ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Multiple Meliorated Security Using Steganography Embedded with Watermarking and Cryptography

Pavithraa S[1], Muthulakshmi S[2], Mounica A[3], Vijay Anandh R[4]

UG Scholar, Dept of ECE, RMK college of Engineering and Technology, Chennai, India [1&2&3]

Associate Professor, Dept of ECE, RMK college of Engineering and Technology, Chennai, India[4]

ABSTRACT: One of the most important factors of information technology and communication is the security of information. Steganography is the method through which the very existence of the message can be kept secret. Various security mechanisms have been developed by integrating steganography with cryptography. This involves encrypting any file (piece of information - data) through cryptography and encapsulating the same in another such file (carrier or container - image) and then securing it with a secret key. Among the various algorithms available for steganography, LSB algorithm is the simplest and comparably more reliable. It involves modifying the LSB of the pixels of an image with the encrypted message bits such that the basic characteristics and underlying properties of the carrier remain unchanged. However the techniques should be robust enough to prevent detection and removal of embedded data. Hence we propose to embed steganography with watermarking. Watermarking is establishing the identity of information to prevent any unauthorized usage. The objective of watermarking is to make the image perceptually and statistically invisible to others. This system provides a second layer of additional security to the existing system.

I. INTRODUCTION

Considering the scaling trends, the vandalism of electronic information has been gaining an upper hand. The detriment towards handling the secret or cipher data is mostly illegitimate. This scenario pushes us to tighten the security of the cyberspace society which demands the use of the well known concepts of **Steganography** and **Cryptography**. These are used to manipulate information to cipher their existence.Ideally scanning should fail to prove the very existence of the secret data.

Cryptography is the concept of encrypting a secret message before transmission so that no adversary can crack the code. This will then be decrypted at the receiver using the same algorithm used at the transmitter side which would yield the necessary secret data or message. However, the very presence of an encrypted data will arouse suspicion. This can be counteracted by incorporating Cryptography with Steganography.

Steganography is the practice of concealing a file, message, image, or video within another such media. The prepotency is that the intended secret message does not attract attention to itself as an object of scrutiny.

Also, preserving the ownership of information has become a sine qua non currently. Thus to provide a second layer of security is the need of the hour. This is accomplished by watermarking.

Digital watermarking is the process of conveying information by imperceptibly embedding it into the digital media (audio, video, or still images).

These digital watermarks remain intact under transmission / transformation, allowing us to protect our ownership rights in digital form. Watermarks may be visible, whose use is two-fold — to discourage unauthorized usage and to act as an advertisement. However, the invisible watermarks are preferred, as they do not cause any degradation in the aesthetic quality or in the usefulness of the data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

I. PROLOGUE

The leeway in the cut-rate digital recording and storage gave rise to an environment,where effortless replication and distribution of digital content without negligible loss in quality emerged. The continuous growth in this sectorspawnedvarious other crises like digital privacy, piracy, the use and distribution of copyrighted digital data. **Digital rights management (DRM)** schemes are various access control technologies that are used to restrict the usage of proprietary hardware and copyrighted works. DRM consists of two prominent technologies — encryption and watermarking. Our project specifically focuses on the application of watermarking and Steganography to ensure **authenticity**, **integrity** and **confidentiality**.

Cryptographyis the practice and study of techniques for secure communication in the presence of third parties called adversaries.

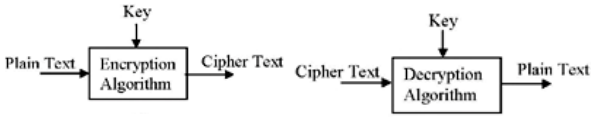


Figure 1 Processes of Encryption and Decryption

The message to send is the plain text and disguised message is the cipher text. ***Enciphering*** or encryption is the process at the transmitter side and ***deciphering*** or decryption is the converse.

Steganography simply grabs a piece of information and hides the same within another piece of information. Many computer files such as audio files, text files, images contain few blocks of data that is either *unused or not significant.* Steganography takes advantage of these unused areas and hides the encrypted message.

The term "***Information hiding***" can be related to either steganographic field or watermarking technology.

The purpose of embedding information depends on the application and the needs of the owner/user of the digital media. In essence, it should be *impossible to remove the watermark* without drastically modifying the quality of the object. Any small modification to the cover medium may destroy the concealed information.

