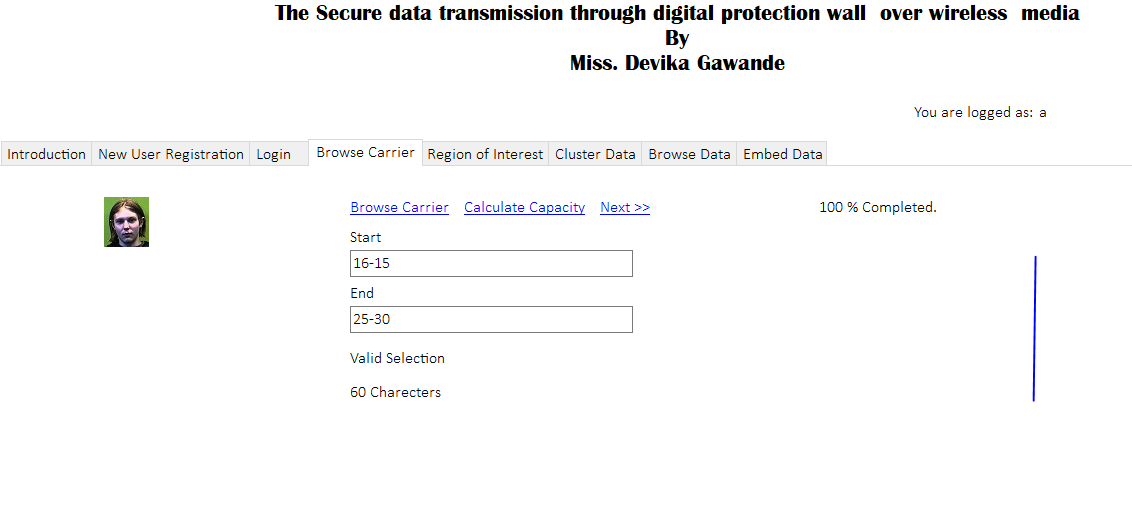
Where P1 and P2 represents pixels of image

Pw=Region|x2-x1,y2-y1|

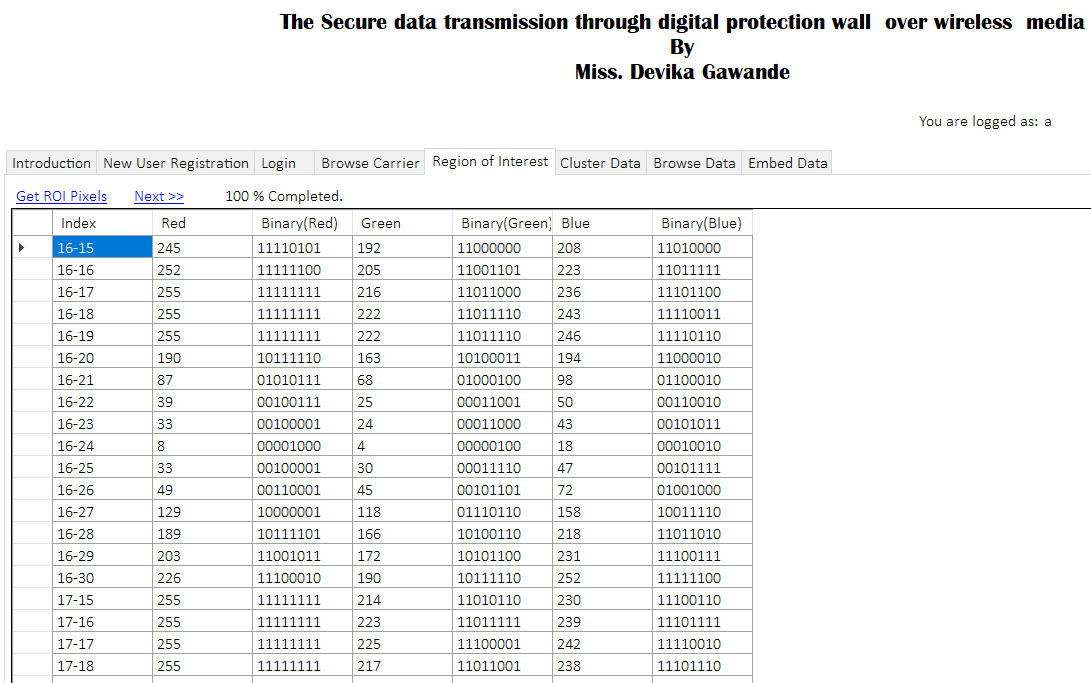
* x2>x1-------Valid region x1>x2-------Invalid region
* y2>y1-------Valid region y1>y2-------Invalid region

**Region Of Interest (ROI)**

Once the protection wall limits are set,then the pixels within the ROI is extracted.Here ROI is the Region Of Interest where user want to hide the data.Basically image is made up of no. of pixels,each pixels has three basic component RGB.Each RGB has 0 to 255 component range.

