CHAPTER 1.

INTRODUCTION

1. Introduction

With the strong stimulation of computer networks, the Internet has revolutionized our society prosperity and dissemination of digital information, computer users increasingly important to find better ways to protect personal and confidential information. A common way to ensure that such information is unreadable string encryption of sensitive data to prevent unauthorized access and viewing. Unfortunately, the encrypted data is pulled toward the obstacle you do not need concentration, assuming that the encrypted data may be worthwhile to privacy and confidentiality. Therefore, the encrypted data is often an object, so it is vulnerable to illegal interception of data transmission through the public communication channel from unauthorized tampering. In order to conceal the existence of confidential information. Hope for the future of security and safety has been discussed a memo sent antiquity.

Information is any organization's wealth. This makes the first, deal with the problem of confidential data security issues. Whether we choose security purposes and methods of burning concerned about security. Steganography is introduced as an alternative data protection solution.

Some information is hidden in the general idea of digital content, has a broader application classes. In such applications, the technology involved is referred to as information hiding. For example, a document may be printed on the image, it may cause the user's high resolution version of the metadata annotations. Under normal circumstances, the metadata provides additional information about the image. Although the meta-data can also be stored digital image file header, this method has significant limitations. In general, when a file is converted to another format (for example, from TIFF, JPEG or BMP), meta-data will be lost. Secondly, cutting, or any other form of image processing destroys metadata. Finally, the metadata may only be attached to the image, as long as the image of the digital form and printed images are

missing. Information hiding, the metadata file format and image state (digital or analog) image, regardless of travel.

There are three basic principles behind the hidden information. The first is the ability, which is on the cover files that can be embedded in the amount of information. Information hiding algorithm capable compact messages are stored in a file, it has a message can not be found no benefit, but also a serious impediment to its size. The second is security, it refers to how easy it is in a file that can detect hidden information third parties. Intuitively, if the message is to be hidden, an ideal algorithm for the way information is stored, it is very difficult to detect. Finally, robustness, modified before the message can withstand the amount destroyed a third party. In hiding and watermarking, surgery is more concerned about the capacity and safety, mainly concentrated in the robust watermark.

Information hiding is applied to the three principles of information hiding embedding technology and coding techniques.

Information hiding two techniques can be used, i.e. the secret message data in the file is modified in a specific pattern with different possible combinations, then the data transmission in a communication network with the target key code pattern. In this case, a hacker can send that message, but the same can not be explained, because the key to the message is modified, and may assume it as spam or several redundant information. This art is called information hiding encryption. Cryptography can be used for message security can also be used for authentication.

Strict security encryption technology research began incense, who introduced information theoretical definition of security: cryptographic system is secure, and those who see the ciphertext - fried messaging cryptography - the opponent did not receive additional information about the plaintext - Translation out the contents. Encrypted message files usually require equal lengths of keys.

While encryption technology to protect the content of the message; steganography is hiding its existence. Steganography comes from the Greek word meaning to write covered. Pervious projects are indicated that the recommendation

traffic is exchanged between coded form of communication, via e-mail or mail exchange spy secret communication.

During World War II secret camouflage blank password in an innocent-sounding messages used in the following examples.

"Apparently neutral's protest is thoroughly discounted and ignored. Islam hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suits and vegetable oils."

Taking the second letter in each word the following message emerges:

"Pershing sails from NY June 1"

With the advent of the internet, Steganography has found new applications. But, at the same time it is also vulnerable to more powerful attacks since the medium is relatively insecure. Discussion of above is that there is nothing doing on GIF image.

1.2. Limitation of the current Technology

- The most of existing tools worked on single images.
- Steganography has been used and many heavy Steganographic tools are existing but firstly never GIF has been as a secret file.
- Existing technique used text, single image, audio as a cover file but till now Video file has not used as cover file.

1.3. Problem statement

Thus the main Problem Statement which can be summarized form the above discussion is that GIF image we may used as a secret file and hide it inside a video file by using cryptography and DCT algo.

1.4. Proposed Approach

- GIF image used as a secret file
- Cryptography applies on GIF image.
- Hide crypto applied file inside a video.

- Used DCT algorithms on video.

1.5. Dissertation Outline

The central idea of this thesis is to develop a code for securing the message as a GIF image over a cover video file using DCT Steganography for which an algorithm may also be designed to embed message level security.

- **Chapter 2** introduces the basic techniques of security and related work on which the proposed work has been drafted.
- **Chapter 3** will be the proposed work
- **Chapter 4** will have analysis and results of the performance of the designed tools
- **Chapter 5** will be the Conclusion, limitations & Future Work followed by references and Appendices.

CHAPTER 2

LITERATURE SURVEY

2.1 What is steganography?

Steganography to obscure the actuality that announcement is enchanting position, by hiding information in other information. Sculpture is the Greek word surreptitious derivation and resources "concealed writing", denotation "covered or protected" from the Greek word graphei means "writing." Steganography, therefore, it does not seem all relevant information is hidden in the information hiding. Some people think that if a person or object is hidden inside a thing then his or she will not have any idea there any hidden information, so people will not try to decrypt the message. Basically there is nothing secret is to use human perception, human senses qualified to seem for paperwork within information they have, though this software is available.

Now you can ask, what is called steganography. Steganography is the most common use of hidden files inside another file.The purpose of steganography is covert communication from third parties hidden messages. Steganography in the contemporary intellect of the phrase usually refers to information or documents have been hidden in a digital image, video or audio files. Steganography is basically the use of human sensory perception of people who do not look at the training of hidden information inside the file.

Steganography, under normal circumstances, the actual information cannot maintain their original format, so that it is converted into another equivalent multimedia file, which is hidden in another apparent object. This message (called as the cover text, such as images, video or audio according to the usual conditions) sent to the recipient via the network, the actual message is separate.

2.1.1. Steganographic Methods:-

The subsequent method provides a very nonspecific portrayal of the pieces of the steganographic development:

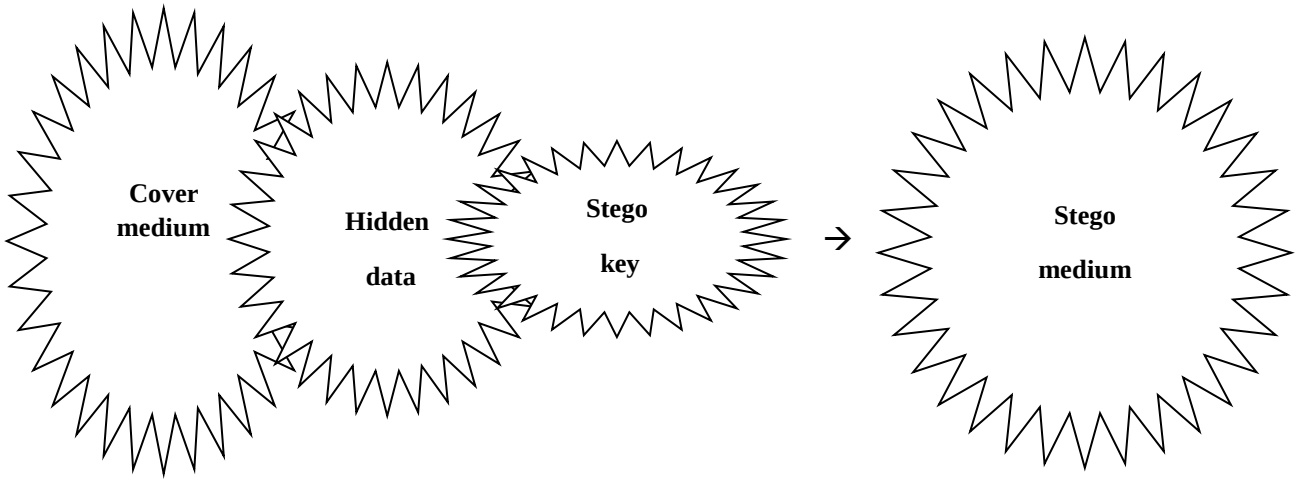


Fig 1: Process of creating stego medium

Cover medium→ is the file in which we will hide the hidden data.

Hidden data→is the secrete data file.

Stego key→ is the shared secrete key known to intended recipients.

stego_medium→is the resultant file obtained after embedding process.

2.2.2. Steganography Techniques:-

- **Text Techniques**
- **Image Techniques**
- **Video Techniques**
- **Sound Techniques**
- **Other Techniques**

But here we will discuss two techniques.

First is Image techniques and Second is Video Techniques.

A. IMAGE STEGANOGRAPHY TECHNIQUES

The various image steganographic techniques are:

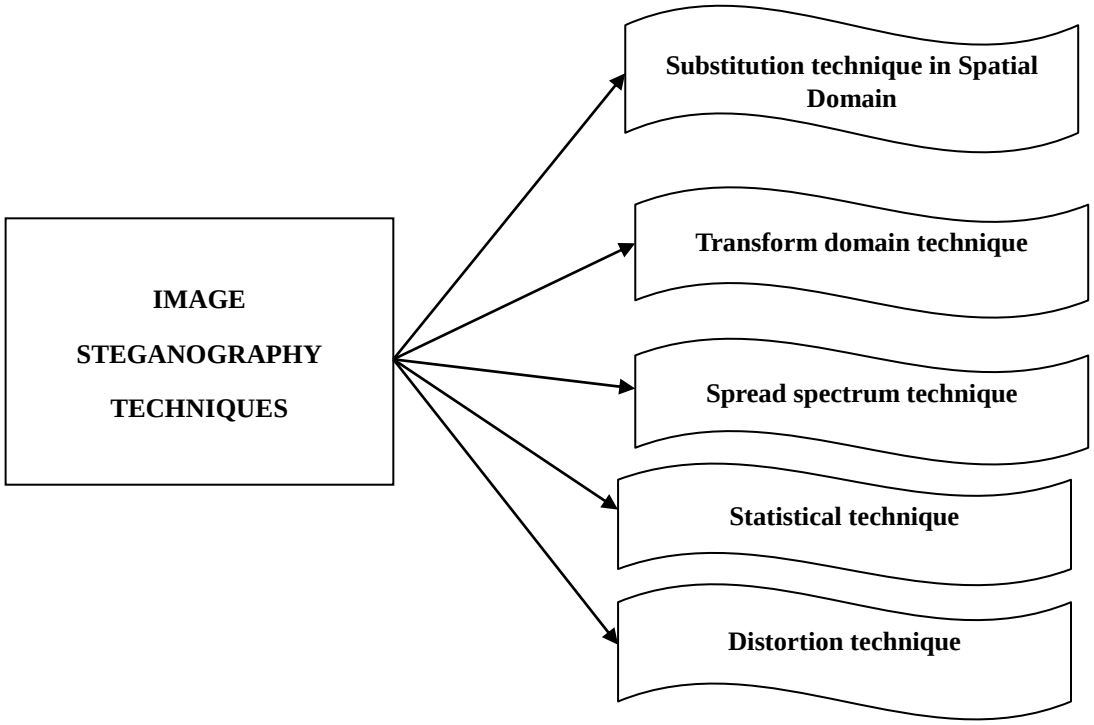


Fig 2: Type of Image Technologies

1. **In the spatial domain alternative technologies**:

   In this technique, only the most important target site lid replaced a complete covering of the object, without modification. This is a simple data hiding method, but it is very weak against even simple attacks, such as robustness, alteration, etc..

2. **Transform domain techniques**:

   Various techniques transform is separate cosine convert, the separate wavelet convert and quick Fourier convert of the cover image of the convert coefficients of a added commanding assault, such as compression, so that to hide information, the filter.

3. **Spread Spectrum Technology:**

More than the minimum bandwidth required to send a message, the message is stretch in excess of a extensive occurrence bandwidth. In every occurrence posse signal to noise ratio (SNR) is tiny. Therefore, does not destroy the cover image is difficult to completely remove the message

4. **Statistical technique:**

Quantity is separated into block, each block of information bits to be hidden. By shifting the cover up the values of the attribute information indicates the encoding. The amount of block remains unchanged if the message block is zero.

5. **Distortion technique:**

The information stored in the signal distortion. Add sequence changes encoder and decoder checks cover original cover, twist caps recover the secret information of the various differences.

The following discusses some common image camouflage technology has been in liberty and convert field.

- **Spatial Domain Steganographic Method**

  - **Data Hiding by LSB:**

In this has been projected in the invented story concerning the various data hidding technique. Particular of the technique used, is according to the function of the cover image by direct replacement message bit LSB of the smallest amount noteworthy bit of the plane. LSB method is typically a high capacity, but unfortunately into LSB minor image processing, such as cropping and compression.

  - **Data Hiding by MBNS**:

2005, Zhang and Wan also more symbol-based systems (MBNS) based on human visual sensitivity (HVS) proposed adaptive steganography program. Hiding capacity of each image pixel is called by a local change. The calculated attractive into explanation the limited variations in the human visual sensitivity factor. Local values represent a great change in the region is a pixel belongs busy / marginal zone, which

means more secret data can be hidden facts. On the differing, when the narrow variation is small, less confidential data will be hidden to the image block, as it is in the smooth region. In this way, the hidden image-quality deterioration is not observable to the human being eye.

❖ **Data Hiding by MBPIS:**

Many image plane camouflage (MBPIS) proposed by the Nguyen Yin and Li in IWDW06. The algorithm is designed for some classic RS steganography methods, such as security. The main objective of this paragraph is a detail which is dedicated to the uncompressed image steganography algorithm.

❖ **Data Hiding by QIM:**

Quantization index modulation (QIM) is a commonly used data digital watermarking technology, which can use secret. Quantizes the input signal x to an output y of a set of quantized parameters, i.e., become Qm (). Quantization is using gritty by the message bits m.

❖ **Data Hiding by PVD:**

Wu and Tsai's pixel values difference method (PVD) can be successfully camouflaged images while provided that elevated embedding capacity and first-class imperceptibility. A pixel value difference of the corporal vapor declaration (PVD) process of classification into non-overlapping blocks of pixels includes two connections and modified data is embedded in each block (pair) of the cover image pixel difference. The pixel values the original large difference allows a greater modification. In the extraction stage, in the original scope of the table is necessary. It is used to partition the image hidden by the same method used for the cover picture. PVD methods based on a variety of method have been projected. Chang et al, which proposed a new method that uses three-way with respect to the embedding competence and PSNR than the original PVD method, which is better pixel value difference.

➢ **Transform Domain Steganographic Method**

Transform domains hidden in the major areas of cover images, which makes them resistant to various image processing operations, such as compression of

the news, and many other enhancements transform domain methods exist. Conversion function is widely used including discrete cosine convert, Fast Fourier convert, and wavelet transform. And DCT, FFT or wavelet hidden information of the basic method is to cover picture, adjusting the coefficients, and then reverse the transformation. If the selected coefficient is good and manageable size changes, then the result is very close to the original.

❖ **DCT based Data Hiding**:

DCT is a mechanism 88 for successive pixel blocks 64 DCT coefficients in the frequency domain from the spatial domain transform images in JPEG compression algorithm. The quantify DCT coefficients, the least significant bit are used as one of the hidden messages embedded in the redundant bit. DCT coefficients of a single modification affected all 64 image pixel. This modification, since the place in the frequency domain and space domain, there are no obvious visual difference. DCT transformation has the advantage in excess of former transformation can able to be obtained by 8 × 8 sub-image becomes visible boundary between (to be referred to as block artifacts) to minimize the appearance of the equal wedge. Statistical properties of JPEG file are also saved. The trouble is that this development only applies to JPEG files, as it assumes that there is a certain statistical distribution are common JPEG files cover data.

Some common DCT based steganography methodologies are described below.

⇨ **JSteg/JPHide:**

JSteg and JPHide are two classic JPEG steganography tools, the use LSB embedding technology. JSteg secret information is embedded into a cover image, by successively replacing the secret information bits zero quantized DCT coefficients LSB. Unlike JSteg, quantized DCT coefficients will be used to hide secret messages in JPHide bit randomly selected a pseudo-random number generator, which can be controlled by a key. Furthermore, JPHide selected coefficients only modify the least significant bit, but can be switched to a mode in which the modified bit the second least significant bit plane.

⇨ **F5:**

F5 steganography is Westfield. Coefficient absolute value, instead of replacing the message bits LSB of the quantify DCT coefficients is concentrated by individual, if it is needed to be modified. F5 embedding algorithm randomly selected message bits of the DCT coefficients, and the use of unseen communication entrenched in the matrix certain length, minimizing the number of changes required. In the embedding process, the message length and the number of non-zero AC coefficients used to determine the optimal number of the matrix embedding the modification cover image is minimized.

⇨ **OutGuess:**

Provos got that UNIX source code. There are two well-known releases: see through 0.13b, it is vulnerable to statistical analysis and see through -0.2, including the ability to save statistical properties. When we talk about see through, it is called seen through 0.2. See through the embedding process is separated into two stage. First of all, see through embedding secret message bits, skipping 0's and 1's random walk to the quantized DCT coefficients LSB. Embed after correction coefficient, which is embedded in the process did not choose to make the world a DCT image matching camouflage cover image histogram. It can not through the chi-square test.

B. VIDEO STEGANOGRAPHY METHODOLOGY

We have several new approaches for video steganography literature. Some of the most well-known methods are discussed. First, the most commonly used method is the least significant bit (LBS) hide secret data most significant bit host video. This method is very simple, you can hide a lot of data, but the hidden data might be missing some files after conversion. Another well-known method of study is called also spreading. This method satisfies some geometric transformation using robust criterion. The small amount of hidden data is lost. Hide the amount of the loss is also small, even with a low bit-rate compressed file. This method satisfies the other criteria are also introducing some security. There methods dimensional lattice structure, based on the data embedding rate is high, is a powerful motion compensation coding or enable high levels of hidden data and the high number of the host through changing the number of data quantization level embedded data. Wang et

al. people proposed a technique for high-capacity data hiding using a separate cosine convert (DCT) transform. Its main goal is to maximize payload, while maintaining robust and simple. Here, the secret data is surrounded into the congregation indicator is modulated on the I frame blocks of quantized DCT coefficients. Vectors made in embedding method, the method uses a reliable method, the video codec standard (MPEG-I and MPEG-II). This method is embedded in host audio information of the video frame pixels. In addition, anti-rotation, scaling and translation (RST) method is also used in video watermark. In this method, the secret information is embedded into the watermark pixels along the time axis of the lowest segment (WMS)

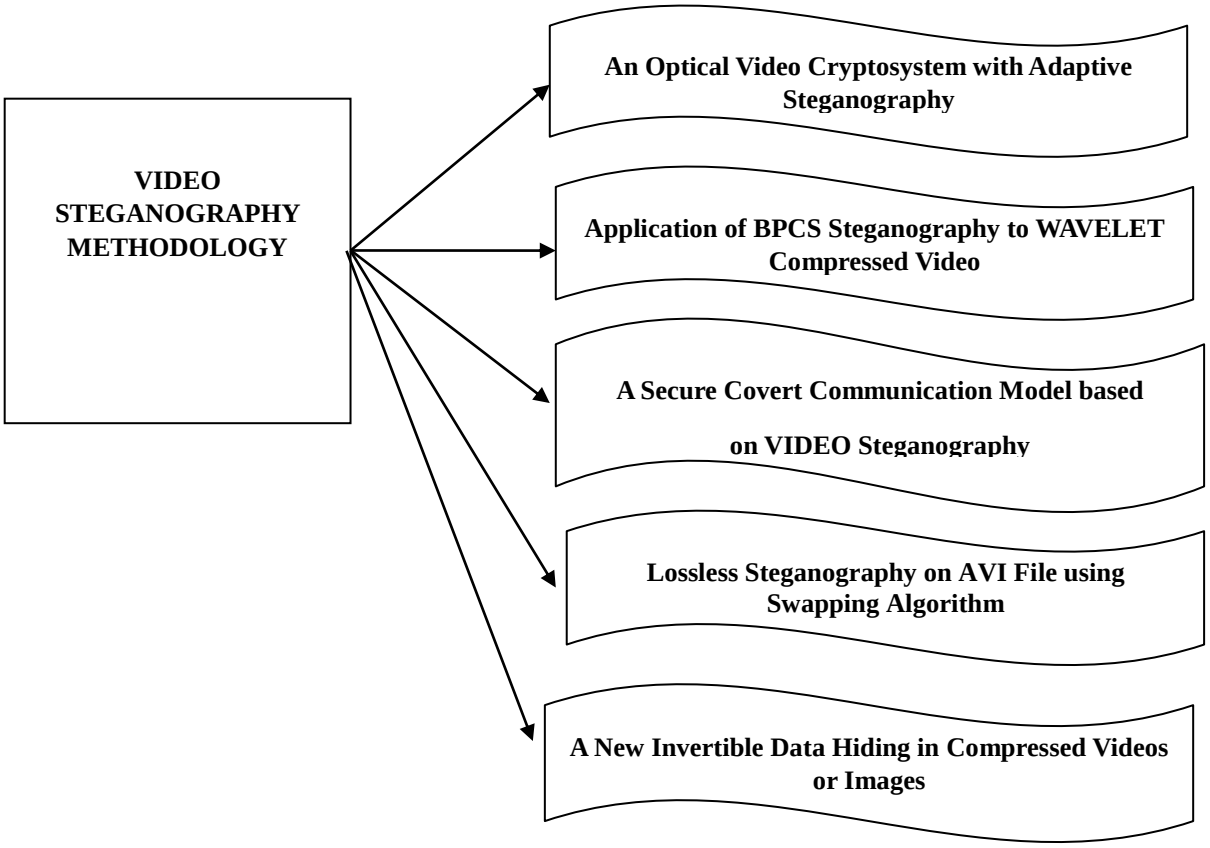


Fig 3: Types of Video Steganography Technic

A. BPCS steganography application of wavelet compression video

Steganographic method uses lossy compression of video, it is provided a ordinary way to send large amounts of not to be disclosed data. The prediction method was based on wavelet compressed video data and bit-plane involvedness segmentation

(BPCS) steganography. D is set based on wavelet transform video solid methods, such as hierarchical tree segmentation algorithm (SPIHT) and discrete wavelet transform into digital planar structure Motion-JPEG2000 video wavelet coefficient; it was applied in the wavelet domain BPCS steganography. Three dimensional SPIHT's BPCS steganography, motion JPEG2000, BPCS steganography and testing, which is an integrated 3 - Video Coding SPIHT of BPCS steganography and motion JPEG2000 and BPCS, respectively. Experimental results show, 3-D SPIHT's BPCS Embedded Motion JPEG2000 is the advantage in terms of performance.