Digital watermarking in Steganography enables useful rights protection mechanisms. Digital watermarks are mostly inserted as a *plain-bit sample* or a *transformed digital signal* into the source data using a **key-based embedding algorithm and a pseudo noise pattern.** The embedded information is hidden in low-value bits or *least significant bits* of picture pixels, frequency, or other value domains, and *inked* inseparably with the source of the data structure.Data hiding techniques can also be classified with respect to the extraction process:

1. **Cover escrow methods** need both the original piece of information and the encoded one in order to extract the embedded data.

2. **Blind or oblivious schemes** can recover the hidden message by means only of the encoded data.

COMPARISIONS *STEGANOGRAPHY VS. CRYPTOGRAPHY*

The term steganography means "concealed writing" whereas cryptography means "secret writing". Encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. So there is no protection after decryption. It isthus overcome by using steganography with cryptography.

STEGANOGRAPHY VS. WATERMARKING

Steganography deals with the hiding of information by embedding it in a cover media while watermarking nails the ownership of the information**.** In steganography, viewer or user must not know about the presence of the concealed information whereas in watermarking, this feature is *optional.*

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Video steganography literally means hiding data or media inside a video. Videos are always represented as frames and the data to be ciphered may be embedded into any one of the frames. This also provides additional security. The receiver can decipher the data only if the key frame is known in which data is hidden. This procedure involves encrypting the data or media and then storing the same in any of the frames (key frame). Thus the secret data is secluded from theadversaries.

Based on different formats of video, theencipher and decipher algorithms change accordingly.In a video sequence, the same object and background is present in successive frames with only a small change in the location of the frames. Therefore, the contrary change of resemblance region and object in successive frames can cause the visual artifacts to appear to be moving when the video is presented in real-time fashion.

Video Watermarking is also possible.There exists a complex trade-off among three parameters in digital video watermarking: data payload, fidelity and robustness. The data payload is the amount of information that is encoded by the watermark. The fidelity is the distortion that the watermarking process is bound to introduce; should remain imperceptible to a human observer and the robustness of watermarking is the ability of the detector to extract the hidden watermark from some altered watermarked data.

II. STEGANOGRAPHY AND CRYPTOGRAPHY

CLASSIFICATION AND REQUIREMENTS

There are two different applications of steganography.

1. The first is what we call **classical steganography**, and its aim is that of transmitting a message by means of another innocent or casual-looking medium.
2. The second is invisible **digital watermarking**, whose purpose is to assess the ownership or integrity of some pieces of information.

In modern approach, depending on the cover medium, steganography can be divided into five types:
1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communications. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level.

Hiding information into a medium requires following elements:

i. The cover medium(C) that will hold the secret message.
ii. The secret message (M), may be plain text, digital image file or any type of data.
iii. The steganographic techniques-ALGORITHMS
iv. A stego-key (K) may be used to hide and unhide the message.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

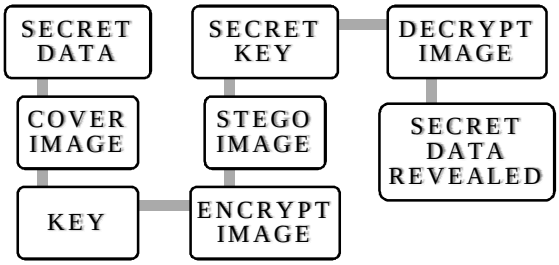


Figure 2 Flow of Steganography

IMAGE STEGANOGRAPHIC TECHNIQUES

These techniques form the crucial development stage of Steganalysis.
They can be performed in two domains

- Spatial domain
- Frequency domain

The other classifications include

- Masking and filtering
- Distortion techniques

The techniques can be combined together and executed.

SPATIAL DOMAIN TECHNIQUE

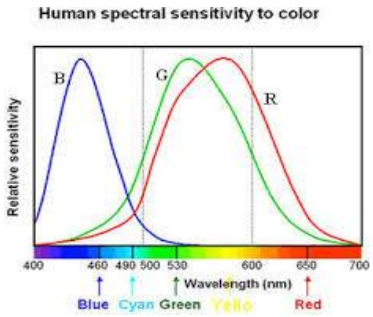


Figure3 Human Eye Perceptibility

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly.

Least Significant Bit (LSB) replacement technique,Matrix embedding,etcare some of the spatial domain techniques.

Advantages of spatial domain LSB techniques:

1. Degradation of the original image is not easy.
2. Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages of LSB techniques:

1. Robustness is low.
2. Hidden data can be destroyed by simple attacks.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

FREQUENCYDOMAIN TECHNIQUE

In Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against attacks.Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

This method uses the following transform functions in general:

1. Discrete Fourier Transform (DFT)
2. Discrete Cosine Transform (DCT)
3. Curvelet Transform
4. Discrete Wavelet Transform (DWT)
5. Radon Transform

IMAGE STEGANALYSIS

The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image.