****

Consider an example if the protection wall limits are set between (x1,y1)=16,15 and other as (x2,y2)=25,30 ,then pixels within that ramge of image are extracted in order to hide the data within that limit.Thus from below it is clear thet ROI pixels are extracted and converted into corresponding binary form.



**How the capacity of ROI is calculated**

After extracting the pixels of ROI it is then become necessary to know that how much amount of data ROI can hide.It is very easy to get the information about the capacity of ROI by simply taking into consideration the two coordinate points.

Where ‘ P’ represents pixel of carrier image

Capacity=(x2-x1)\*(y2-y1)

Capacitymax=(x2-x1)\*(y2-y1)\*3 bits

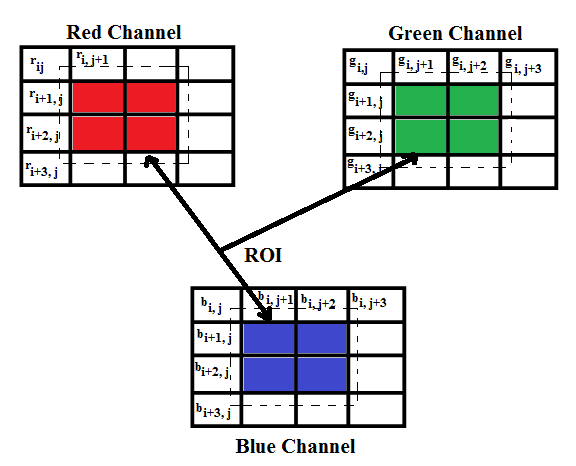


Fig. shows the corresponding RGB component of ROI

**4.2.1.3 Data Hiding Algorithm**

After extracting the pixels of ROI and after converting them into its corresponding binary form,the actual process of data hiding is carried out.For hiding the data the particular position of bit which is need to be replced is choosen first.Uptill now while encoding the data within image(carrier) mostly LSB are used to replace with secret data.Also it is very easy to encode the data at lower LSB side as it involve less complexity.But problem while using these bits for storing the secret data is that they are more vulnerable to unauthorized access.As today most of the hacker knows that even if the carrier is alter it may be alter at the lower LSB side as it is very easy to decode at the receiver level.Hence taking into the consideration of above problem , the proposed work tends to hide the data at the higher LSB side,so that even if hacker come to know about the secret dat it wont be possible for him to decode that particular pattern.As with higher LSB it is very difficult to identify that which particular bit is of the carrier is alter.

**Classification of bits**

When particular higher LSB bit i.e. 5th,6th or 7th bit position is selected to hide the data,the classification of bit is carried out.Here classification named as ‘Class 0’ and ‘Class 1’.Here ‘class 1’ contain all the component of ROI that have **bit 1** at particular position of bit which is selected for replacement, same as case for ‘Class0’. More specifally consider an example, if ROI first component is **‘16’** and the position of bit choosen to hide the data is **‘7’** then if 7th bit of component 16 is **‘0’** then this component will be placed in **‘ class 0’** and if the bit within the component is **‘1’** then the corresponding component will be placed in **‘Class 1’**.In this way the classification of bits is carried out.

**How the data hiding is carried out**

Once the classification of bits is done and the corresponding component is placed in there appropriate class then finally the secrete data comes into consideration.The secret data is first converted into its equivalent binary form.If binary secret data (bsd) first bit is ‘0’ and the first component corresponding bit where data is to be hided is ‘1’ then corresponding component closest match is found in ‘Class 0’ and replaced with corresponding component. But if the ‘bsd’bit is found in that particular calss,then there is no replacement.That particular component will kept as it is.

For this consider an example, ifBinary Secrete Data Bit == 0 and Component =32 then there will be two possible conditions through which bit is replaced

* If 32 Found in Class 0 then there is No need of Replacement
* If 32 is not Found in Class 0 then Find Component from Class 0 with best match/fit.