B. Adaptive steganography an optical video cryptosystem

Steganography adaptive encryption system to encrypt and decrypt the video sequence. Using double random phase encoding optical encryption algorithm for undetectable and detectable of video sequences. First transferred to the RGB video signal pattern, and then separated into three channels: RGB. Each channel consists of two random phase masks generated session key to encrypt. For higher security, the session key is an asymmetric transformation. Video frame encryption key, and then embedded content and low distortion data embedding technique dependent. Hidden key was generated video signal data encrypted by sequencing a particular frame hidden LSB zero. Experimental results are showed that the adaptive steganography has better performance than traditional secret video encryption.

C. Video-based steganography a secure covert communication model

Steganography models cover with the existence of former susceptible data, regardless of the format of the video file. Pixel-wise manipulation of color original video files embedded secret data on the basis of the proposed model. Secret message is divided into blocks embedded in the video before the lid. This block was embedded in the pseudo-random. Locations are from reordering agree key. In addition, each video frame of statistical information by the secret message block position, even if the original video interceptor cover can be dynamically changed to reduce the possibility of re-ordering. Four types of confidential data; they are used of quantitative valuation reproduction. The model is assessed compared to overwrite the original video signal height indication to sound ratio mean reduction, and measuring all the video frames in between the original file and the secretive average mean square error (MSE). The results show minimal degradation secret any type of video data files, and various sizes

of secret messages. Finally, the embedded video file size estimation is proposed based on file formats and sizes

D. Lossless AVI files using steganography exchange algorithm

Cooperative Photographic Experts Group (JPEG) image stegano stormily cells and Audio Video (AVI) video stegano connecting the value and dimension of the key exchange algorithm performed. Increase strength, and through the use of UTF-32 encoded files lossless stegano AVI Comparative analysis technology. However, the payload capacity is low.

E. A New Invertible Data Hiding in Compressed Videos or Images

Adaptive reversible stirring picture experts group (MPEG) video information hiding method. Hidden data can be restored without the need to indicate the target, the first secret video, if desired, can restore the original copy of the MPEG video data. This technique is in the frequency domain. It has a secret communications applications with low complexity and low visual distortion. However, people with low load capacity.

2.2 What is cryptography?

“Cryptography "is from the Greek word κρυπτο (hidden or secret) and γραφη (written). Curiously, the encrypted secret writing is an art more generally, it is considered as an art of the dislocation obvious way is difficult to understand allowing Arcane unmangling information encrypted encryption technology to provide basic services by the client to send information, it can prevent others from reading between the participants in this book represent information concentrated we will numbers and mathematical manipulation of these numbers are based on what kind of encryption technology. This cryptography can also provide other services, such as ...

- **Integrity Check** → reassuring message that has not been the recipient .Change, because it produces a legitimate source

- **Verify**→verify someone's identity

However, the conventional use of passwords. A meaning in its unique figure is known as plain text or clear text. Erroneous information is called ciphertext. This process was called encrypt the plaintext from the ciphertext generated. Reverse encryption and decryption.

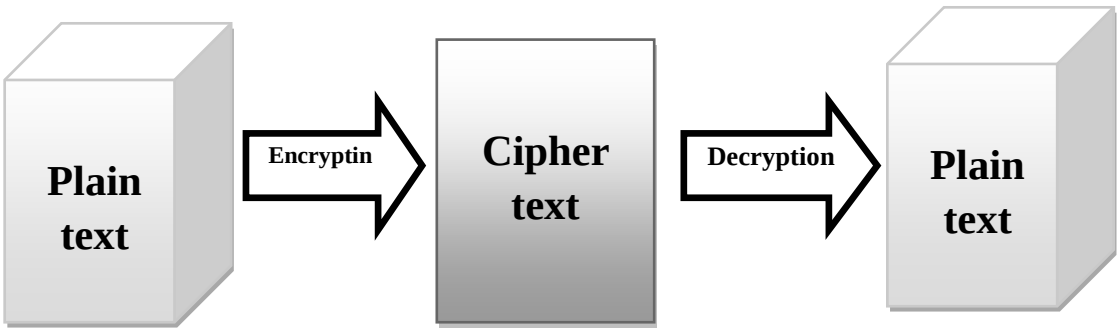


Fig 4: Basic of Cryptography Process

Although cryptographer was invented ingenious logo, cryptanalyst are trying to break these two disciplines code. These constantly are trying to stay in advance of every other. At last, the victory of the code-breaking, encryption the elementary purpose.

"Lacking a lot of tidy populace to solve a problem,

Then it most likely will not be resolved (soon)."

Encryption systems often involve algorithms and secret values. Secret value is called the key. In addition to the algorithm is a key reason is that it is complicated to keep the design of new algorithms that is allowed to reversible scrambling information, it was difficult for new design algorithms include: explaining people with whom you want to start to communicate strongly. By the way of a good encryption scheme, it is absolutely OK to have all and sundry, including the shocking guys (and password specialists) know algorithm, key algorithm, because there is no knowledge, is not conducive to anti-suit (unmangle) information.

A key concept is similar to the combination lock combinations. Although it is well-known concept, combined with the lock (secret number you dialed the correct

sequence and locks open), you can not open the lock, it is easy not know combinations.

2.2 .1 TYPES OF CRYPTOGRAPHIC FUNCTIONS

Encryption has three functions: a hash function of the secret key function and public key functions. Public key encryption, involves the use of two keys. It included the uses of a key encryption key. Hash function is used of the zero key.

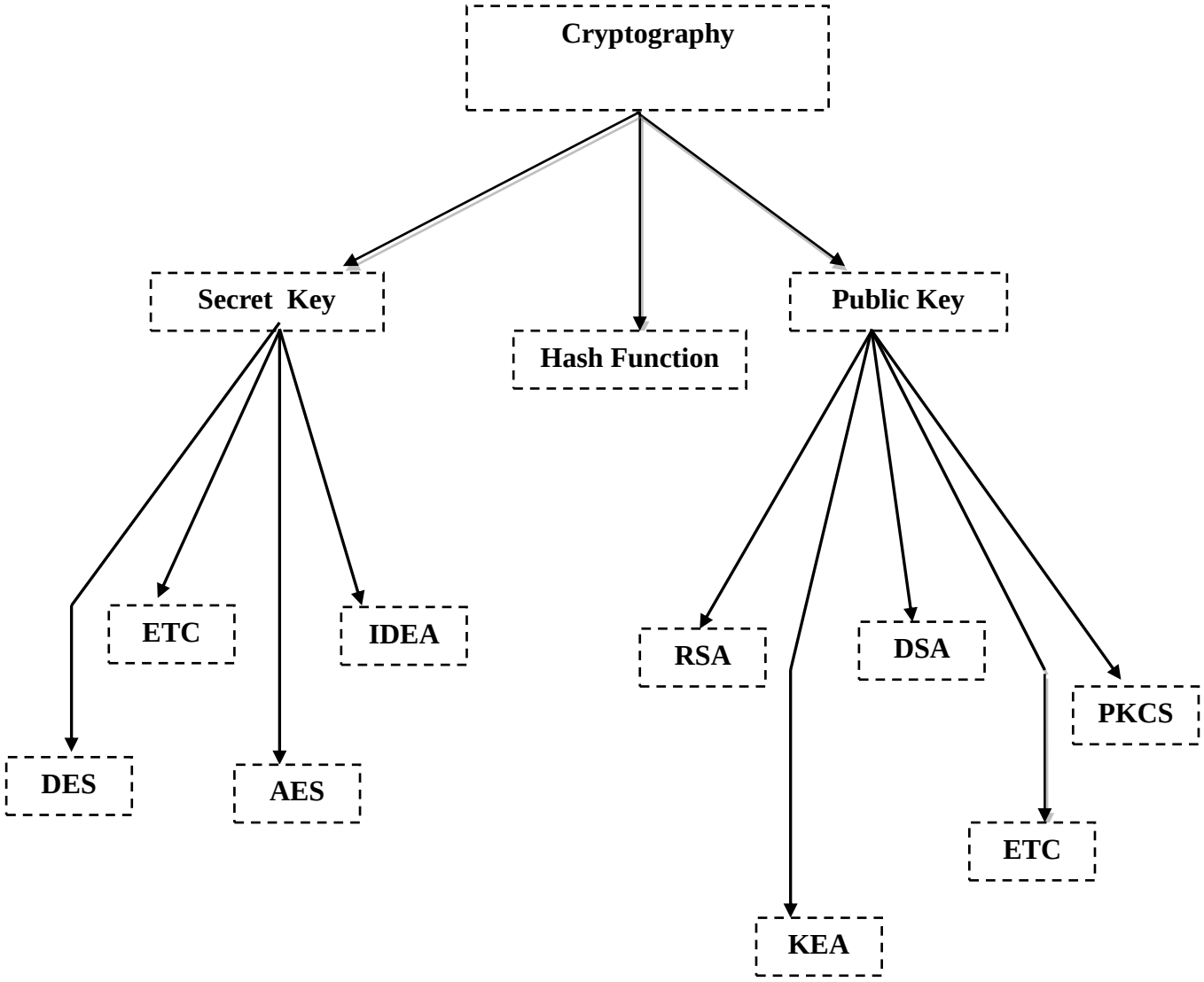


Fig 5: Detail summary of Cryptography Types

As key encryption may be the most sensitive part which we have to introduce the first.

A. SECRET KEY CRYPTOGRAPHY

Key cryptography included the use of a single key. In the message (called plaintext) and encryption key data incomprehensible (called IRS Publication! This is just one finger sliding, we mean "ciphertext"), which is about the same length as the plaintext. Decryption is the reverse encrypted, and uses the same key to encrypt.

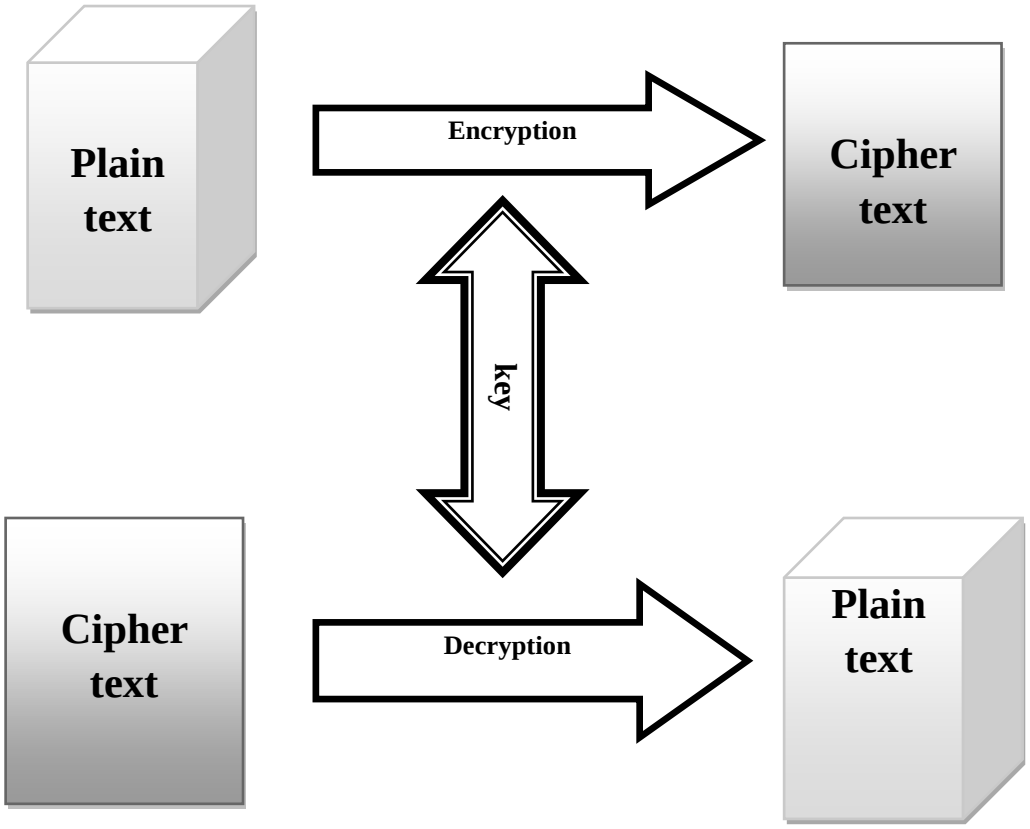


Fig 6: Process of the Secret Key Cryptography

Sometimes it referred to as a conventional encryption key to encrypt the symmetric encryption. Captain code and single code encryption key algorithm, the two examples, although they can easily be broken.

B. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography was sometimes called asymmetric encryption. Public key cryptography was a relatively new pasture, fantasy DIFF76b (There was

rumoured that the National Security Agency, or similar organization might find this technology early). Key encryption key cannot be shared. Instead, each person has two keys:

→ Requires a private key will not be disclosed to any person,

→It is best key as a world's public key.

In any case, used of public key encryption key. In this world, there is a person in life, whose whole purposed is to try to confuse people. They used the long-term key, public key encryption private key, or private key is used term. The key technologies are used here. We was carried on to the field is mainly significant assistance was to convince people to using the correct terminology felt a strong long-term means to use only one key encryption key figures. Long-term private means, you were using public key encryption, the key must be disclosed.

There is something about the terminology of public and private misfortune. These two words start with the sports; we want to have a single letter represents one of the keys. Letter P will not do. We will use the letter e is the public, because the use of public key encrypted significance. We will use the letter D refers to the private sector, because the private key to decrypt the communication. Encryption and decryption are two mathematical functions are inversed.

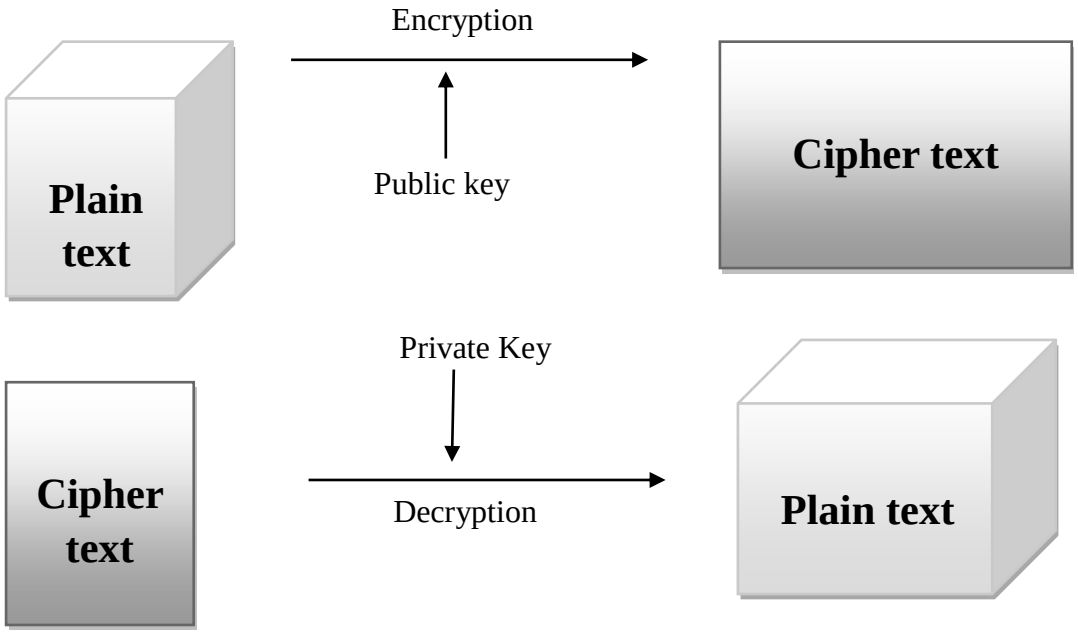


Fig 7: Process Of The Public Key Cryptography

There is an supplementary fixation you can do, which was to generate a digital signature public key technology news. Message number about digital signatures,

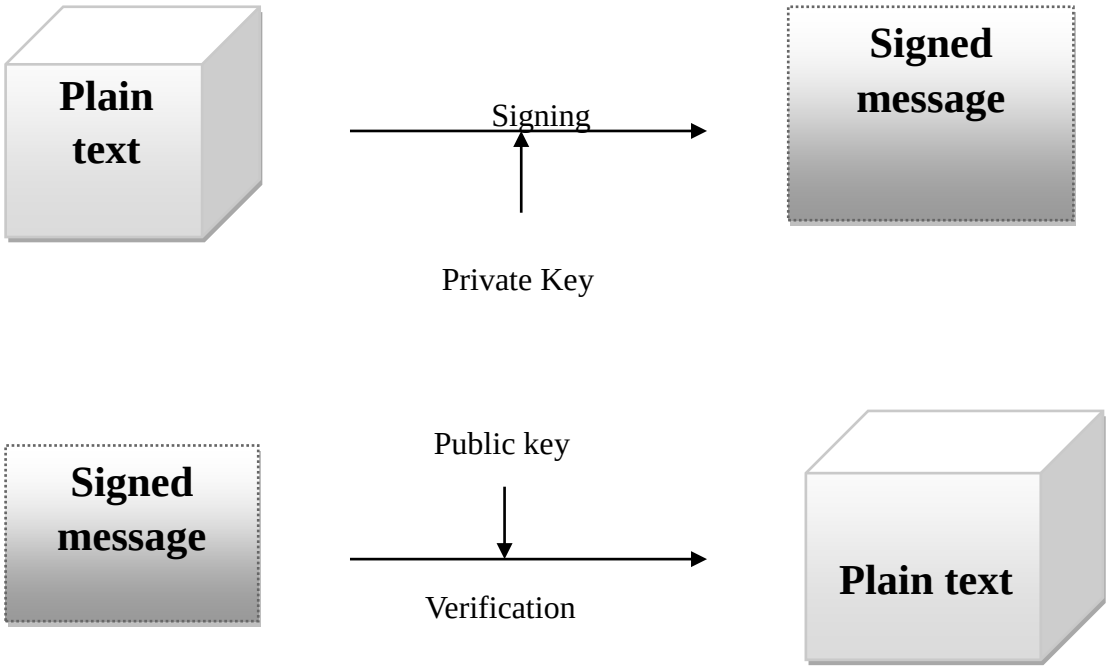


Fig 8: Process Of Signing System In Cryptography

Description integrity checked to verify or message integrity code (MIC). However, different parity, anyone can be produced, can be only generate a digital signature be acquainted with the private key. Because unlike a secret secret key used to create the necessary knowledge MIC public key to confirm the signature. Therefore, any one who can authenticate the MIC can also generate one, it can be replace with a changed message and the corresponding MIC. Instead, you only need to know the public key signature verification. Therefore, Alice can generate a signed message, only she can produce, while others can verify that it is Alice's signature, but could not forge her signature. This is called a shared material goods signature, but it is able to distinguish handwritten signature can be forged.

C. Hash Function

Hash function, also known as a message digest, and a one-way encryption algorithm,the use of a key (C). Instead, a fixed-length of the plaintext hash

value, manufacture it unfeasible to restore the contents of plaintext or length. Hash algorithms were typically used to providing a digital fingerprint of the file's contents was used to make sure that the file had been intruders or viruses had not been altered. Hash functions were usually many operating systems to encrypt passwords. Hash function was provided a measure of the integrity of the file.