Similarally the case for class 1. Here the term best fit or match is defined as mimimum difference between the two component.By considering above example, if component 32 is not found in class 0,then best match is searched , if there are two component in Class 0 which are near to 32 such 35 and 28 ,then minimum difference between the two is ‘3’ and ‘4’resp. So, the component ’35’ is selected for data hidind in such way all the remaining bits of secret data are hided inside the ROI.The algorithm given below makes clear all the process of data hiding.

**Algorithm**

Step 1: Start

Step 2: Input the secrete data(Sd)

Step 3: Load classes(0,1)

Step 4: For i=1 to length(Sd)

If Sd(position)==0

Find the best fit in Class 0 and replace in image

Else

There is no replacement

End

If Sd(position)==1

Find best fit in class1 and replace in image

Else

There is no replacement

End

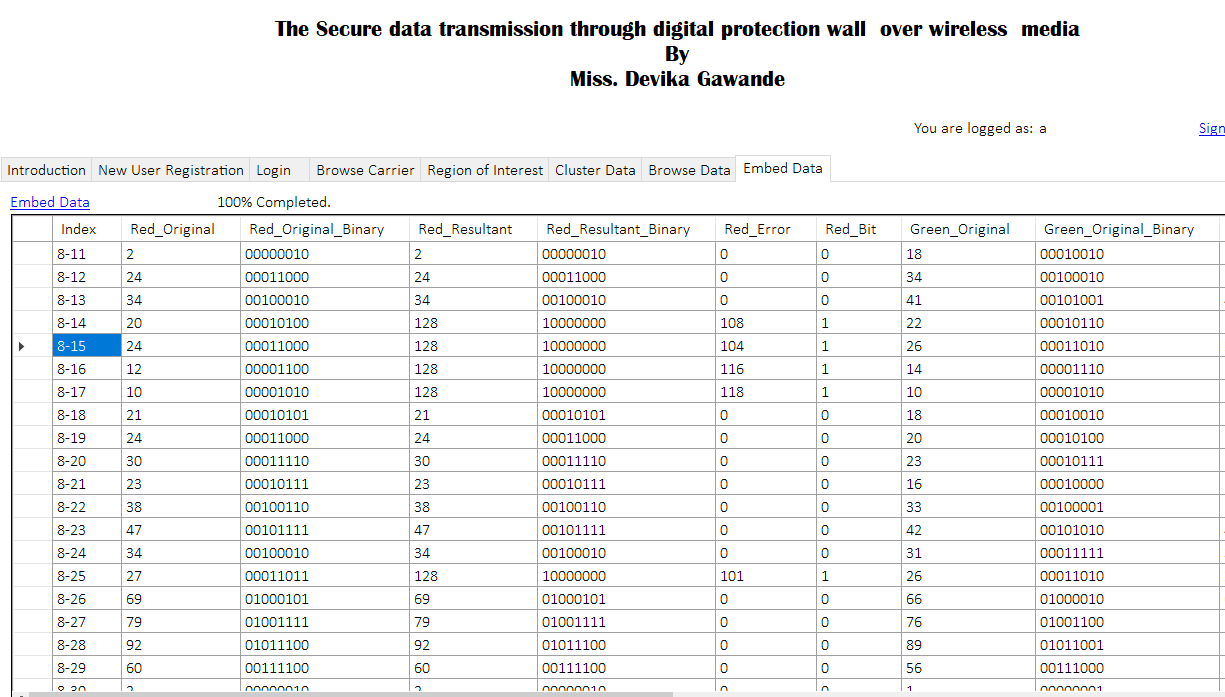
End

Step 5: Save the result image

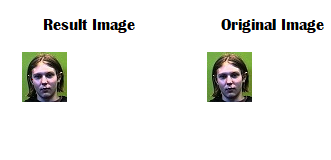
Step 6: Stop.

Here Sd means secret data

After following the hiding algoriyhm all the bits are replaced and finally we get secret data embedded carrier.