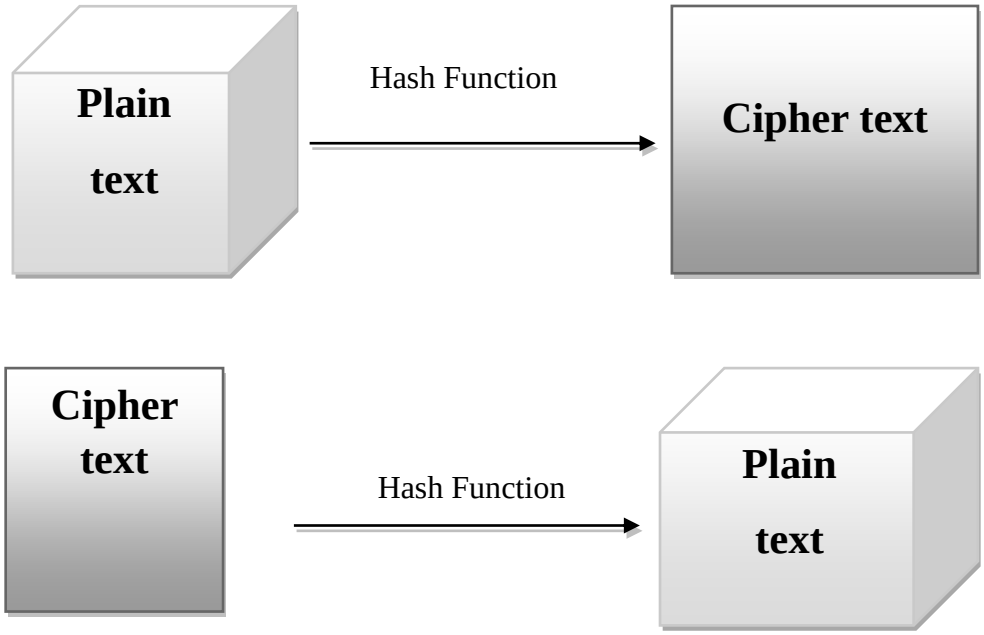


Fig 9: Working Process Of Hash Function

2.3 STEGANOGRAPHY WITH CRYPTOGRAPHY:

- **Relatively hidden and encrypted**

Information hiding and encryption technologies are closely related. Encrypted message contention, it cannot be understood. Steganography on the other hand, the hidden messages, so there is no acquaintance of the continuation of the message. Encryption technology is relatively plaintext and ciphertext portion. Steganography, more able to cover the media, secret between the media, as well as part of the message may be. The end result is a cipher text encryption, privacy, and the end result is secretive media. Steganographic information capacity or non-capacity be encrypted. If it is encrypted, then the password is applied to the analysis techniques to extract information.

- **Combination of information hiding and encryption.**

Those who seek the ultimate in personal communications can be combined with encryption and secret. The encrypted data are used for carrier medium than the

plain text naturally occurring phenomenon, mostly tricky to distinguish. There was numerous tackle, the data could be encrypted and hidden in the selected medium. In some cases, send an encrypted message was span suspicion, but the message is not visible. Both methods can be combined together to produce better protected messages. Steganography failure message, it can be detected; it was still useless because it was used of encryption technology.

2.4. History of Steganography→

History provides numerous cases whereby information had to traverse the hostile or enemy territory to reach the destination undetected. By age that has spent many ingenious ways to conceal information, and over time, invariably discover new ways to improve old as well as processes. These examples are:

- In ancient Greece, the method, that is, a person is selected as a messenger, they shave their heads. Secret message to his bald head tattoo hair was allowed to grow again to its normal length. Messenger and then continue through any security check purposes, and introduced myself, who will then shaved his head to read the secret messenger text message receiver. A major disadvantage of this approach is the time lag

- Another way in ancient Greece wax-covered tablets. Wax tablet will be scraped off, the message written on the bottom of wood wax re-hide messages. The tablet receiver then simply scrape wax message is displayed again.

- A famous Greek, Aeneas tactical design methods, so that the Greek alphabet letters represent boring holes into wood plate. Yarn, and then through the hole, so that they will spell out a message.

- During World War II, invisible ink for the seemingly standard, non-toxic memo or letter, to conceal information. Invisible ink common source is milk, vinegar, juice and urine. The benefit of this move towards is that when heated, each of these materials darken, are particularly effective at this time, due to the fact that the source can be readily available.

- German particle covert communications technology invented in 1941. In the micro-points, neither hide or encrypt these messages, but its too tiny to make out by the naked eye. Particle technological advances continue to this day, the embedded messages using genomic DNA strand steganography the latest technical developments.

One way smarter Gaspar Schott and detailed his book SCHOLA Steganographica. It involves encoding information through specific notes in a paper match letters. Normal glance, this seems to be an ordinary song. If a person really plays a musical instrument, however, chances are, it will not be happy ears.

2.5. Modern Steganography:-

As early as last discussion, the encryption technology has become very popular science. Secret encryption knowledge and its function is very close, you can highlight the main difference. Encryption is hiding the message content. The encrypted data packet at the same time itself is valuable evidence of the existence information. Steganography goes a step further, so that unofficial users cannot see the ciphertext. Hereby we can define additional attributes encryption and secret, the output looks the same.

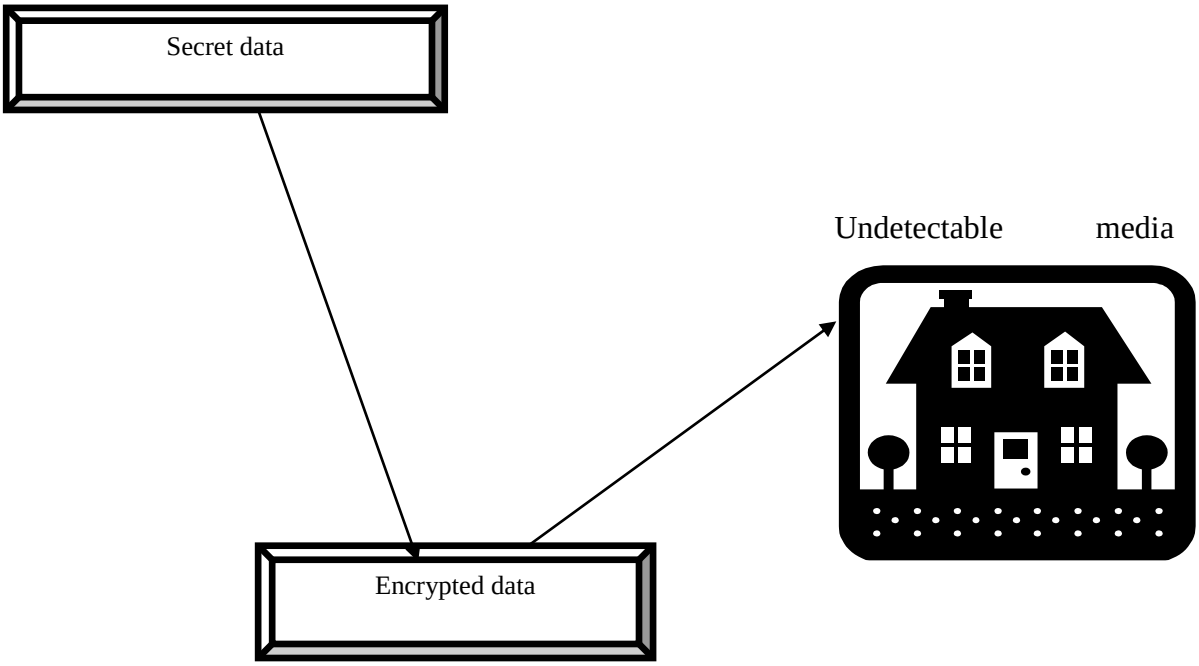


Fig.10: Steganography working technic

Imagine a common situation, when a person of his important business data encryption. Robbers suddenly capture and torture him to disclose the encryption key. They asked him to give their private key, or they are highly suspected criminal. Next, if the police bribe. Would not it be better if he could plausibly deny the existence of important data?

Repeat steganography famous example is the issue of prisoners Simmons. Bob and Alice in prison, they are trying to escape. Their cells far at a distance from all other, allowing only traffic through the prison staff to send messages. If the warden detected any signs of conspiracy, he would ensure their cells, or even more. Bob and Alice are aware of these facts.

Happily, they were arrested before they have agreed to a stegosystem. Stegosystem described secret message is embedded into a cover text (seemingly innocent messages)

One can discriminate among submissive and energetic warder stegosystem. Just passively guards monitor the communication channel. He can pass through a number of statistical tests cover texts, but do not modify them. When the network data are picketed through intrusion detection system is the same situation. From the application of this grassland is frequently referred to as "traffic safety.

On the other side, active warden cover text manipulation to exclude the possibility of covert communication. Bob and Alice must use very complex embedded algorithm. Hidden information has got to be capable to survive a multiplicity of cover media recoding, use of error-correcting codes recommendations. A typical real-life applications are watermarks and fingerprints.

Now, I want to explain what to do video secret. Several authors use a text file as a hidden message inside the video images, such as JPEG, BMP, other authors use the video file as a hidden file information, and cover. After reading all these files, I get, gif image as a hidden message in the video file, nothing has been done.

- **"Mrs.Archana · Vaidya, Puga N. More, Rita · Fegade, MadhuriA.Bhavsar, Puga five Laut, RH"** a secretive process. It is not like the spatial domain methods, the undisclosed in sequence is embedded in the discrete

wavelet transform result in high frequency coefficients. An encryption algorithm is used to modify the difficulty in understanding the form before embedding secret messages. These algorithms have news, an unexpected user self-destruct on the Internet, thus providing satisfactory security. Blowfish algorithm uses block encryption using the undisclosed key to encrypt and decrypt the message. Blowfish is a gradual increase of more than DES, 3DES, etc. designed to improve security and performance. The algorithm was used a changeable key in size is 448. Que, in the frequency domain embedding secret messages

.

- **"ChangyongXu, Zhengzhou, Xijian flat, Zhengzhou, Zhang Tao,"** the author in this article, secretive related algorithms in MPEG-compressed video stream recommendations. In each GOP, to reduce the data to extract the be in charge of in sequence is embedded in the I frames, P and B frame, the data was transferred again embedded in a chubby stirring speediness of the macro block motion vectors used to place video processing firm.

- **"S Suma's Christal Mary"** Author describe in the paper shows real-time information hiding, which is a compressed video bit stream using a new process. This technique was depended on the real-time video steganography information hiding. Steganography methods are two techniques, secret image and video steganography very similar. This paper propose a new packed together video secure steganography algorithm expansion. In this algorithm, the embedding and detection operation was performed entirely in the packed together domain, not the decompression process.

- **"POONAM V Bodhak, BaisałGunjal**" this article the author describes design software to develop a steganography application data remains hidden video files in the computer's text and receipt of hidden information. This design can be embedded in a video file in secret files and video does not lose its function, use the DCT and LSB modification method this method is suitable for subtle changes to this proposed approach is committed to high-security eavesdropper cannot detect concealed information.

- **"P.Paulpandi1 Dr.T.Meyyappan Karaikud"** the authors describe a new process, using the motion vector, the hidden data in the object movement. In

addition, to enhance security of data, the data was encrypted by mean of the AES algorithm, then foot of the wall. These data are hidden in objects moving horizontal and vertical components. PSNR value is calculated after the video quality assessment data hiding.

- **"Dipesh G. Kamdar1 Dolly Patira, the CH Vithalani Doctor,"** the authors say, in order to allow the faithful and secure communications, double hiding technique is proposed in this paper.

- **"AMR A. Hanafy, up I. Salama and Z. Mohasseb of Yahya's"** the author described a secret model to cover up obscure the continuation of other secreted data, regardless of its format video files. The representation is absolutely dependent relative on the pixel-wise color embedded confidential data manipulation original video file. Secret message is divided into blocks before the video is embedded in the cover. Block, and then embedded in the pseudo-random positions. Rearrange the position are derived from the agreed key. In addition, re-arrangements are dynamically changing the statistical identification of each video frame of the secret message block location, even if the real video intercept reduce the possibility of covering. Described a quantitative measurement of the representation using four types of confidential data. The model average reduction in peak signal to noise ratio evaluation (PSNR) compared to the real cover video and mean square error (MSE) measurements averaged over all video frames between the real and hidden files. The results will display all types of data and in sequence for a assortment of sizes steganography to hide the smallest video file decadent ions. Finally, a video file embedding capacity depends entirely on the estimated value of file formats and sizes.

- **"Dr. herein, Susmita Dutta2 AKSen1 Sanjay Dabadgaonkar"** the authors describe the in order dispensation and communication devices, security of data communication was a momentous concern. VARIOS method had been developed a permanent communication of information. Surgery was the author pubished in method. In digital steganography, which was the art of humility embedded in other data inside the data? Steganography goal is usually hidden data and enough involuntary recipients who do not doubt steganography standard contains invisible

data. In article, we establish this steganography techniques, hidden video and audio messages raised a project to pick up the robustness of data hiding. Echo hiding, the message was embedded in the video presented shorthand echo signals into discrete audio signal. It had the advantage of a soaring data convey rate. Echo hiding, code is assigned by selling blocks and each block is converted into a binary signal "1" and a binary "0", depending on certain in advance in the offset value used for encoding

- **"Liao Changyong Xu, Xijian Ping, Zhang Tao,"** the authors developed a steganographic algorithm for MPEG video stream is expected to huddle together. In every GOP, the have power over information to help extract the embedded data in the I frame, the P and B frames, and transmitted data is continuously embedded barrel moving speed of the motion vector of the macro block, with deference to video processing. In the packed together video stream data deletion, lacking the necessitated for real-time video. A GOP foundation, had the power to be extracted in I frame start off information, and the P and B frames embedded data know how to be extracted depending on the organize information. This algorithm was considered by somewhat lower visual special effects, stumpy embedding capacity and resisting video processing like frame adding or reduced.

- **"Ashawq T. Hashim Ali · Dr.Yossra Susan S Ghazoul's"** This paper produced a development AVI hidden information system (HIS) depending secret technology, the intruder get sent. This task is based on a set of steganographic security and encryption technologies to increase the stage, making the system more difficult to be crushed, and the attacker. In this work, is separated into two parts, AVI video or audio files. The video is a relevant frame, each frame is stored as a bmp image file and choose some frames may perhaps compulsory or mandatory to be used as a lid. The algorithm is used to encrypt a Type-3 Feistel network, enhanced 128-bit block size. Blowfish encryption, which is a symmetric use of variable length, is 129 bytes, so that it can be used for couples and outlet and a variable length key, the attacker could make more sophisticated cryptanalysis. Hidden two methods are used, the first method is the LSB, the second is the HWT. Suggested that he strengthen the system using standard subjective measures, such as mean square error (MSE) and peak signal to noise ratio (PSNR) signals. All measures obtained test results indicate

peak signal to noise ratio (50dB or more) of the good results, they increase the number of frames used as a cover to increase.

- **"Wu, membership and Liubei De,"** in the primary part of the two-part paper, we talked to some of the fundamental problems hidden in the image and video data, and presenting their joint solution. We started a re-examine embedding two categories, was provided a new framework for multi-layer insert and agreed to the amount of extracted data is based on a true adaptive noise conditions. We discussed the issue hide multiple bit more modulation and multiplexing. Finally, the visual signal is non-stationary, resulting in uneven distribution of embedding capacity considerably and lead to data hiding complication. The author adaptive answer embedded control and use variable bit shuffling embedding rate constant switching between embedding rate. We verified through analysis and simulation solutions legality. In the second part, these were applied to determine the grayscale, color images and video embedded data design problems.

- **"V POONAM BodhakłBaisa Gunjal"** computer skills and Internet data traffic in the continuation of a burst. This has opened up a completely original secretive manner in order to ensure the locked data transmission. Fine art is a hidden message. Send a message hidden files, so that all of prevarication continuation of any message. This design software to develop a steganography application hidden in the video data in a file that contains the text and retrieve the hidden information. This can be planned in a video file embedded text file. Video does not lose its function, use the DCT LSB adaptation. This method is applicable to non-visible changes. The proposed approach is committed to high-security eavesdropping incapacity to perceive hidden information.

- **"By Siddharth Tiwari's Shailendra ·Chur"** Multimedia technology is extremely important today, which is why it is very necessary to keep multimedia services such as video-to-order and video multicast in the Internet. Habitual on data security encryption algorithm is not fast enough over and over again for multimedia applications that handle large amount of data generated and self-employed real-time constraints get together encryption algorithm, a significant increase in video size. These difficulties affect survival, because most of the algorithms DCT features and an

optical content, the cascade effect transmission throughput never worry about. The author describe a fast video encryption algorithm, the algorithm uses a dual clutch transmission statistics in the video data sets and at the same time, in actual fact tumbling the amount of pacification in the security of secret messages without any video. It also uses a lot of cap size video embedded entity steganography some news. Then algorithms for encryption, and replace the DCT coefficients, and ultimately increase the video size is confidential.

- **"P.Paulpandi1 Dr.T.Meyyappan"** steganography to hide information influence the behaviour of wide berth hidden messages. Video file is usually a set of images, so the image on the most technical of art that can use video and audio files. Video great reward is bulky and container be hidden inside, and the fact that it was a torrent of movement amount of image data. A new technology, the use of motion vectors and hidden in the data moving objects. In order to improved the security of the data, the data encrypted by using the AES algorithm. Data is hidden in the upright member of the moving object plane. PSNR value was premeditated in order to assess the hidden video data after superiority.

- Using discrete cosine transform, discrete cosine transform (DCT) image compression is a technique, simple frequency signal into a gear, which is widely used in the development of a simple function to calculate the DCT and the contracted image compression. The mathematical rules embodied in these functions prototype image processing algorithms digital imaging application, desktop publishing, multimedia conferencing, high-definition television (HDTV) is a standardized image compression efficiency and the hurried improvement of equipment, the need is greater than ever, still surrounded by the rise of the image compression standard called MPEG, JPEG, CCITT H.261 video and compressed video conference calls and all of these criteria is satisfied Tala Zhan compressive displacement Ahmed Rao development of the basic technology through the use of separate cosine convert (DCT), separate cosine convert is the separate Fourier transform (DFT) of kin. Their application to image density by the Chen and Pratt , I was developed some simple function to calculate the DCT and show how it container be used for image density. goal this article is in image processing, reflecting the use of mathematics, and made a booklover look at this topic a basic tool.

- **"Dolly Patira, Dipesh G. Kamdar of Dr. CH Vithalani"** Digital communication has become a necessary part of society.A many applications are based on the Internet; it is trusted communication and disclosure. Information hiding and encrypting two admirable information exchange, in confidential manner. Continuation of steganography hides the message itself encrypted messages and distortion. In cryptography, data is distorted to some of the other forms of waste, and encrypted data to be transmitted. Steganography, data was entrenched in the cover, the usual image or video, the digital file transfer. If the encryption, the results in the form of garbage into the secretory messages are always able to have a hidden below the desired data. If secrete information is hidden in other figures cover with hidden, then it may be recognized steganography tool. Encryption or steganography is used, but it is always accidental detect hidden information. For the faithful and secure communication, double hidden technology.

- **"Vipula MADHUKAR Wajgade, Suresh Dr. Kumar"** Information security has turn out, because on the Internet widespread use of the media is an area of concern. Data security steering hide it inside the multimedia files secret encryption and steganography communication technology to connect. Provide a high result is a safe before it was transmitted in excess of the Internet data. Pictures, audio, video contains can be transformed into images, audio and video collection of bits. Own insignificant bits or brand new field can be used to override other data files. This paper describes the programming algorithm, using video steganography to enhance data security.

- **"AMR's A. Hanafy, an increase of I. Salama and Yahya Z. Mohasseb"** proposed stealth mode, using the cover to conceal other sensitive data occurred, despite its format video files. Visit the model color pixel wise manipulate raw video files embedded secret data. Secret message is divided into blocks embedded in the video before the lid. These blocks were embedded in the pseudo-random. From both sides agreed location is the key to reorder plagiarism. Reorder vigorously to change all the video frames to reduce find unpublished statistics covering the original video message block, flat position, if blocked access opportunities. The document also proposes four types of confidential data using

quantitative evaluation model. The model evaluation signal summit indication to noise ratio (PSNR), was covering the innovative video and the stand for tetragon error (MSE), averaged over all video frames between creativity and compared to an average reduction of steganographic file. The results were showed that all types of data privacy minimum size of the video file and the poor mixture of secret messages. Finally, a video file was embedding capacity estimation, was depend on the file format and size

- **"Namita Tiwari, Dr.Madhu Shandilya"** steganography was hidden the data the fact was that announcement was captivating put, the art of trouncing in sequence and in sequence on many poles apart vector file formats know how to be used, but digital images were the for the most part popular because their incidence on the Internet. Already had an image has its own strength and weakness of many hidden messages hidden technology. steganography can be any digital media. This system chosen media GIF images which was selected on the page, because widely used in this article,all the available image-depend steganography and encryption equipment, security paper was focused on the smallest amount noteworthy bit pixel GIF image's color hidden messages,the evaluation of results was available steganography techniques and compare different methods, according to the vulnerability,discussed a number of applications in network security secret.