This is how the components and there original and resultant components are given after embedding the data



**Data Extraction**

At the receiver side,when carrier is received by user through wireless media, for decoding the content of carrier it will require three parameter.Thus by putting this condition at the receiver side provide security to the confidential data as only intented user will know the process and factors needed to decode the data.These three parameter are

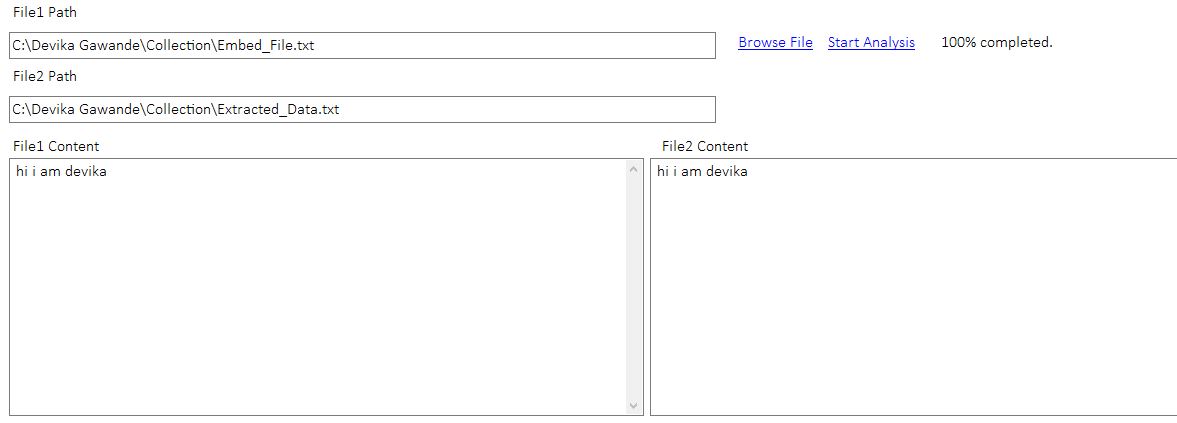
* No. of bits encoded
* Position of bit which is alter
* Limits of protection wall

To extract the data at the receiver side the user must know the limits of protection wall.After knowing the limits, the bits within that limits are first extracted.After extracting the bits within that particular Region Of Interest(ROI),the position bit which alter is then extracted.Once all those bits are extracted,thenuser has to provide the information about the no. of bits tgat are encoded at the sender side.Once all this process is done we get exactly the data which was embedded at the receiver side.

**4.3Result**

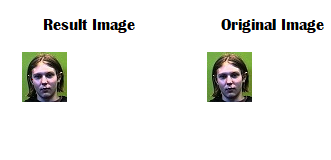
The result of the proposed work is carried out in two parts i.e. in text analysis and image analysis.

**Text Analysis**

****

From the above result it is clear that system provide the exact data which was embedded at the sender side and thus provide 100% output at the receiver side**.**

**Image Analysis**

****

From the above result it is clear the that before embedding and after embedding the data , the carrier perceptual quality is high.The image is looking as it is,making it difficult to identify the unathorised user.

***CHAPTER V***

**5.Result Analysis**

In this section, result analysis is discussed in detail. Image basically made up of number of pixels. Any work that is related with the image can be done on the basis of number of pixels in an image, size of the image, color intensity of the image and the shape of the image. The purpose of this section is to focus on the various parameters i.e. entropy, mean intensity, time required for encryption and decryption, peak signal to noise ratio, mean square error. After performing various operations on the image, it gives different results that one has to focus.

## Peak Signal-to-Noise Ratio

It is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not be. One has to be extremely careful with the range of validity of this image; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content. PSNR can be calculated as,

Where, Mean Square Error (MSE): It measures the average of the square of the error. The error is the amount by which the pixel value of original image differs from the pixel value of decrypted image.

Where a (i, j) represents the original image, b (i, j) is the decrypted image and (i, j) represent the pixel positions of the XY image. Here, X and Y are the height and width of image respectively.

The time required for encryption and decryption of an image is also an important factor.

## Normalized Correlation (NC)

Analysis with respect to AD value, MD, NAE and SC

## Average Difference (AD)

Average Difference is measurement of differences between two images. Here we calculated the average difference by the formula given. As we know that large value of maximum difference means that image is poor in quality.

## Maximum Difference (MD)

Difference between any two pixels such that the larger pixel appears after the smallest pixel. As we know that large value of maximum difference means that image is poor in quality. MD is defined as.

MD = MAX |x(i , j)- y(I , j)|

## Normalized Absolute Error (NAE)

The large value of normalized absolute error means that image is poor quality. NAE is defined as

## F. Structural Content (SC)

The structural content measure used to compare two images in a number of small image patches the images have in common. The patches to be compared are chosen using 2D continuous wavelet which acts as a low level corner detector. As we know that large value of structural content SC means that image is poor quality. SC is defined as.

## G.Quantization Error(Qe)

The quantization error of proposed system can be calculated simply by substarcting resulatant from the original component.Thus quantization error is measure of degradation quality of image,lesser the quantization error less will be degradation of the carrier.

Here the component selection for data hiding is carried out simply by finding the best match with in respective class that is in class 0 and 1.This best maych is nothing but the bearest value of component present with in that class. As we are taking minimum difference between but two component the the quantization error will also be less.

The quantization error is calculated as

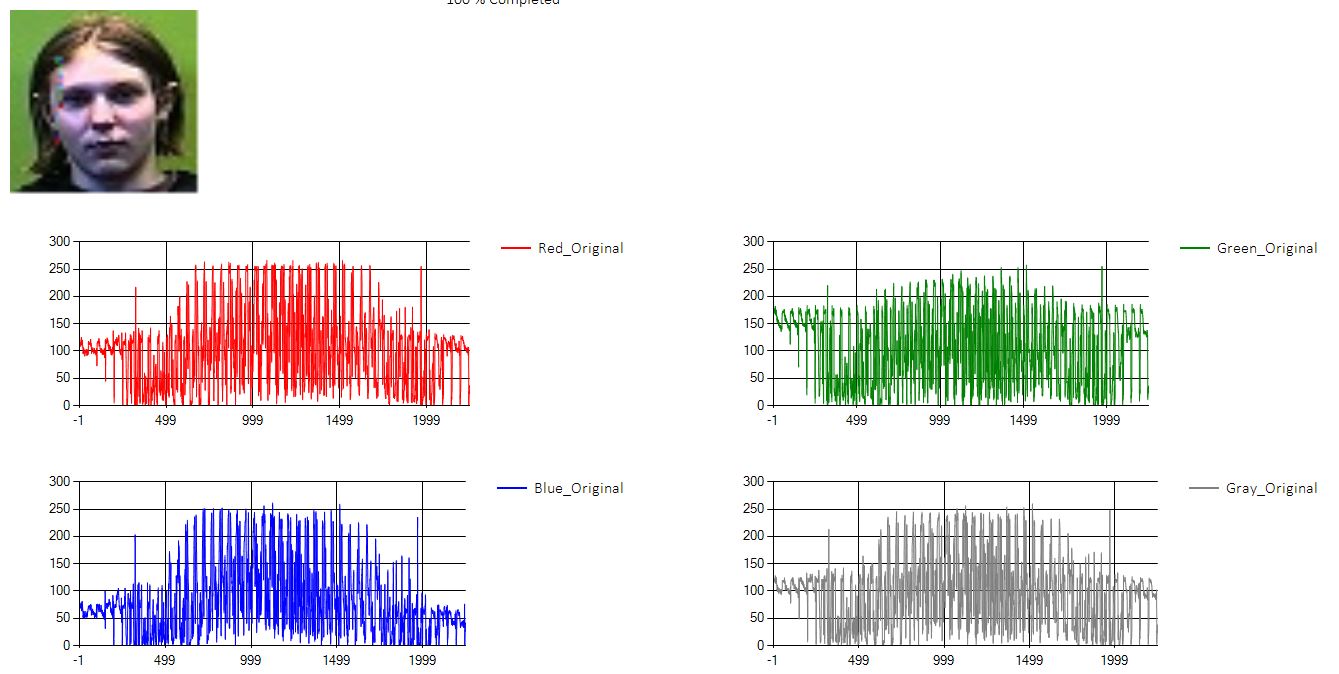
Qe=|Qoriginal – Qresultant|

In the proposed systemthe quantization error must be within the range of 0 to 255