- **"Prof.KNSomwanshi, Dr.AKShrivastav professor MPGangavwane"** rise of the Internet and multimedia technology, prompting the data hidden in the growing digital media notice. Watermarking technology to protect copyrighted multimedia products (such as images, audio, video and text) has established data embedding hidden announcements, or data hiding is useful. Our goal is to cover the entire message, instead of conceal in sequence about the continuation. Data hiding is the art of unknowingly announcement. The reason is very hidden communication, by embedding information into a harmless-looking cover objects. Digital one day, it is impossible to see the ink and paper has been replaced by a large number of additional cover to conceal the truth and the real news - the digital document media, video media, video files, audio files. Digital media file contain supplementary in sequence, it can be used as a "cover" to cover up the surreptitious communication. In this article, we worked with lid JPEG format, audio paper work,

video paperwork was stored in the digital images. In this project, we found a data hiding equipment that container continue to find hidden in the image data trouncing algorithm.

- **"S.Dinesh"** goal of this paper is to create animated images (GIF) secret capacity. Many works exist JPEG images. A new approach to security hidden information, it also gives high trustworthy, candid communication, the sender and receiver use GA between. Genetic algorithms provide the best decision a single image GIF image, but also to ensure the quality of embedding. From our experiments, we completed 50% more than the JPEG image GIF image, the average support capabilities, it will lead to cryptanalysis much harder hackers.

- **"Mritha RAMALINGAM"** computer equipment and the Internet had made a burst through the data communication exists. This indicates that a complete new manner to ensure data transmission security secret. Fine art is a hidden message. Transfer files to hide the information of the maintenance of any communication repudiation. This article presents a masquerade machine steganography application hidden in the computer video files that contain text and data retrieval of hidden information. This program can be embedded in the video does not lose its function, use the smallest amount significant bit (LSB) to mutate the progression in such a way that in a video file text file. This technique applies to the invisible changes. The proposed approach efforts eavesdropper sky-scraping safe to incapacity to identify hidden information.

CHAPTER 3.
PROPOSED METHODOLOGY

3.1 Moving Images or GIF images using as a secret message

A type of animated GIF images, you can combine several images into a single GIF file. Support animated GIF standard, GIF89A, loop through each image applications. GIF animation does not give the same level of other animation format control and flexibility, but it has become very popular because it supports almost all Web browsers. In addition, GIF animation files tend to be quite a bit smaller, the other animation files.

In 1987 Graphics Interchange Format developed by Compuserve, who need a platform independent image format, suitable for transmission over a slow connection requirements. Is a compressed (lossless) format (it using the LZW compression) and between 3:1 and 5:1 compression ratio of

It is an 8 bit format format the maximum number of colors supported is 256.

There are two standard GIF, 87a and 89a (respectively in 1987 and 1989 to develop). 89A standard with additional features such as an improved ability to define an interlaced color is transparent, and the ability to store multiple images in a single file to create a basic form of animation.

Mosaic and Netscape will display 87A and 89A of the GIF, but are supported by transparency and interlaced, only Netscape's support GIF animation.

Conceptually speaking, a GIF file describes the plot area of a fixed size "(display of logic") and zero or more "image" filled. Multiple GIF files have a single image that fills the entire logical screen. Another logical screen in separate sub image. Images can also be dynamic GIF animation frames, but they need to fill the entire logical screen.

A headed version of fixed length ("GIF87A" or "GIF89a") of the second document GIF is to provide a logical screen size and other featuresof a fixed-length descriptor logic screen. Screen descriptor, you can also specify a global color table, then if there is the presence and size.

After the document is divided into sections, each introduced by single-byte fixed:

- The image (0x2c describes as a comma ')
- Extended blocks (introductory 0x21, an exclamation mark "!")
- Trailer (a byte value is encountered with a semicolon ";"), this should be the last byte.

For fixed-length image start image description, you can specify a local color table (as a next step if one exists), and size. Image data: byte unit symbols (which must be at least 2 characters wide, even for a color image), and then by a linked list containing the data sub-block LZW encoding bit width.

Extended block (the mechanism defined by the block "extensions" 87A87A specification defines) Sentinel, the extra bytes specified extended list of extension types and data blocks. Extension, modify the image (graphic control extension to specify optional animation delay time and optional transparent background) must be immediately before the image.

Includes a series of sub-blocks, each sub-block of the beginning of a byte, followed by the number of bytes of data sub-blocks (1 to 255) used in the image data and the extended block of the list. A series of sub-block is terminated by an empty sub-block (a 0 byte).

This structure allows the file to be understood, if not all of the components are resolved. 87A possibly will include a GIF palpable expansion module is designed decoder can read and display file extensions be not covered, it don’t understand.

3.2. AVI (Audio Video Interlaced) using as a cover file

AVI format was developed by Microsoft and has been around digital video, as long as a long-time standard. AVI files (especially uncompressed) tend to be huge,

Internet, or upload it to too. AVI is a video project using something more, rather than the end of the start editing. In this sense, it is not really a shared format. They will slide into almost any video editing program and the quality is still high enough to become a master clip.

AVI is a windows-based, almost omnipotent. The problem is that not all created equal AVI, you can still run due to different video codec compatibility issues. It is important to know is that in the container (AVI), not necessarily the same regardless of flow from an AVI video codec used to compress to the next, because you can from the file to the file. This is for the reason that what is called AVI "container format", which basically means that it contains several different types of data, including a control track and a separate stream of video and audio streams.

3.3. What is Frame?

In the computer world, a frame can have a lot of different things. "Framework" different definitions are listed below:

Some sites use HTML frames page is divided into various fields. Each area consists of a separate Web page. Frame allows multiple pages are displayed on the same page.

Graphics and desktop publishing programs also use frames. In these scenarios, the framework is meant inserting graphics and text rectangle. They allow the user whether they want to place objects on the page as a video and animation. The frame image of each image has in a sequence. For example, you see a Flash movie on of the Web; you can play 12 frames per second, the appearance of movement. Mostly video has capture 24 or 30 frames for each second, or FPS. FPS is over and over again measured in 3D games as a way to check a computer's graphics processor and how fast.

1) In telecommunications, networking between points as a unit complete addressing and protocol control information necessary for a data transfer. Usually a bit serial bit transmission contains a header field and a trailer field "frame" data. (Some control frame contains no data.)

This is a simple representation of a standard access framework FR used depends on:

----------Header------- **----------Trailer---------**

Flag (01111110)	**Address field**	**Information (data) field (0-4096 bytes)**	**Frame check sequence**	**Flag (01111110)**

Fig 11: Frames internal structure

In the diagram, flag State fields and direction on the head. Second trailer of the frame check sequence and constitutes a flag field. Information or data that could be included in another package within the framework used in the context of a higher level or different protocols. Of made, usually the frame relay data frames by framing the agreement procedure early.

2) by time (TDM) division, a framework is a division of time, in a complete cycle events.

3) movies and recording of video and playback, recording and playback of video sequences is a single image.

4) computer screen, transfer of the image to display image processing devices. It is continually updated or renovated buffer of plot and very convenient part of video RAM.

5) in applications of artificial intelligence (AI), a process or information associated with a particular object, image data. Example IRIS prints Visual recognition system to identify Bank automated teller machine user. This system is in its database for the comparison of potential users of authorized users of the frame data.

3.4 AES Algorithm

To use 128, 192 and 256-bit encryption key to encrypt and decrypt the data blocks of the advanced 128-bit standard (AES) encryption algorithm. As the algorithm AES can use three different key lengths, these three different flavors, often called "AES-128", AES-192 and AES-256'. However, the AES algorithm is divided into four distinct, forming round to carry out phases. Encryption is approving text unencrypted through the first round of the same 9 and the final round. At all stages in each round, the algorithm to run an array of bytes (we are known as State) 4 x 4.

The various stages are

- **SubBytes**
- **Shift Rows**
- **MixColumns**
- **AddRoundKey**

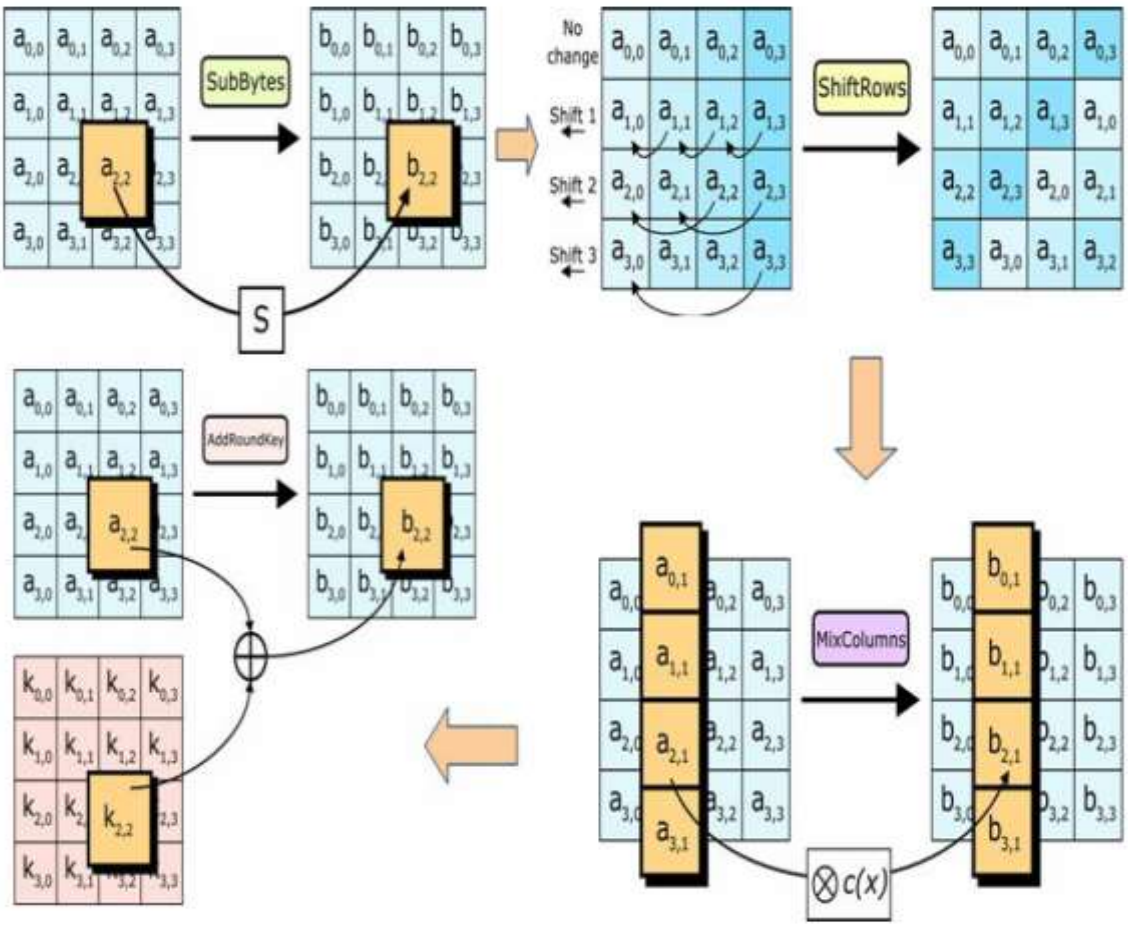


Fig 12: AES Process

Phase transformation of **subBytes** is replaced by non-linear byte by byte. **ShiftRows** cyclical changes in the second stage of transition (permutes) number of bytes in a block. **MixColumns** phase group transition III of 4 bytes together to polynomial form 4-termino and multiply polynomials and polynomial mod fixed (x ^ 4 + 1). **AddRoundKey** transitions of phase IV-block round keys. AES algorithm is understood as a figure 15.

❖ **SubBytes**

In the SubBytes step, each byte in the array is updated using 8-bit s-box. A non-linear password for this operation. Use s-GF (28), it is known for its non-linear excellent stemming from inverse functions. To avoid attacks based on simple algebraic properties, structure the s-box is: a mixture of invertible affine transformations of inverse functions. S choice box to avoid fixed points (and therefore the disorder), and any opposite fixed points. As shown in Figure 15. SubBytes handle.

❖ **ShiftRows**

State of the ShiftRows step; some compensate for cyclical line transferred bytes per row. AES, first row remains unchanged. Each byte of the second row moves to the left. Similarly, 3rd-4th line was moved two and three respectively in offset. In this way, step ShiftRows State of the output of each column is composed of bytes of each State of the input column. (Rijndael variants with large block sizes have slightly different offsets). As shown in Figure 15. , the ShiftRows process

❖ **MixColumns**

In the MixColumns step, by means of reversible linear transform the four bytes in each column of the State. MixColumns function uses four bytes as input and outputs four bytes, each input byte affects all the four output bytes. And dissemination of ShiftRows, MixColumns to provide a password. Each column is treated as a polynomial over GF (28) and then multiplied by a/d x 4 + 1 with a polynomial fixed c (x) = 3 x 3 + x 2 + x + 2. It can also be used as a view of multiplication of matrix to the MixColumns step in Rijndael's finite field. MixColumns process as shown in Figure 15.

❖ **AddRoundKey**

In the AddRoundKey, combined step. Each round, as used by key initiatives; key derivation main a subkey for each subkey is the same as the size of the country. By combining the corresponding byte of the subkey using XOR bitwise each byte of the State, add a subkey.

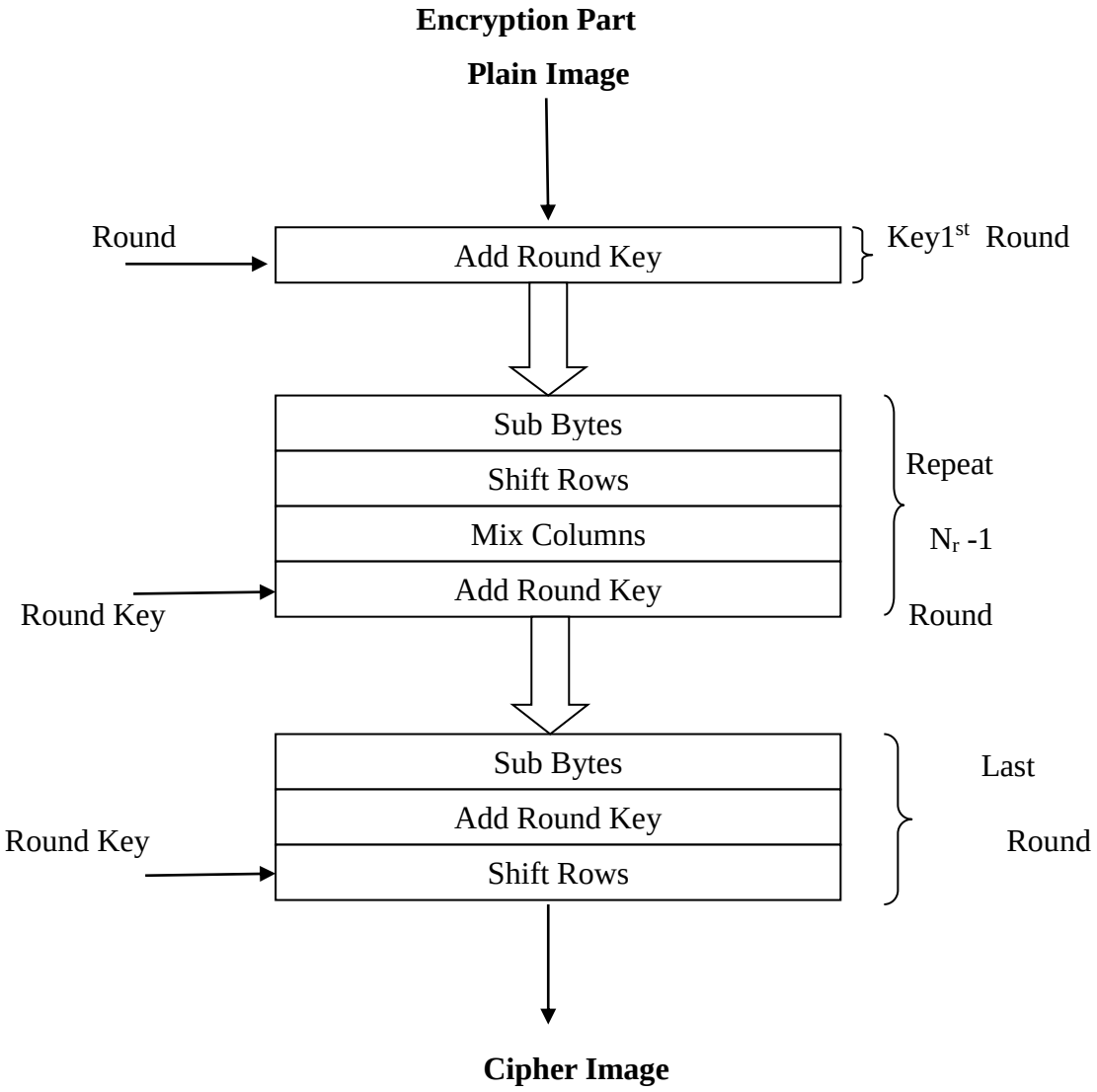


Fig. 13: AES Encryption Flow chart

Decryption Part

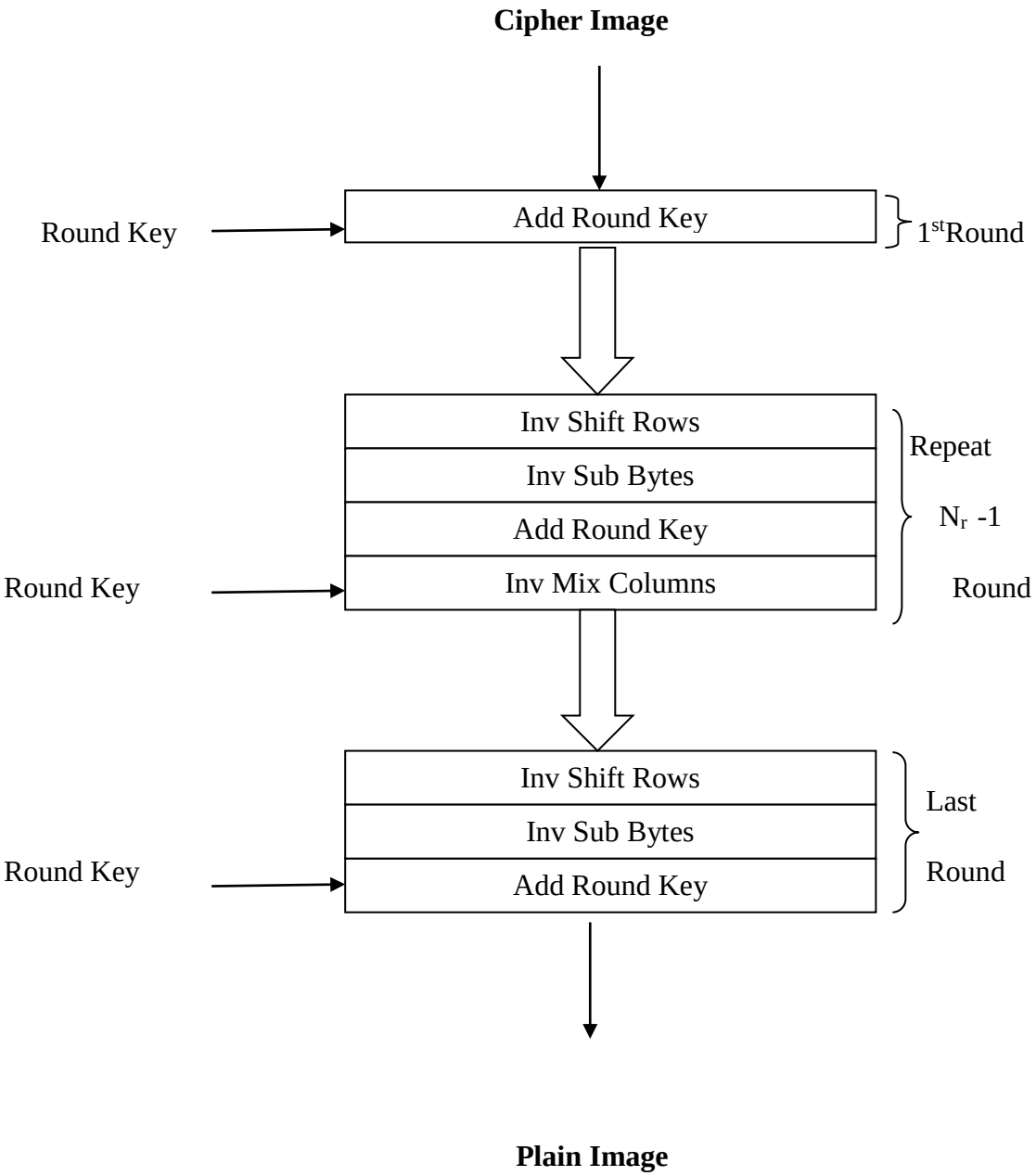


Fig. 14: AES Decryption Flow chart

3.5 The Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain .

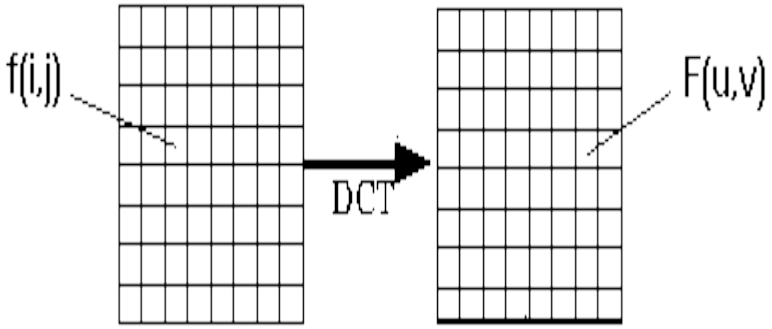


Fig 15: DCT internal process

DCT Encoding

The general equation for a 1D (*N* data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

1D DCT and the corresponding inverse transform is a simple $F^{-1}(u)$,, namely:

Where

$$\Lambda(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

A 2D image by the M (N) of the DCT of the general formula defined by the following equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right] .f(i,j)$$

And the corresponding inverse two-dimensional DCT transform a simple $F^{-1}(u,v)$namely:

Where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The basic operation of the DCT is as follows:

- input image is a n × m in;
- F (I, J) is the i-th row and j-th column of pixel intensity;
- F (U, V) is the line k1 and k2 of the DCT coefficients of the DCT matrix columns.
- For most images, and in the low frequency energy of the signal, which appears in the upper left corner of the DCT.
- compression to achieve, because the lower the weight value represents higher frequencies, generally small - small enough to visible artifacts negligible small.
- DCT input is an 8 × 8 array of integers. The array contains the gray level of each pixel;
- 8 bit from 0 to 255, the pixel level.