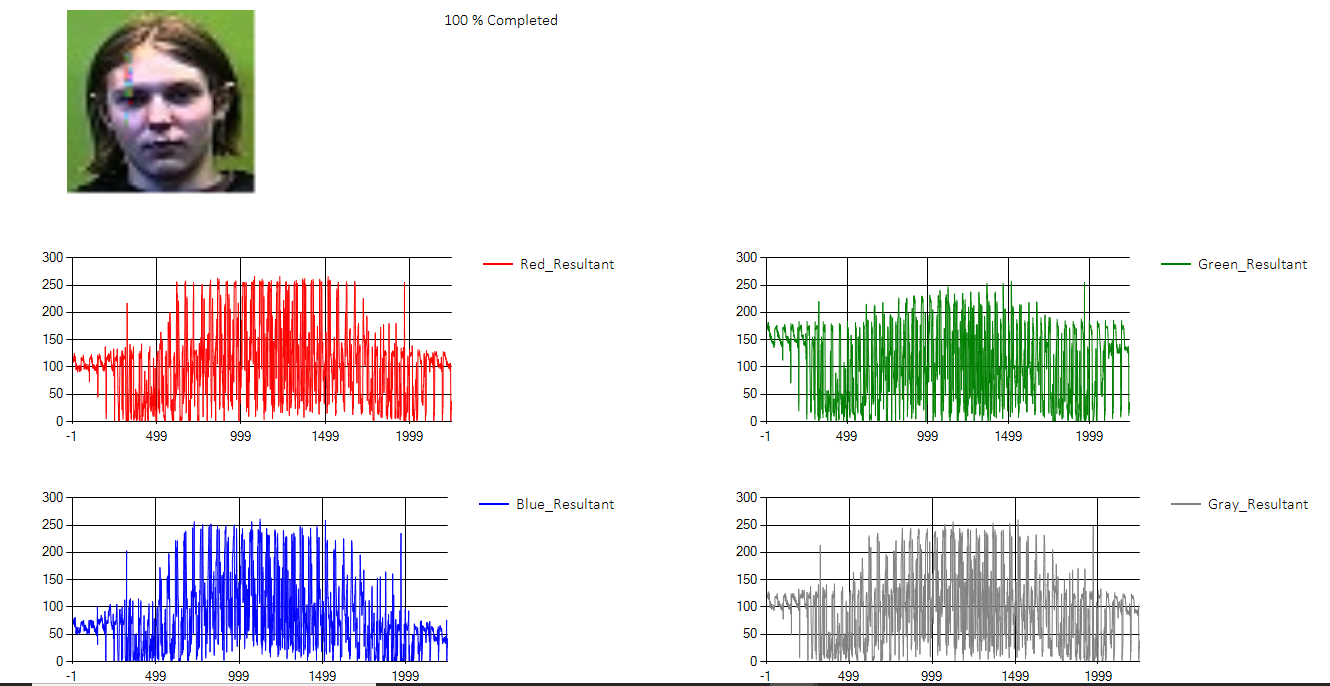
0>|Qe|<255

The following charts shows the trade off between the original and resultanat image component.

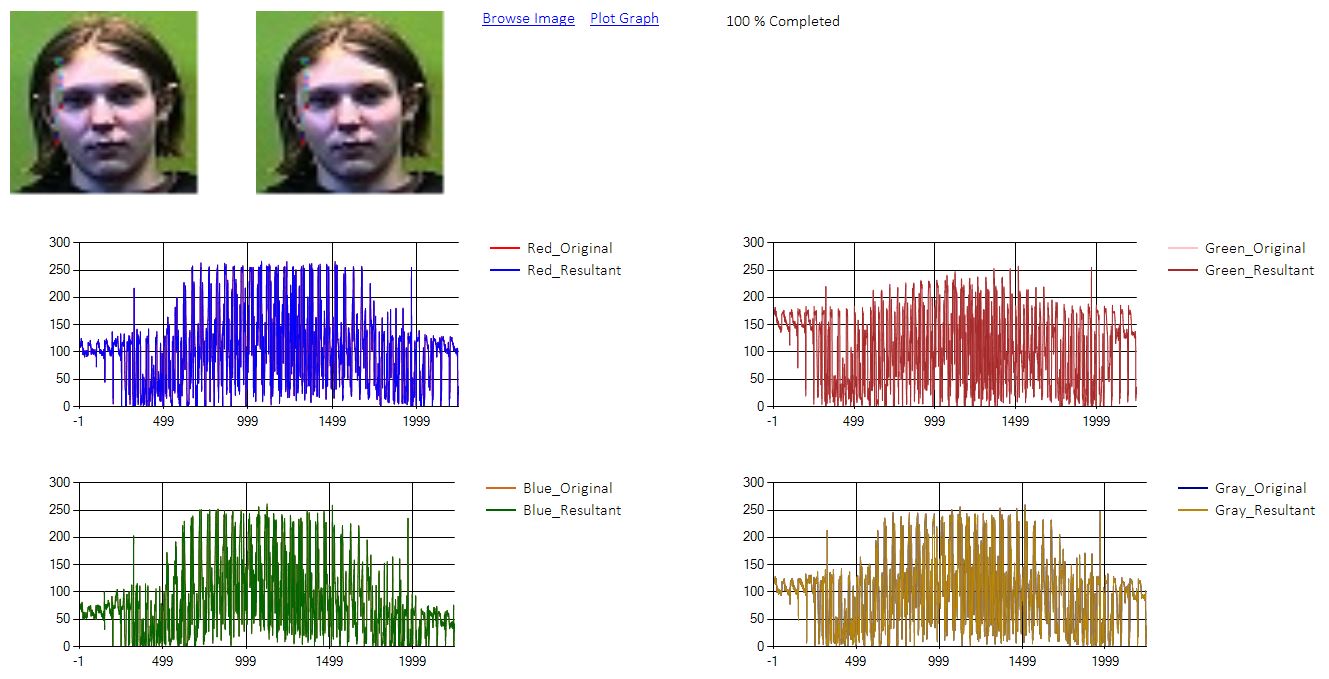
Input (Carrier) quantization error chart:



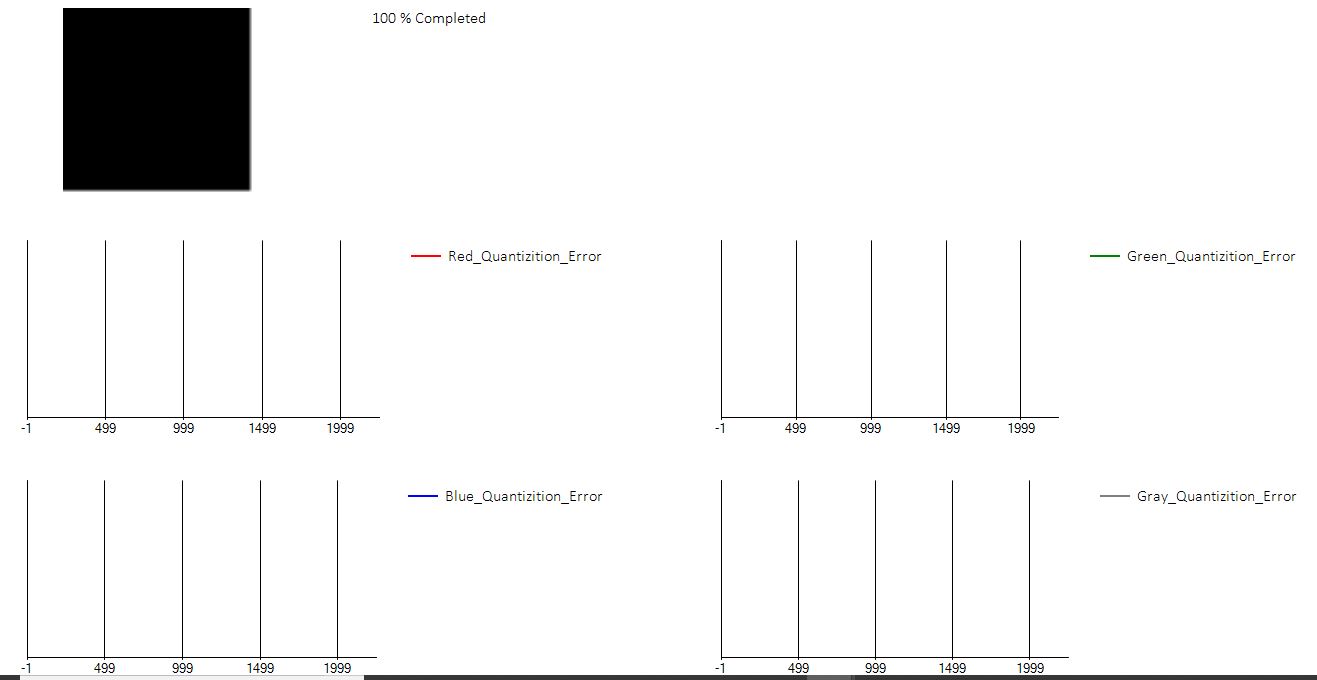
Reciver side (Qe)