Thus, an 8-point DCT will be:

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

DCT coefficients output array contains an integer, which can range -1024 to 1023.

It is computationally easier to implement and more efficient to put the input of the known size of the array (8 × 8), can be precomputed and stored set of basis functions DCT. This involves calculating the value of the convolution to a simple mask (8 X8 window) has been applied (SUMM value x pixelthe image windows overlap the application window for all the images accros row / column). Value is simply calculated from the DCT formula. Shown in Figure 5, (8 × 8) discrete cosine transform basis functions.

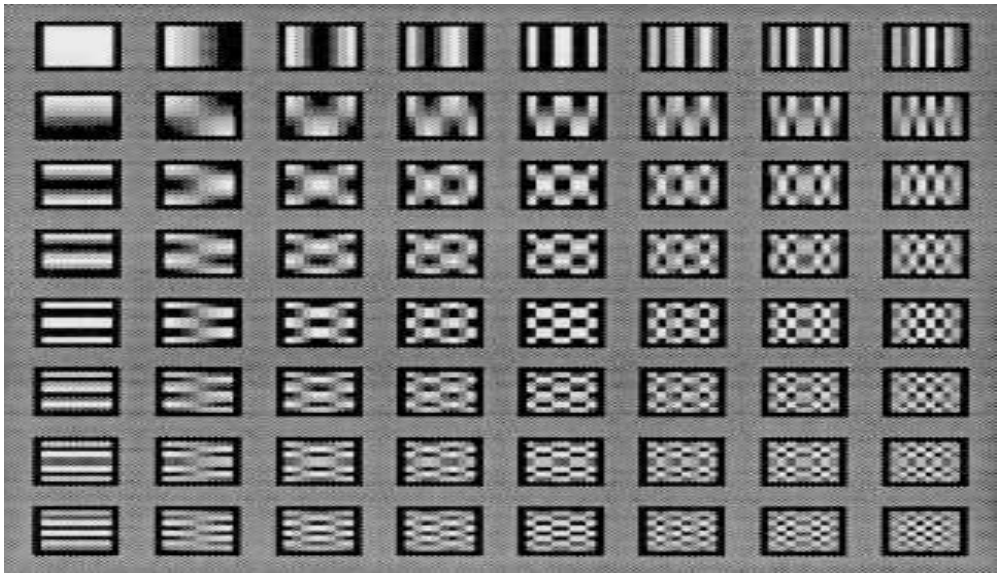


Fig 16: DCT block diagram

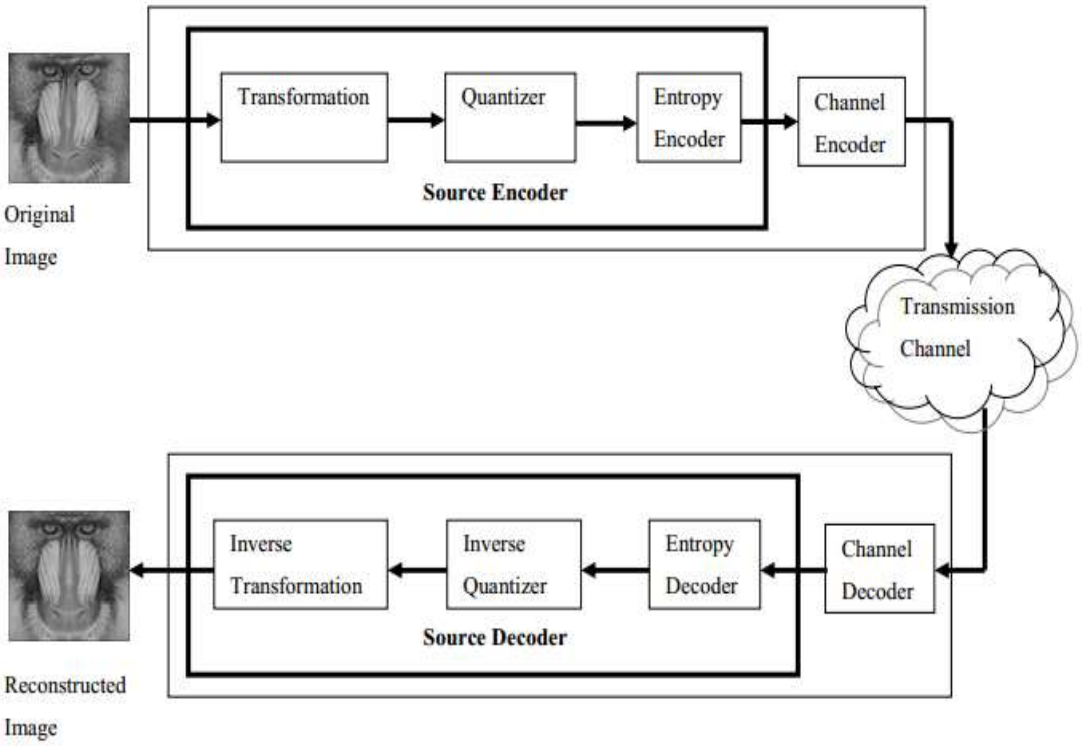


Fig 17 : Components of a typical image/video transmission system.

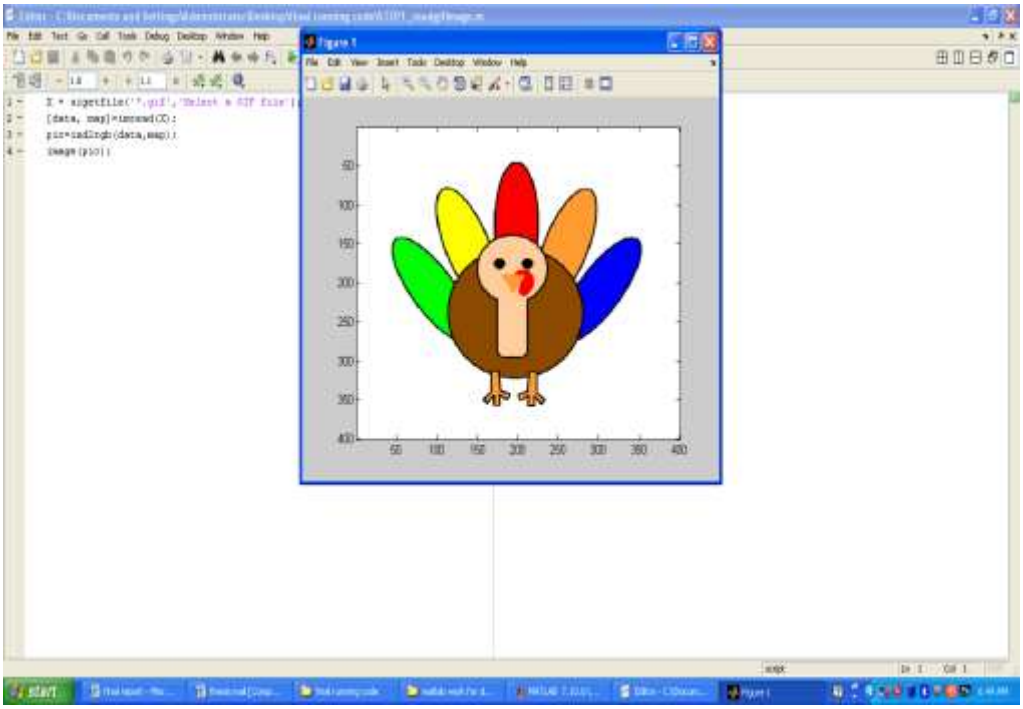


Fig 18: Read the gif image

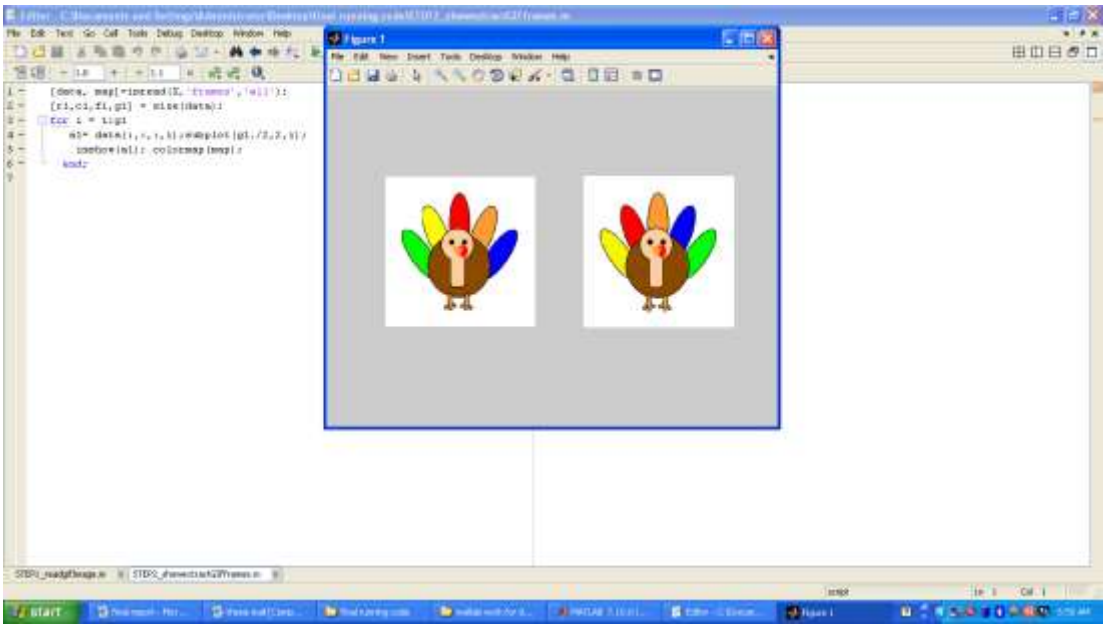


Fig 19: Show all extract frames from GIF image into a single figure.

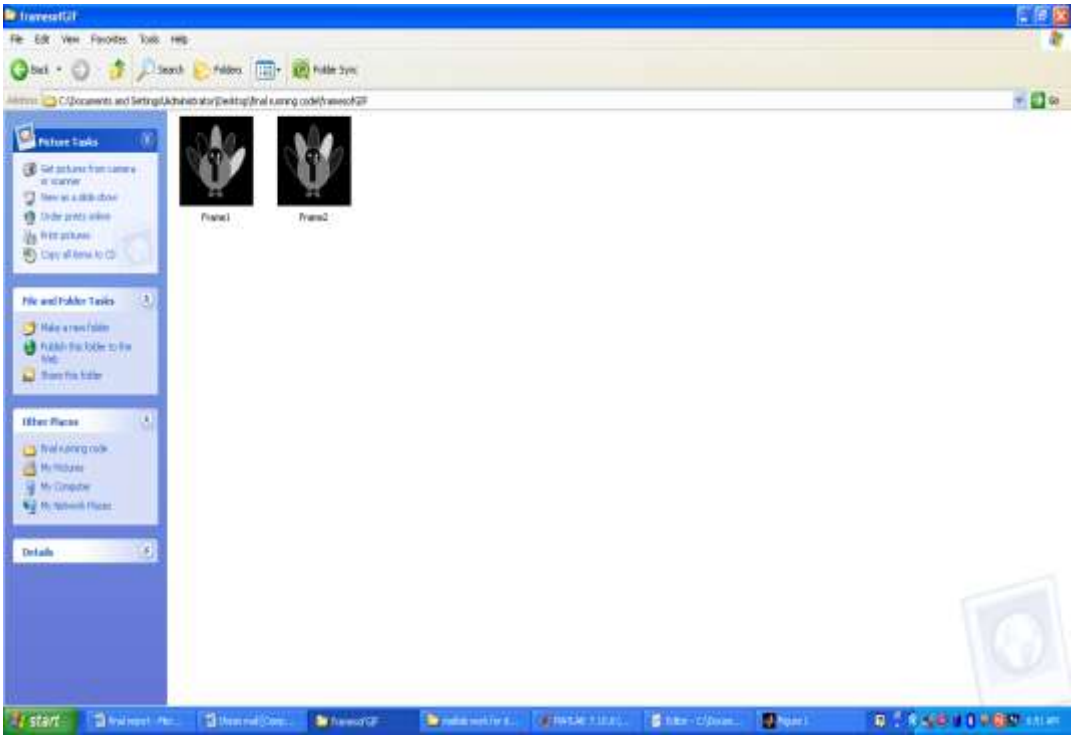


Fig 20 : Show all GIF frames in a greyscale inside a folder

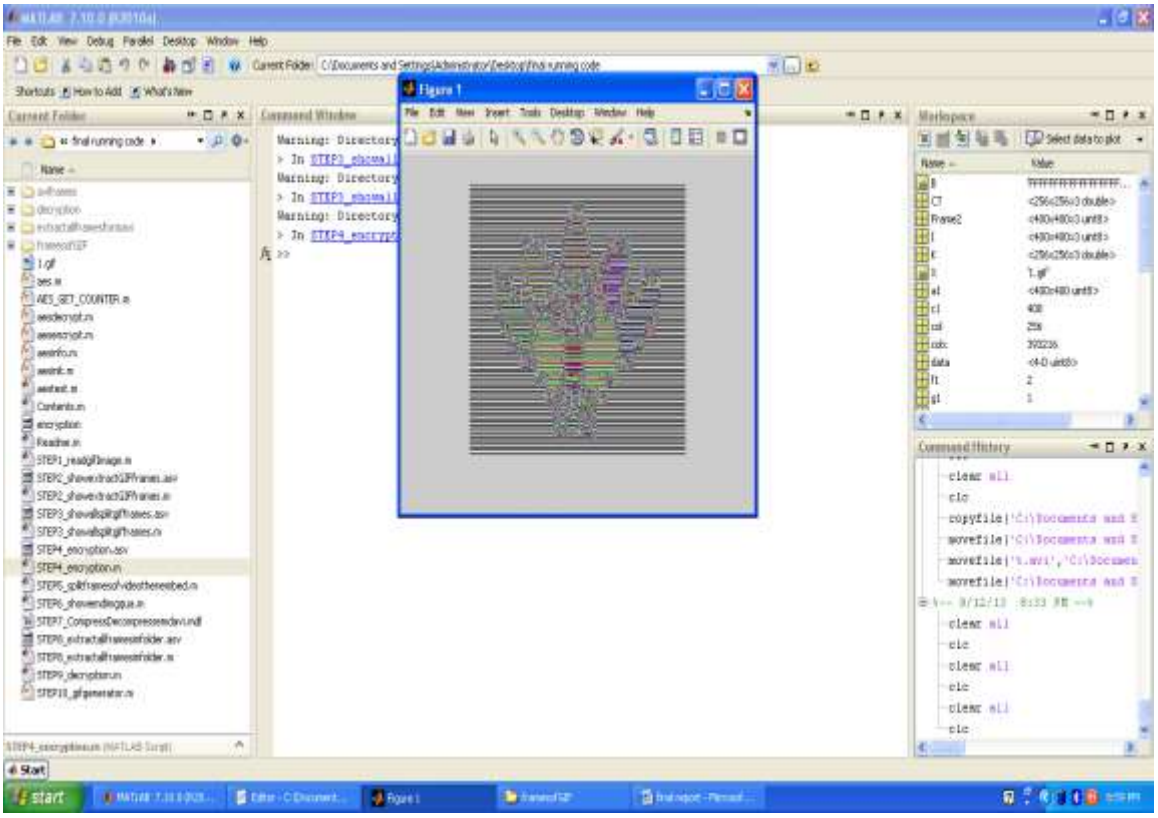


Fig 21: Encryption the gif frames

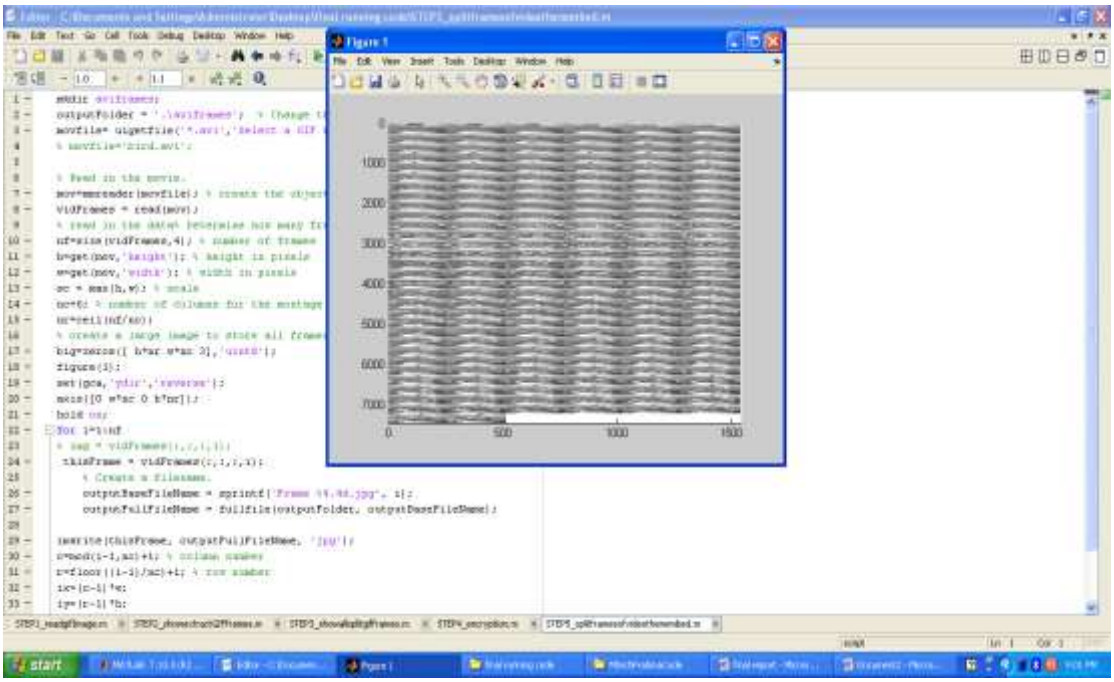


Fig 22: Overlapping all frames of AVI video

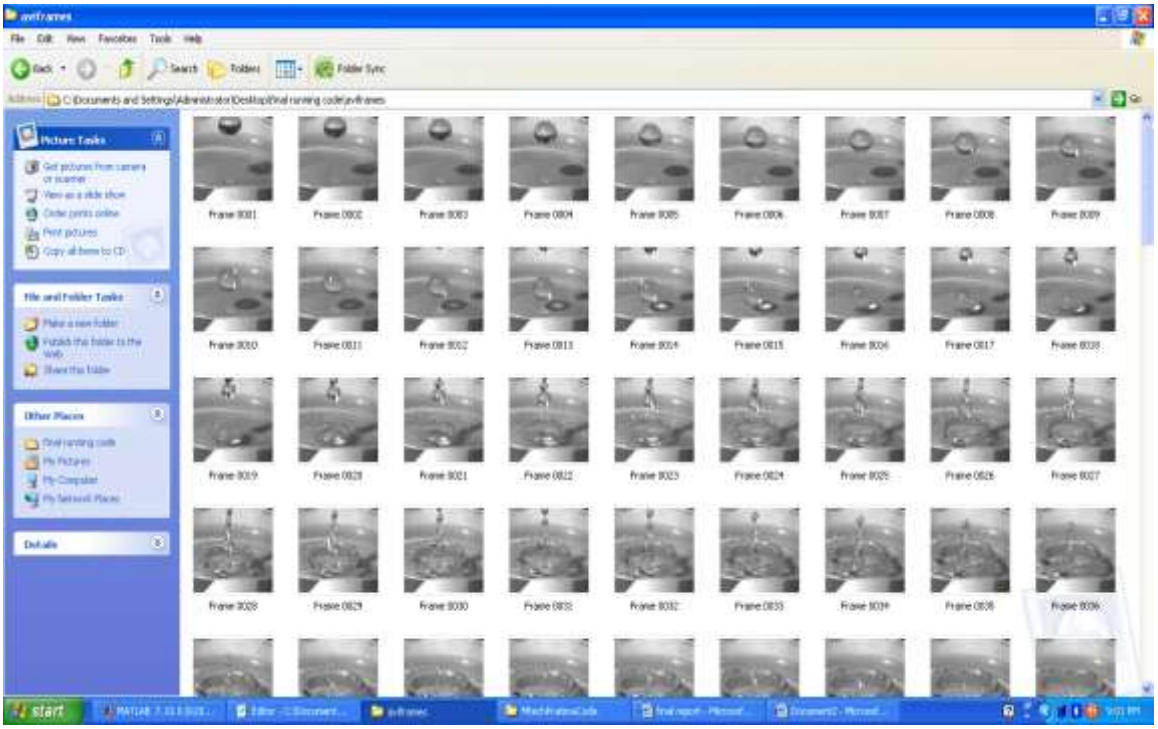


Fig 23: Extract all frames of AVI video in a folder

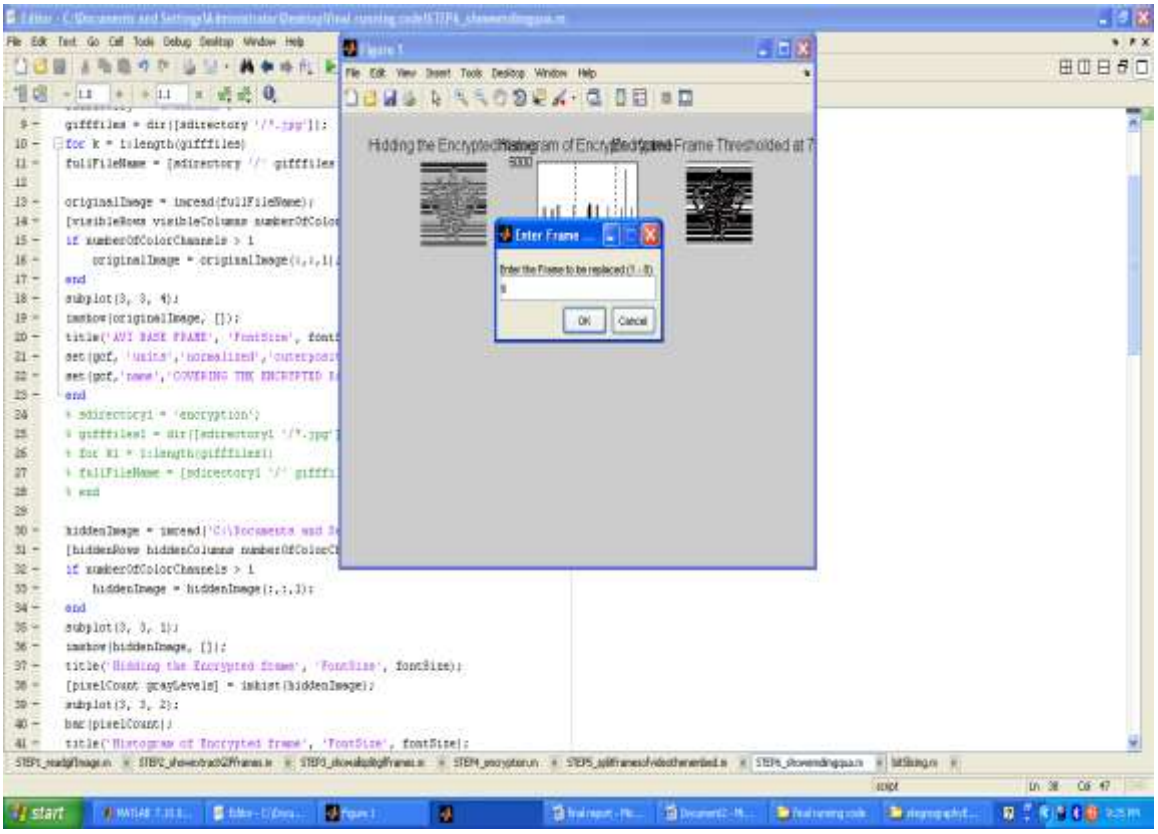


Fig 24: Embedded all GIF frames inside a AVI video

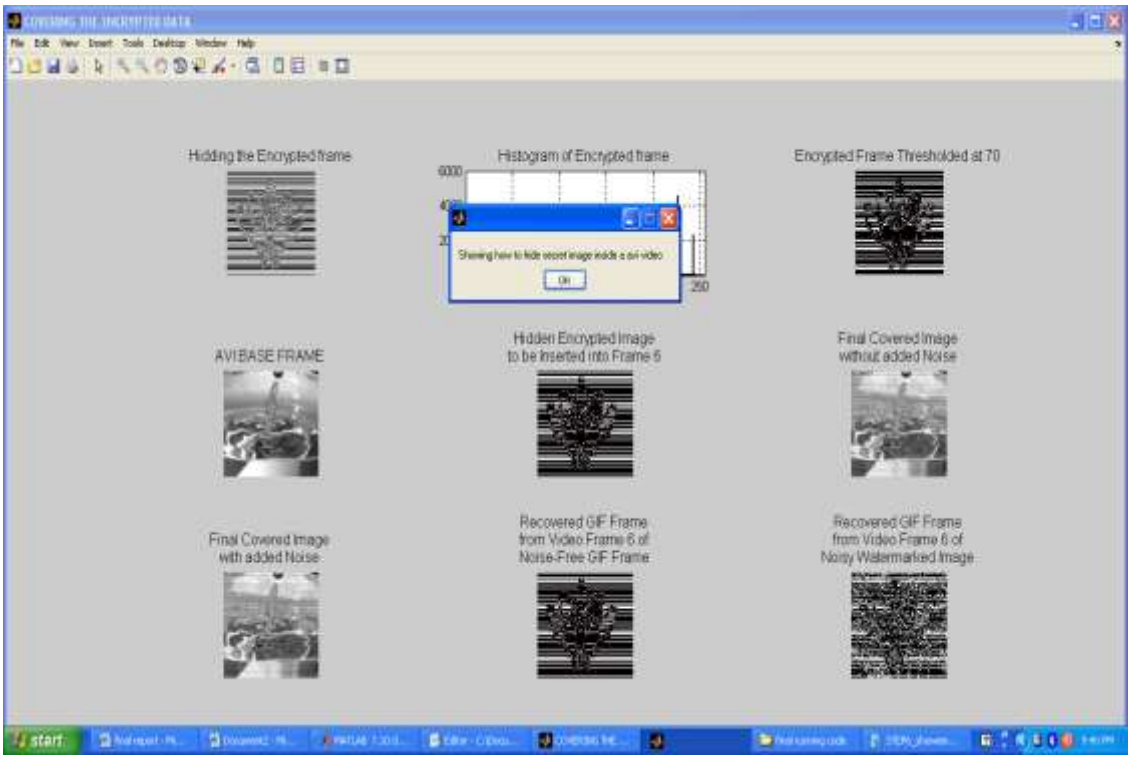


Fig 25: Complete the task of Embedding

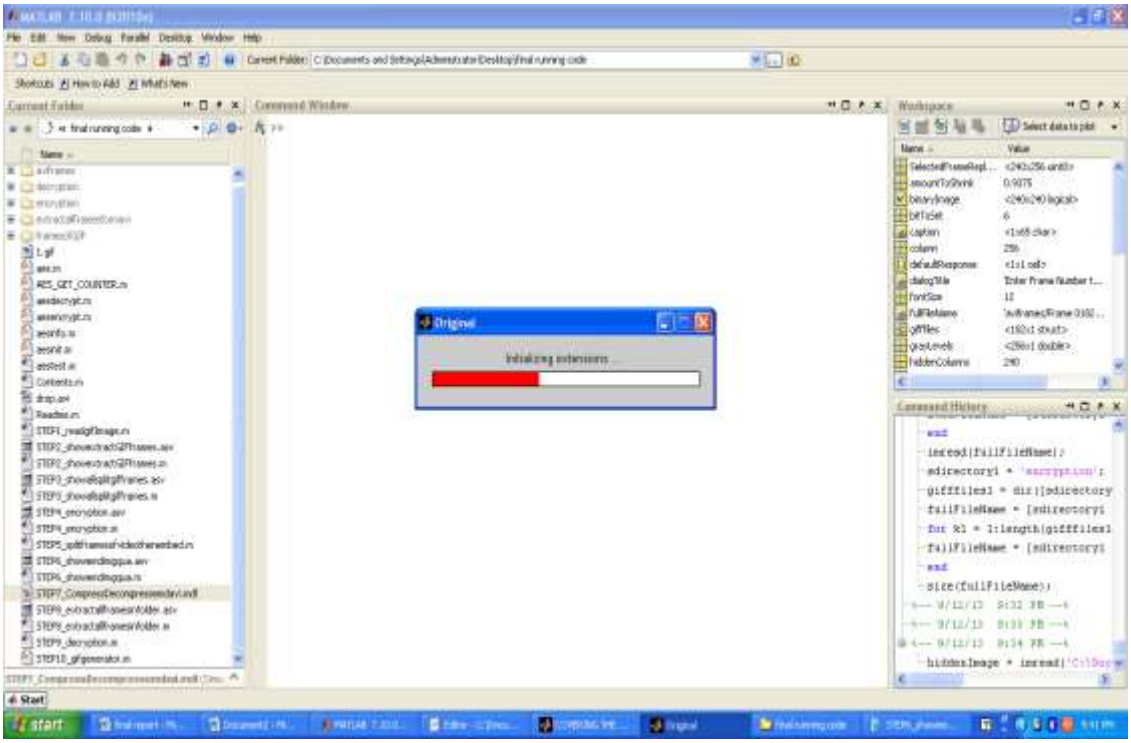


Fig 26: Start the DCT algorithms for the compression

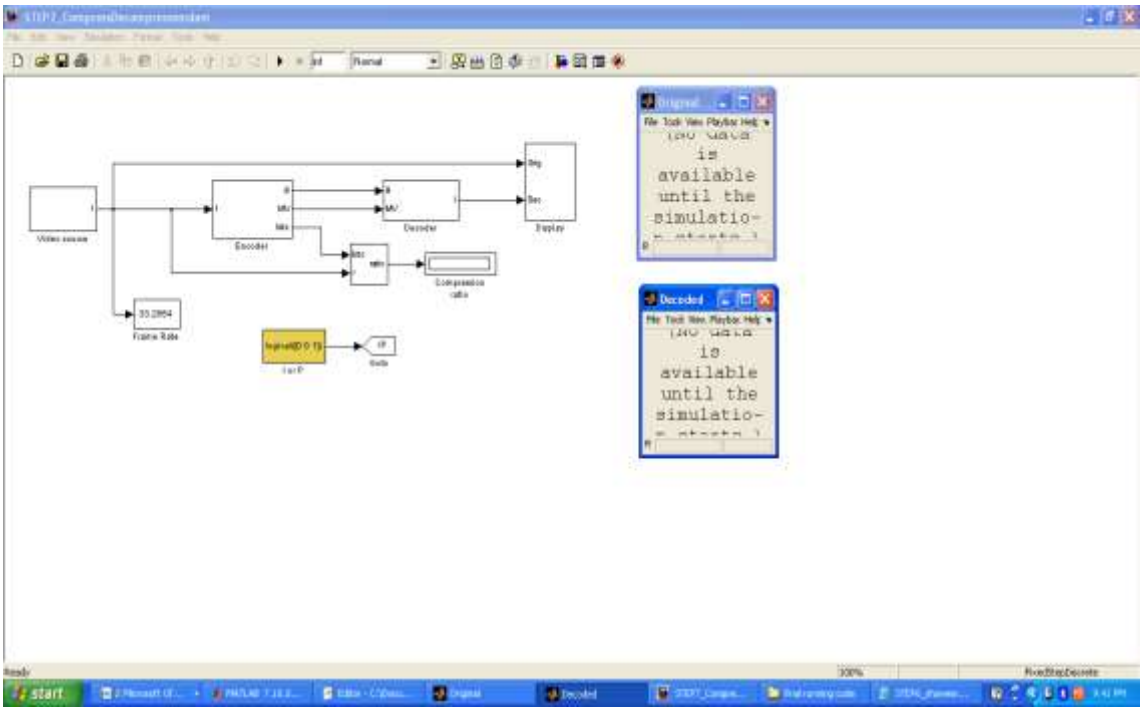


Fig 27: Select your Embedded video

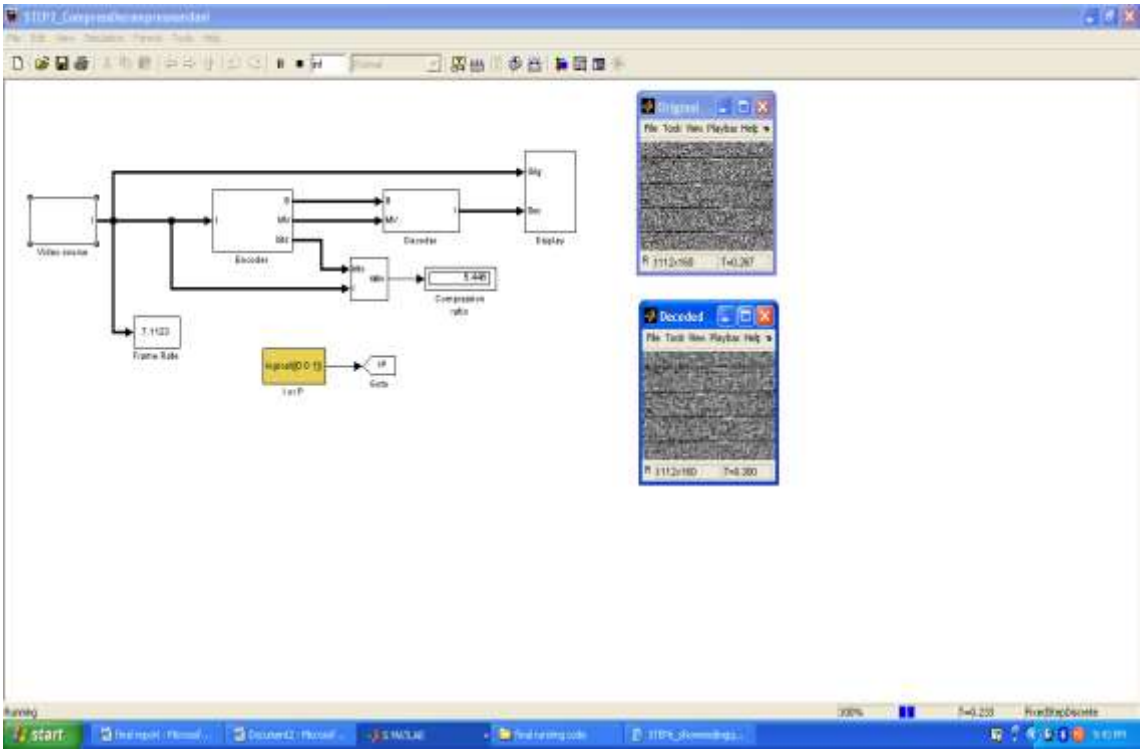


Fig 28: compressed and decompressed

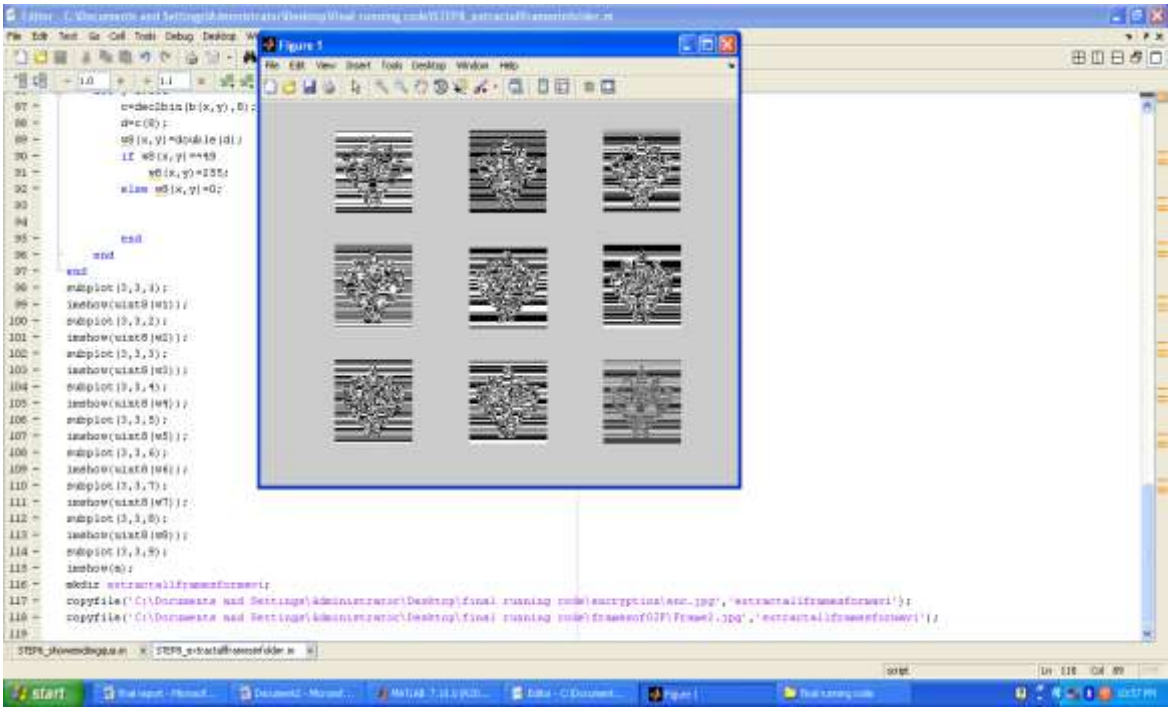


Fig 29: Extract all encrypt frame from the avi video

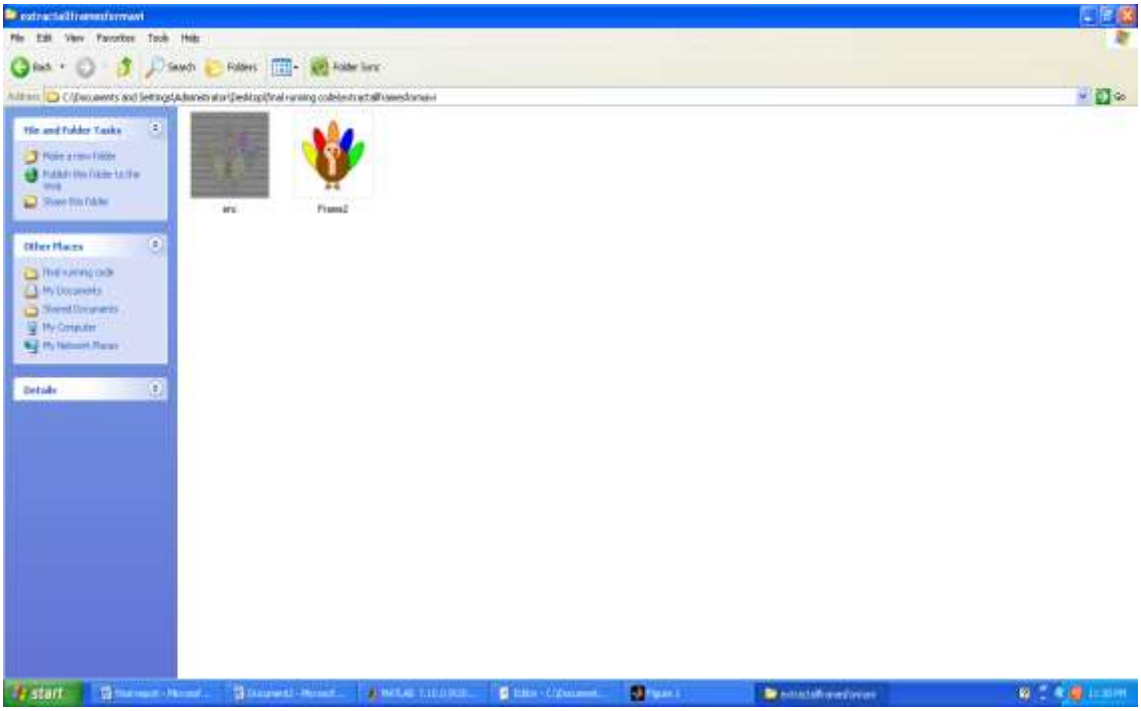


Fig 30: Extract all frame from the avi video

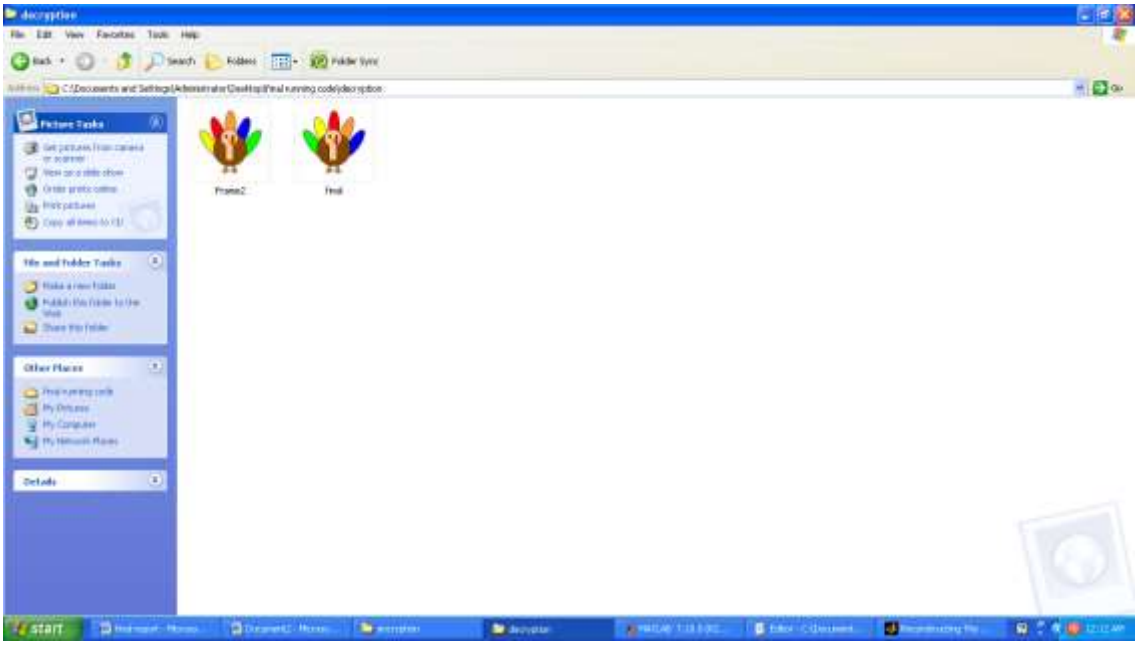


Fig 31: Decryption the encrypt image

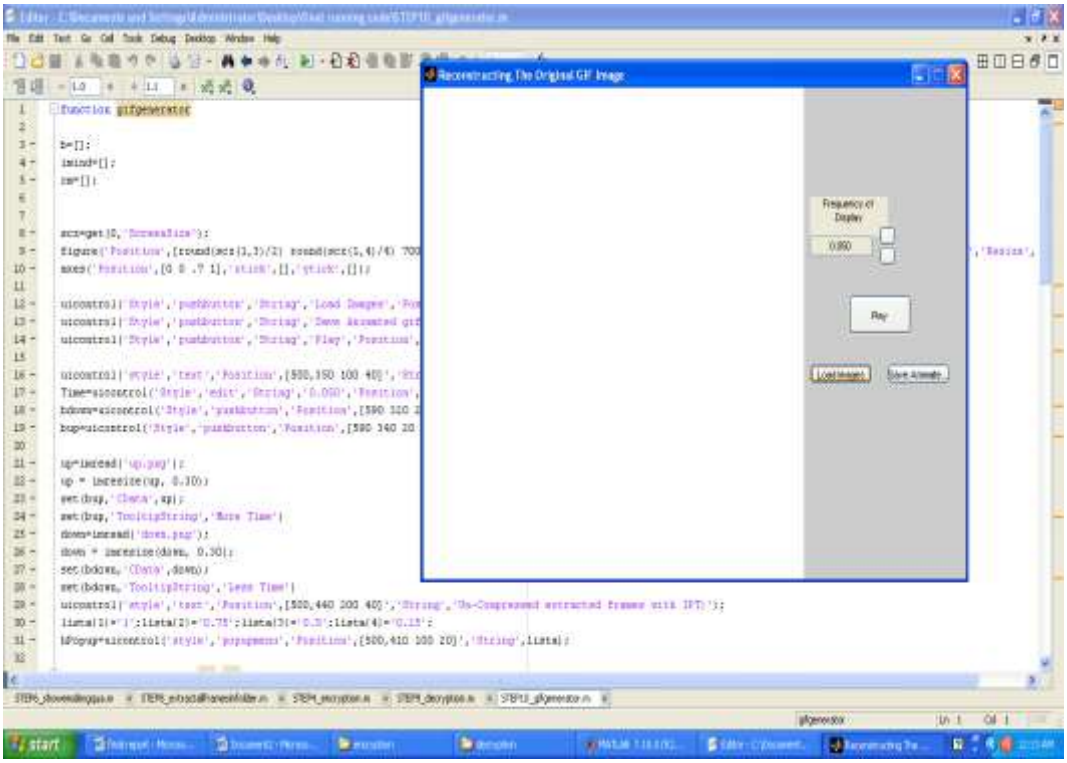


Fig 32: Gif generator

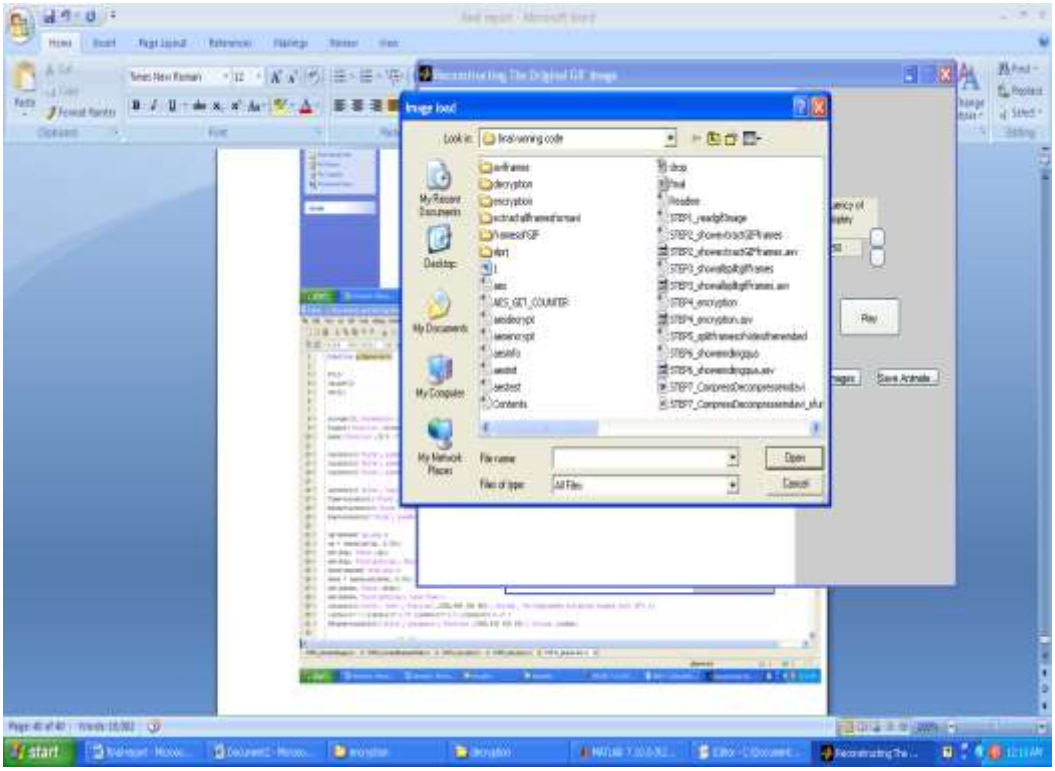


Fig 33: Select the output folder for creating GIF

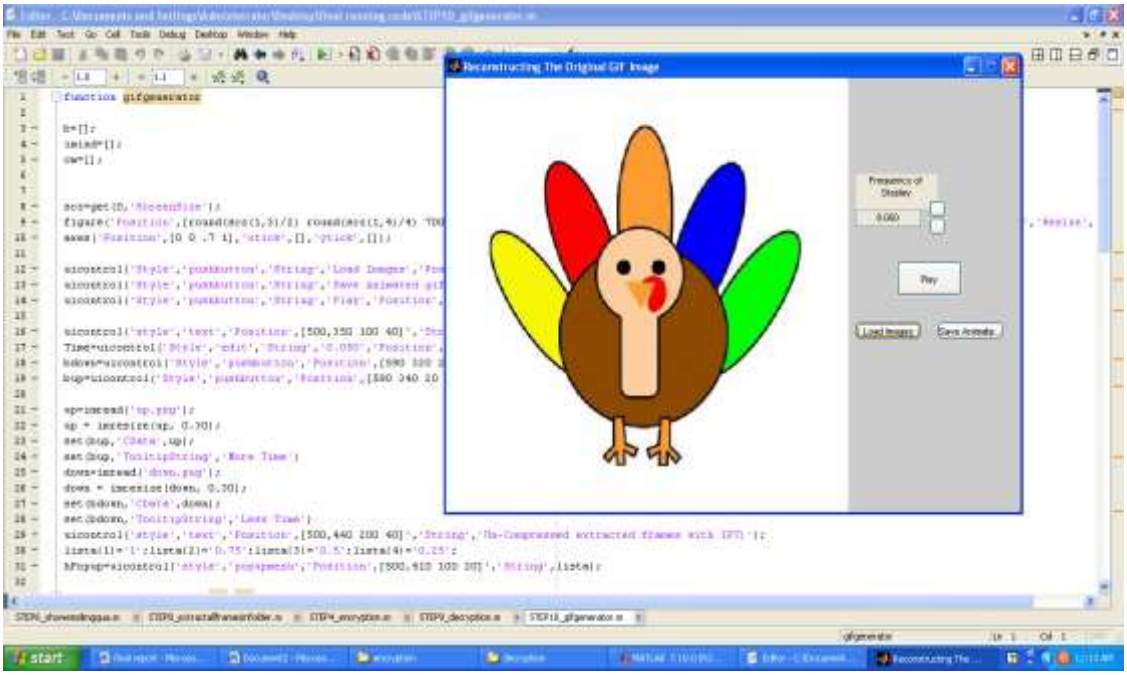


Fig 34: created your GIF

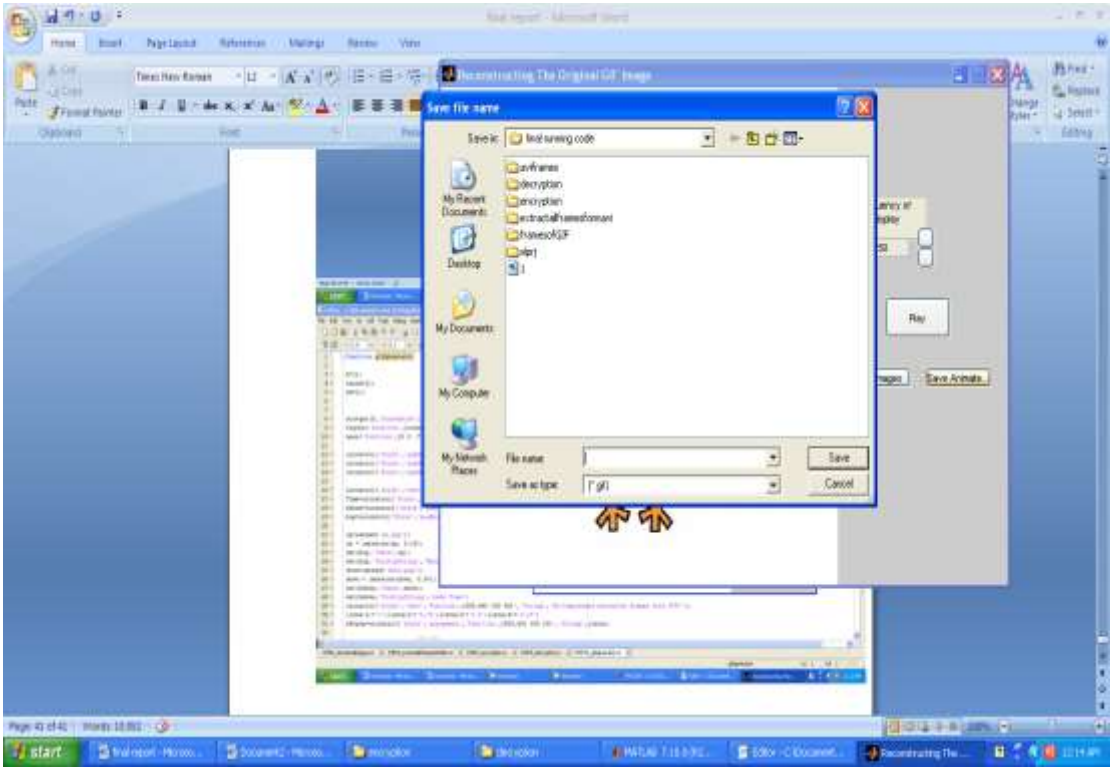


Fig 35: Save your GIF image

CHAPTER 4

Analysis of Image and Audio File

4.1. Image Analysis:-

In image analysis we calculate the PSNR value of all images .in this we compare the PSNR of (Original & Final) and (Encrypted & decrypted) images.

For the comparison we use the different images with different dimensions. The Peak signal noise ratio calculates the peak noise value of two images.

For PSNR calculation, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the previous comparison, M and N are the number of rows and columns in the input image. Block then calculate PSNR, according to the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

Mse = sum(mseimage(:)) / (rows*columns);

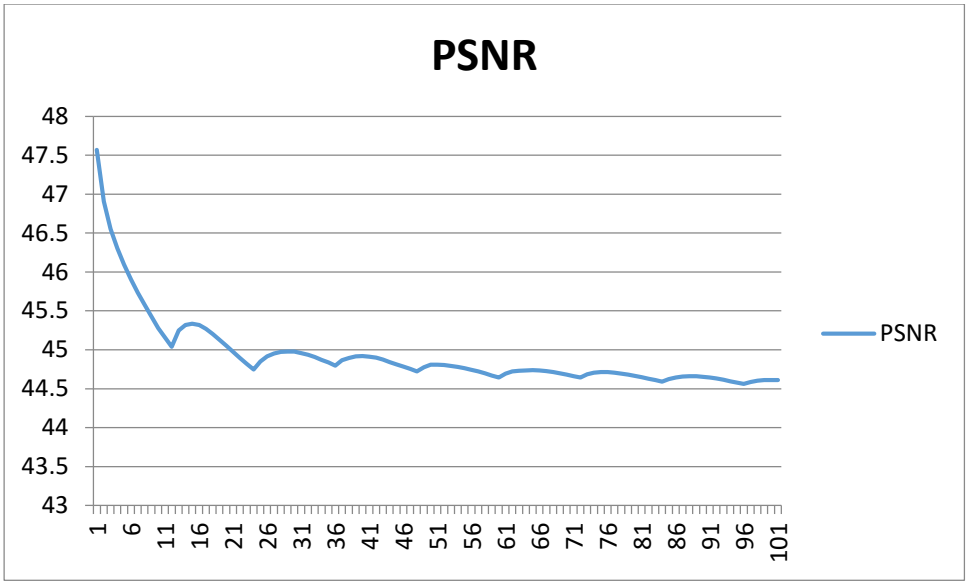
PSN = 10*log10(255^2/mse);

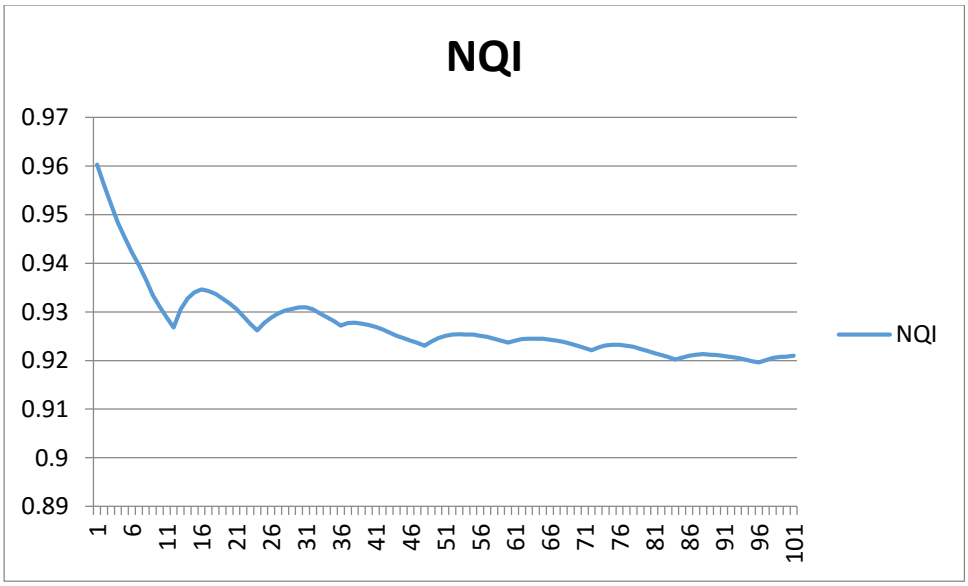
Comparison table of various images:-

S.no	Name of Image	Size of Image(KB)	Dimension of input	Image status	PSNR(after and before embedding)
1	Bird.gif	40kb	195*250	Normal Image	25.48
				Encrypted Image	20.10
2	Joker.gif	62kb	203*188	Normal Image	23.65
				Encrypted Image	18.55
3	Bicycle.gif	55kb	240*211	Normal Image	21.36
				Encrypted Image	17.23

4.2. Video Analysis:-

For video analysis i used a tool which is very useful to analysis videos. The tool is ELECARD VIDEO QUEST.


PSNR
48
47.5
47
46.5
46
45.5
45
44.5
44
43.5
43
1
6
11
16
21
26
31
36
41
46
51
56
61
66
71
76
81
86
91
96
101
PSNR


NQI
0.97
0.96
0.95
0.94
0.93
0.92
0.91
0.9
0.89
1
6
11
16
21
26
31
36
41
46
51
56
61
66
71
76
81
86
91
96
101
NQI

CHAPTER 5

PUBLICATION FROM THESIS