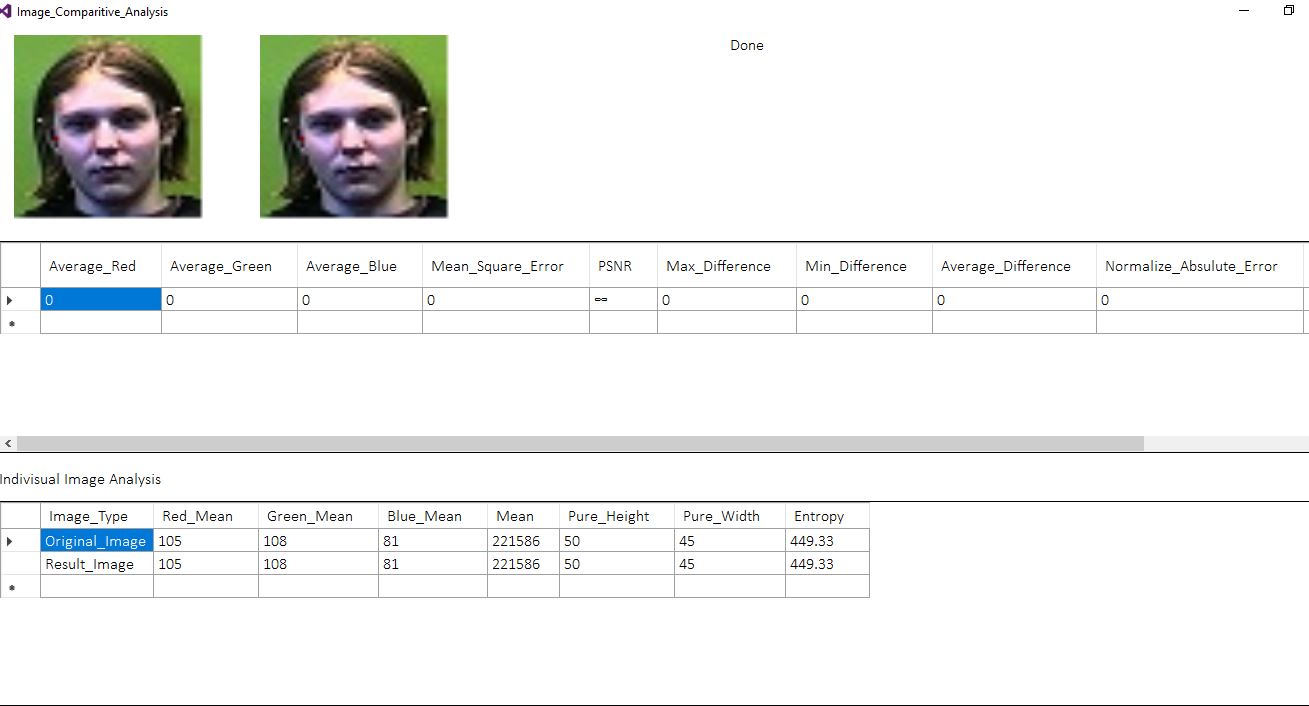
Resultant quantization error



The quantization error chart (Qe)



**Image comparative ananlysis**

****

##### Individual Image analysis

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Image Type** | **Red-Mean** | **Green-mean** | **Blue-mean** | **Mean** | **Pure Height** | **Pure Width** | **Entropy** |
| **Original Image** | 105 | 108 | 81 | 221586 | 50 | 45 | 449.33 |
| **Resultant Image** | 105 | 108 | 81 | 221586 | 50 | 45 | 449.33 |

***CHAPTER VI***

**6.Appilication**

***CHAPTER VII***

**7.1Conclusion**

The proposed framework provide a novel approach for data hiding using half tonning visual cryptography technique.In the proposed work,important parameter to be consider is a digital protection wall.This wall acts as barrier between the secret data and the carrier.Also the the systems hides the data inside the carrier without affecting its perceptual quality.Thus making it imperceptible to unauthorized user.The replacement of secret bit is carried out via Higher LSB rather than the conventional Lower LSB replacement thus gives another advantage for hiding secrete data,so that only intented usr would be able to decode the actual transmitted data over media.

**Future Scope**

In future, depending upon the developing such technology,for data hiding the proposed system can be enhance by sendin the reciver side information within the carrier,so that the user don’t need asked for parameter required for decoding the same. But problem with such system that if data loss occur it mat affect that part of carrier leading ti inefficient transmission of the carrier. But with the advent of more advanced technique this can also be resolved,thus reduce the work of user while using the system