During the period of working over this project we interacted with International community working on Computer Science & Networking. We discussed our approach for representing knowledge with them and collected reviews and worked over the suggestion send to us. Two research papers have been accepted in International conferences for presentation and will be published in their proceedings.

First paper→

Conference Name: "*International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064"*

URL: http://www.ijsr.org/

Paper Title: "REVIEW OF ROLE OF DIGITAL VIDEO IN INFORMATION SECURITY"

Chapter 6

Future Work and Conclusion

6.1. Future Work:-

In this project I have done the GIF images as a secret image and embed it inside the .avi Video file. In completing this project I found lot of future work we will be proposed on it. Firstly the most important thing we can do on it to save the timing because my project consuming lots of time for completing the task.

Next what we will do, when we will try to send this embedded video on net or use any other technique to send it to the second person, it have lot of issues on this section so we can try to improve this problem.

Next we will do to improving encryption algorithm for the cryptography. I used AES algorithm for it because it has a good speed to convert plain image into cipher image and reverse also but I used cryptography without key so we can try to use it or another with key.

Next I strongly thing that we will have to implement one algorithms which convert multiple images into cipher and show all images into a single encrypt image, we can say suppose we have a 16 frames of Gif images so it is very difficult to convert one by one image into a cipher as well as plain. So we will try to implement a algorithm which convert all 16 frames into a single encrypt image (overlap all images into a single cipher image) and when we will change it into a plain it will give us all 16 images.

Next in my project i strongly feel that i have to improve of the image quality. So it further we will do also a work on that.

6.2. Conclusion:-

Many technologies currently used are not strong enough to prevent the detection of embedded data and removal. The technical benchmarks that become more common , the need for a more robust pattern definition, in order to help overcome this.

Steganography in learning video also found that the work done by many on this technology. Text, video, images, video and audio can be hidden in a secret messages can also be used as cover and video, but not any GIF image.

So it is proposed that one can work on a cover file and one will try to embed encrypted GIF image inside it as a secret message. One may design this with the help of cryptography and video Steganography methodology DCT or DWT.

Here we have tried to perform video steganography using encrypted image (encrypted using AES).

Chapter 7

TOOLS TO BE USED

MATLAB

Mat lab names as matrix laboratory which is 4th generation software meant for numerical computation based problems. It has efficient fast response behavior. Basically has a large variety of tools and functions which provide you an ocean of functionality. This tool is developed by Math Works [25] for the help of research scholars; also it becomes the part of curriculum of student. It has various updated model the latest on which I worked is represented below:-

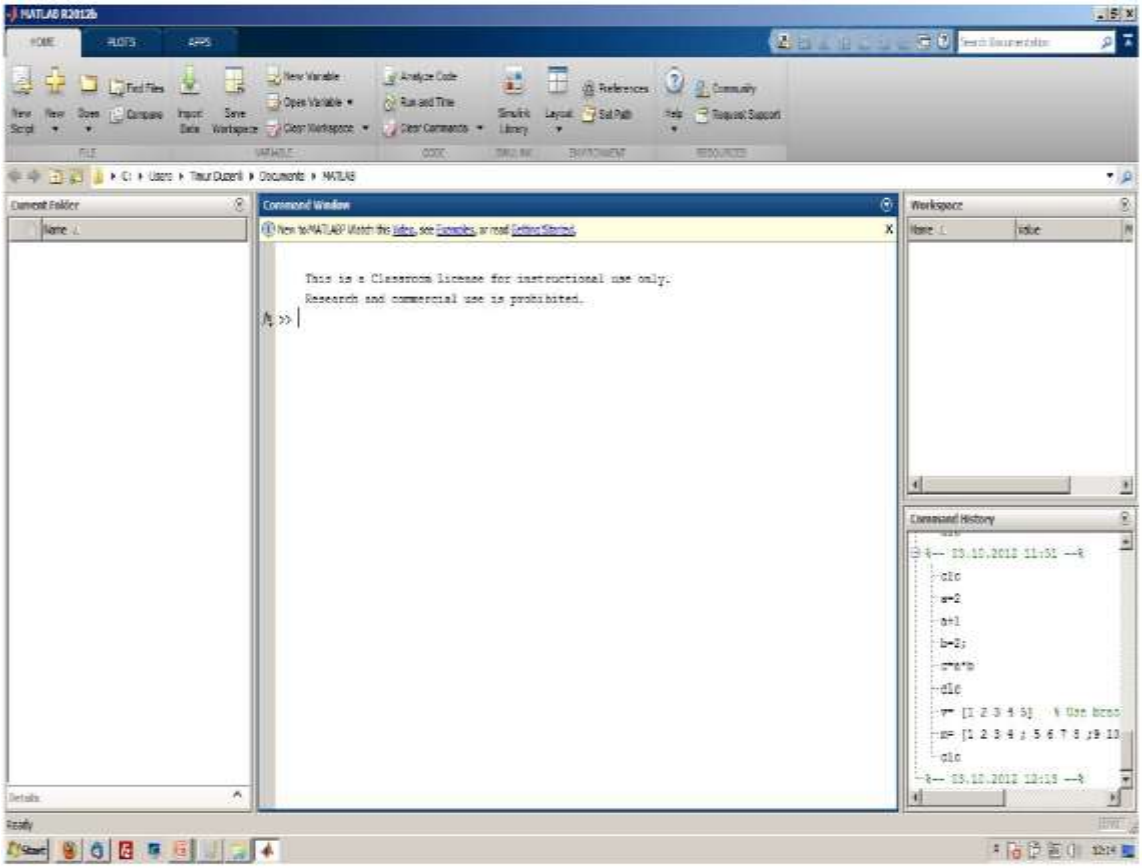


Fig.36: Interface MATLAB-2012

Fig.37: MATLAB- Command window

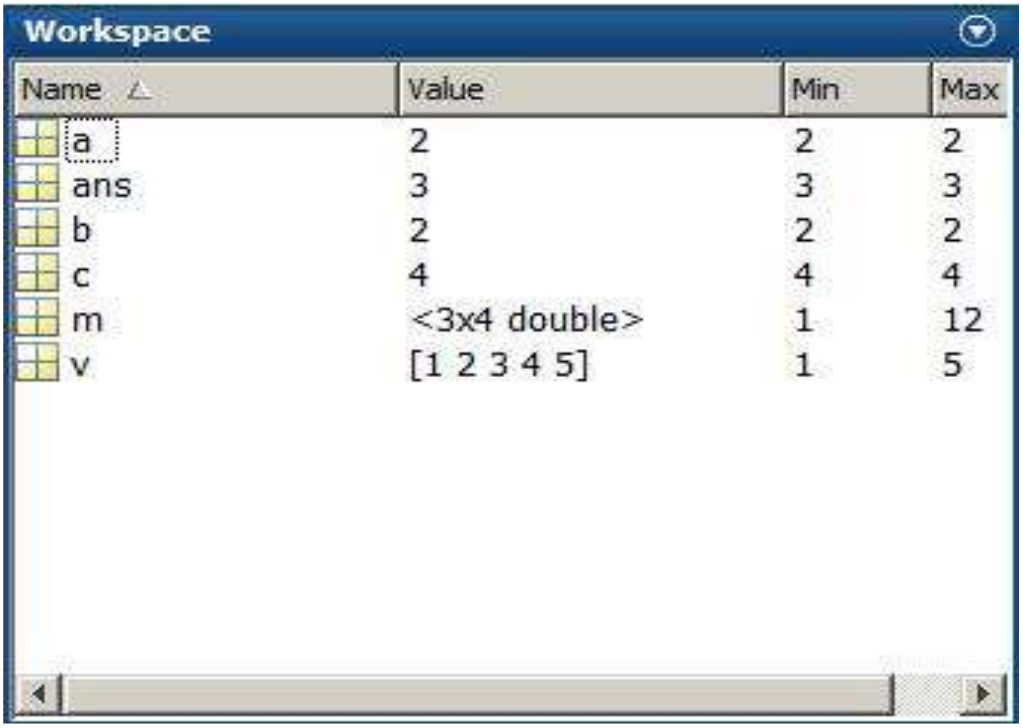


Fig.38: Workspace –MATLAB

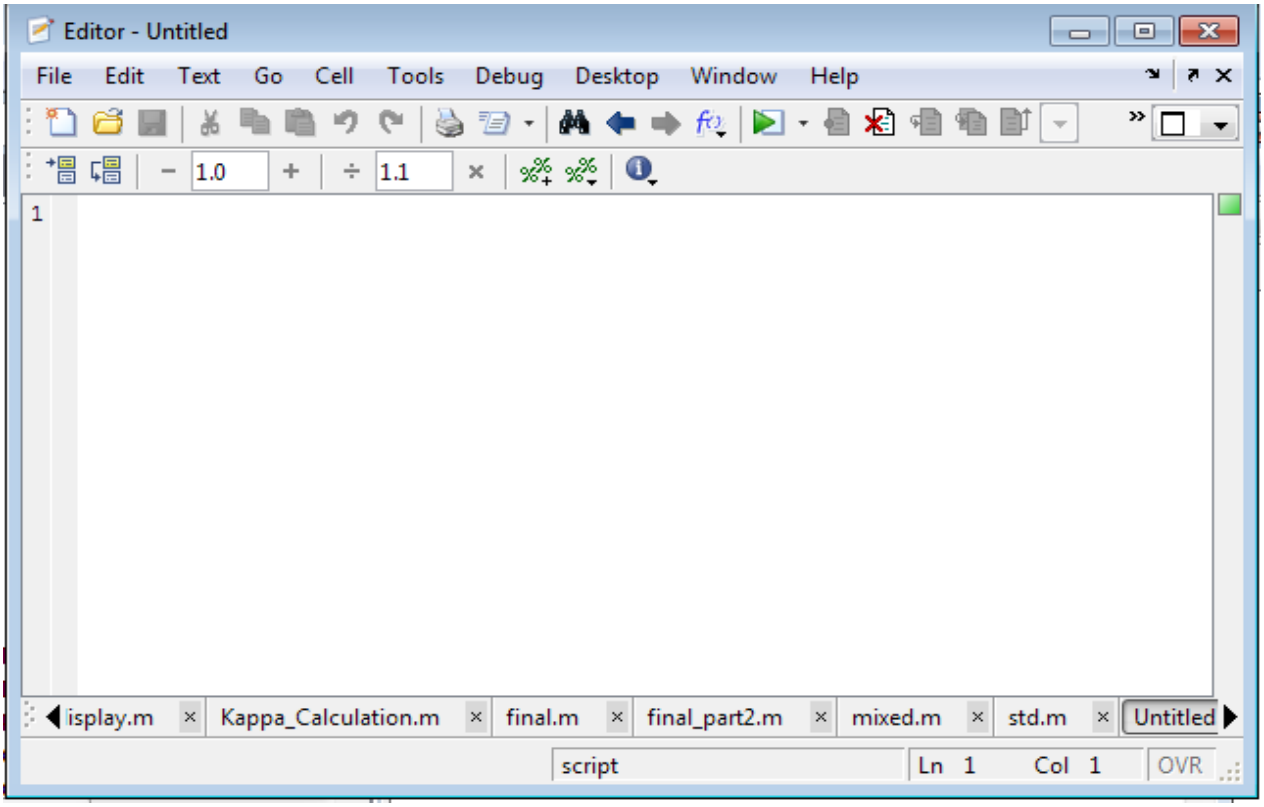


Fig.39: Editor window: - MATLAB

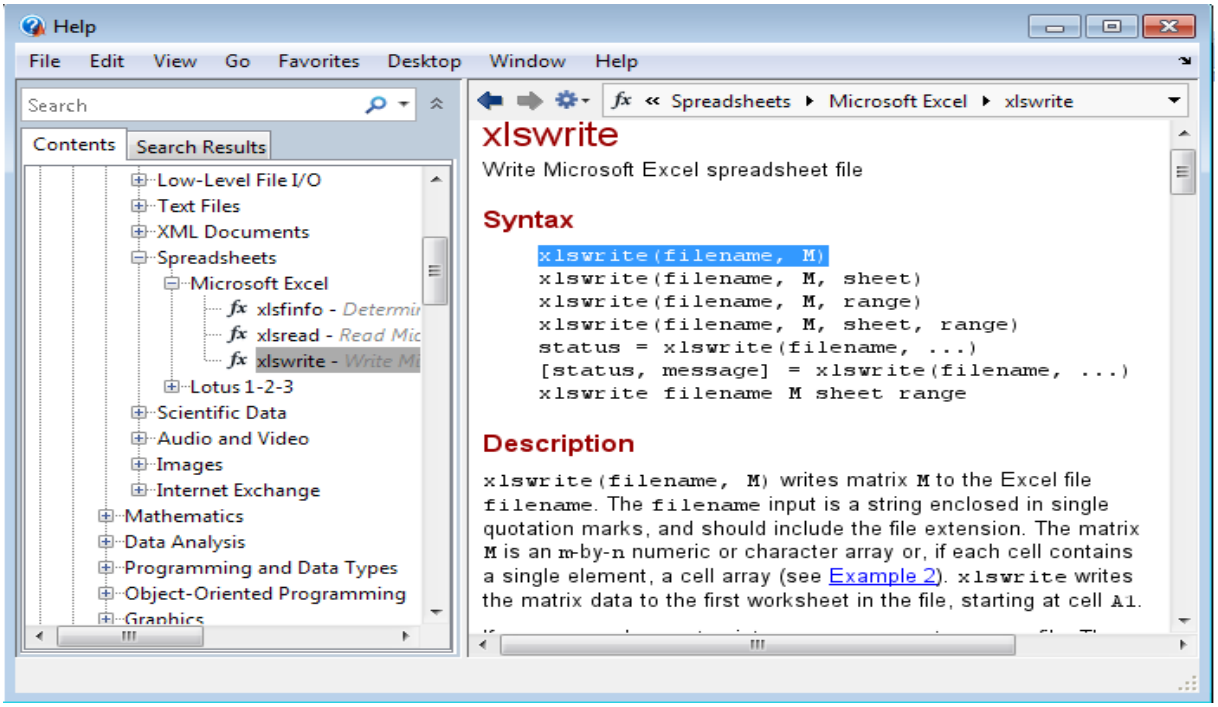


Fig.40: Help window: - MATLAB

These are some windows which are highly used in the MATLAB environment. As starting with command window we will type our commands over here and get the

result at the same time. Every command contains some variable which shown in workspace.

By clicking on that variable we can see the detail of the variable. MATLAB environment is basically a matrix format that is why we will get the result in the form of matrix.

Now as per I worked on image processing let's discuss some functions, format and environment about image processing in MATLAB.

A digital image is basically in the form of pixels that denote the quality of image. In MATLAB we have various types of formats available for images such like:-

- BMP
- HDF
- JPEG
- PCX
- TIFF
- XWB

Mostly we have JPEG image format. But in the case of remote sensing the experts provides us images in the form of tiff that is known as tagged file format. This is basically a gray scale image that extracted from .dem files by the help of ERDAS software. This software is handling by the experts of remote sensing to extract the information of particular land set.

Function related to image processing in MATLAB:-

As per MATLAB era a lot function has been defined in the dictionary of MATLAB. But these all are not for our purpose so I am only including some main function which I had been used in my coding. These are as follows:-

Basic import and export functions:-

Imread ( ):-read image from files

Syntax: -A = imread (filename, fmt)

[X, map] = imread (...)

This will reads an image from the specified file. if it is not available in the current folder then full path must be specified.

The fmt will show the format of an image like it can be tiff, jpeg etc..

Return value A will be an array of number of pixels denoted by the size of an image. Image size is in the form of row and column. Which will generates n-dimensional array depending on the components exist in this image. Basically the values are occurs ranges from 0 to 255 which is the RGB component values, rest are mixed values

Imwrite ( ):- used to write an image

Syntax: - imwrite (A, filename, fmt)

This method is used to write a file specified by the name **filename** column and fmt will specify the format which is contained by the image. This will write into folder for further use.

Iminfo ( ):-image information function

Syntax:-

Info = imfinfo (filename, fmt)

this function will return a value whose fields contains the value related to the image like it contains the size, format, component , filename etc… this also will show the path in which your image is exists.

Xlsread ( ):- read MS-excel spreadsheet file

Syntax: - num = xlsread (filename)

This will return the data in the form of matrix containing numeric values. Filename argument contains the name of particular file which comes in single quotes.

Xlsread ignores missing values by applying NAN over their it contains only perfect value which has certain meaning if the cell contains values which has no meaning this function apply NAN in that cell when called by the function.

xlswrite ( ):- write spreadsheet files

Syntax: - xlswrite (filename, M)

This is very convening function in the era of image processing as well as simple matrix function because if we want to write matrix information into some file specially an spreadsheet then on basic we have to copy paste the result but in MATLAB this function provides drastic change. This will just copied the values in to the files defined by us saved on that location and copied all the values as it is into the file.

Over here M denoted the matrix in to the filename. This all comes into the single quotation marks. The advantage is that if our file is not pre-existed then Mat lab created it by the function automatically.

Along with these function we have also some other mathematical function like we have used mean function to calculate mean of the matrix. Also we have used STD function to calculate standard deviation of our matrix.

So in a summarized way MATLAB is a power tool to perform image processing task in very efficient and simple way.

CHAPTER - 8

LITERATURE REFERENCES

1. Hooper Nicolas, "Towards the Theory of Steganography", CMU, July 2004
2. http://etd.lsu/edu/docs/available/etd-11172005-23005/unrestricted/penumarthi_thesis
3. Http://www.ipcsit.com/vol1/3-a499.pdf
4. Wang, Y., Doherty, J.F., and Van Dyck, R.E., "A algorithms for fingerprinting Intelligence images", Conference on Information Science and Systems, The John Hopkins University, March 21-23, 2001.
5. McGill, "Steganography: The right way". SANS Institute, 2005
6. Haykin, S., Communication Systems, 4th edition, John Wiley and Sons, Inc, 2001. Chang Chin Chen, Chen Tung Shou, Chung Lou Zo, "A steganographic method based upon JPEG and quantization table modification", Information Sciences Journal, May 2001.
7. Jackson et. al.,"Blind Steganography using Computational immune System", IJDE 1:4, 2003
8. Katzenbeisser S, Peticolas FAP, "Information Hiding techniques for Steganography and Digital Technolog", Artech House Publishers, 2000
9. Yousaf MI et.al., "Direct Sequence spread spectrum Techniques with residue No-system", IJEEE, 3:4, 2009
10. www.cs.washington.edu/education/courses/csep590/.../banerjee.doc
11. Bauer, F. L. Decrypted Secrets: Methods and Maxims of Cryptology, 3rd ed. Springer-Verlag, New York, 2002
12. http://www.hackersonlineclub.com/steganography
13. . http://www.garykessler.net/library/fsc_stego.html
14. Wayner, P. Disappearing Cryptography: Information Hiding: Steganography & Watermarking. 2nd. ed., Morgan Kaufmann, San Francisco, California, 2002
15. . Fridrich, J., Goljan, M., Hogea, D., and Soukal, D. Quantitative steganalysis of digital images: Estimating the secret message length, Multimedia Systems (2003B) 9(3):288-302. Also available: http://www.ws.binghamton.edu/fridrich/Research/mms100.pdf

16. .Farid, H. Detecting Steganographic Messages in Digital Images. Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001. Also available: http://www.cs.dartmouth.edu/~farid/publications/tr01.pdf.
17. .Miroslav Dobsiecek on "Modern Steganography" Czech Technical University in Prague, Czech Republic, 2004
18. David Kahn on "Steganography", The Code breakers, 1996
19. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn on "Information Hiding A Survey" special issue on protection of multimedia content, 87(7):1062-1078, July 1999.
20. Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon on "Image Steganography: Concepts and Practice" April 22, 2004
21. Ross J. Anderson, Fabien A.P. Petitcolas on, "On The Limits of Steganography" IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. ISSN 0733-8716.
22. Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon on *"Image Steganography and Steganalysis: Concepts and Practice"* Springer-Verlag Berlin Heidelberg 2004
23. Aimé Serge, Nguimjeu Nguépi on *"Digital Watermarking"* Fachgebiet Sicherheit in der Informationstechnik, Fachbereich Informatik, TU-Darmstadt, Deutschland, 2007
24. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, on *"Steganography and Digital technology"*, University of Birmingham GNU Free Documentation License, Version 1.2
25. Alain C. Brainos II on *"A Study of Steganography and the Art of Hiding Information"*, East Carolina University.
26. Christian Cachin on *"An Information-Theoretic Model for Steganography"*, March 4, 2004
27. Dean Lewandowski, Mike Palmisano on "Steganography"
28. James C. Judge on "Steganography: Past, Present, Future", GSEC Version 1.2f
29. WP Post on "Steganography- An Enhanced Approach", 2007

30. Pedram Hayati1, Vidyasagar Potdar, and Elizabeth Chang on “A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator”, 2007.
31. Joshua Silman on “Steganography and Steganalysis: An Overview”, august 2001
32. Madhurendra Kumar on “Image Authentication Techniques”, August 2008
33. http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
34. Niels Provos. Defending against statistical steganalysis. 2001.
35. Rakan El-Khalil and Angelos D. Keromytis. Hydan: Hiding information in program binaries.Technical report, Department of Computer Science, Columbia University, 2004.
36. www.wikipedia.com
37. www.sildeshare.com
38. “Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb The Military Technical College,Cairo, Egypt” A SECURE COVERT COMMUNICATION MODEL BASED ON VIDEO STEGANOGRAPHY
39. “Mrs.Archana S. Vaidya, Pooja N. More., Rita K. Fegade., MadhuriA.Bhavsar., Pooja V. Raut. Asst. Prof. Department of Computer Engg.GES’s R. H. Sapat College of Engineering, Management Studies and Research, Nashik (M.S.), INDIA”Image Steganography using DWT and Blowfish Algorithms
40. “ChangyongXuDepartment of Information Science, Zhengzhou Information Science and Technology Institute ,Xijian Ping Department of Information Science, Zhengzhou

    Information Science and Technology Institute, ,Tao Zhang National Laboratory ofPattern Recognition, Instituteof Automation, Chinese Academy of Sciences, Beijing”, Steganography in Compressed Video Stream
41. “S. Suma Christal Mary M.E (Ph.D) ,Lecturer Department of CSE PSN College of Engg& Technology Tamilnadu, India “IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS
42. “Poonam V Bodhak, Baisa L Gunjal”Improved Protection In Video Steganography Using DCT & LSB

43. “P.Paulpandi1, Dr.T.Meyyappan,M.sc.,M.Phil.,M.BA.,Ph.D2 Research Scholar1, Associate professor2 Department of Computer Science & Engineering, Alagappa University, Karaikud Tamil Nadu,India.”Hiding Messages Using Motion Vector Technique In Video Steganography
44. “Dipesh G. Kamdar1, Dolly Patira2, Dr. C. H. Vithalani”, DUAL LAYER DATA HIDING USING CRYPTOGRAPHY AND STEGANOGRAPHY
45. AN OVERVIEW OF IMAGE STEGANOGRAPHY
46. Steganography.pdf
47. Jain Ankit, "Steganography : A solution for data hiding", Guru Nanak Dev Engineering
College, Ludhiana
48. http://technofriends.in/2009/07/13/steganography-how-to-hide-data-in-images-and-video-files
49. .“Steganography : Reversible Data Hiding Methods for Digital Media “ – Andrew Tilley
50. http://www.comp.leeds.ac.uk/fyproj/previous-titles/bsc2002.html