Steganalysis are of three different types:

a. **Visual attacks** discover the hidden information, which helps to separate the image into bit planes for further more analysis.

b. **Statistical attacks** may be passive or active. *Passive attacks* involves with identifying presence or absence of a secret message or embedding algorithm used. *Active attacks* are used to investigate embedded message length or hidden message location or secret key used in embedding.

c. **Structural attacks**, the format of the data files changes as the data to be hidden is embedded.Identifying this characteristic structure changes can help us to find the presence of image/text file.

We consider in our paper, still images, as those are being most frequently exchangedon the Internet and the methods for information hiding in them are quite mature.

An advantage in using still images for data hiding is that they represent a noncausal medium, since it is possible to access any pixel of the image at random.

DATA HIDING IN STILL IMAGES

The various techniques for data hiding in still images are:

- LSB insertion
- Spread spectrum
- Texture block
- Patchwork
- Orthogonal projection coefficients manipulation
- Other methods:
  - ✓ dithering manipulation,
  - ✓ perceptual masking,
  - ✓ DCT coefficients manipulation.

To remain invisible to the eye, these techniques must exploit "holes" in the Human Visual System (HVS) vice:

1) The masking effect of edges.
2) The varying sensitivity to contrast as a function of spatial frequency.
3) The low sensitivity to small changes in luminance for random patterns.
4) The low sensitivity to very low spatial frequencies, such as continuous changes in brightness through an image.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

III. ALGORITHMS AND TRANSFORMS

LEAST SIGNIFICANT BIT(LSB) INSERTION

LSB is the simplest form of all algorithms and less complex to implement. It basically involves altering the LSBs of pixel values in the images that possess high redundancies.The concept was proposed by Rhoads - method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted.

PROCEDURE

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

- **24-bit color**: every pixel can have one in 2^24 colors, and these are represented as different quantitiesof three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- **8-bit color**: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- **8-bit gray-scale**: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

Any other kind of picture transformation, like blurring or other effects, usually will degrade or even destroy the ciphered data.

PROBLEMS AND POSSIBLE SOLUTIONS

Having stated that LSB insertion is good for steganography, we can try to improve one of its major drawbacks-the ease of extraction. We don't wanta malicious attacker be able to read everything we are sending.
This is usually accomplished with two complementary techniques:

i. **Encryption of the message**, so that who extracts it must also decrypt it before it makes sense.
ii. **Randomizing** the placement of the bits using a crypto graphical random function (scattering), so that it is almost impossible to rebuild the message without knowing the seed for the random function.

In this way, the message is protected by two different keys, acquiring much more confidentiality than before.

This approach protects also the integrity of the message, being much more difficult (we could say at least computationally infeasible) to counterfeit the message.

Anyways, since encryption is not our only objective, we must concentrate on the purpose of making the communication hidden.
The two most important issues are:

- The choice of images
- The choice of the format

The cover image must seem casual, so it must be chosen between a set of subjects that can have a reason to be exchanged between the source and the receiver.

Then it must have quite varying colors, it must be "noisy", so that the added noise is going to be covered by the already present one. Wide solid-color areas very much magnify any little amount of noise added to them.

Second, there is a problem with the file size that involves the choice of the format. Unusually big files exchanged between two peers, in fact, are likely to arouse suspicion.

Let's calculate, for instance, what the size would be for a 500x300 image (150,000 pixels), quite common for pictures on the Internet, with the different color representations:

- 24-bit color: 150,000 pixels x 24 bits/pixel / 8 bits/byte = 90,000 Bytes ~= 440KB
- 8-bit color / grayscale (the occupancy is the same):

150,000 pixels x 8 bits/pixel / 8 bits/byte =150,000 bytes = 146KB

Looking at the size, we can see that a 24-bit uncompressed picture is of a quite uncommon size, because it's very strange that the sender didn't compress it, a practice that's widely used and wouldn't have worsened the image quality.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

To solve this problem, a modification to the JPEG algorithm is used that inserts LSBs in some of the lossless stages or pilots the rounding of coefficients of the DCT used to compress the image to encode the bits.

Since we need to have small image file sizes, we should resort in using 8-bit images if we want to communicate using LSB insertion, because their size is to be considered normal.

The problem with 256 colors images is that they make use of an indexed palette and changing a LSB means that we switch a pixel from a position to an adjacent one. If there are adjacent contrasting colors in the palette, a pixel in the image changes its color abruptly and the hidden message becomes visible.

DISCRETE COSINE TRANSFORM ALGORITHM

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image 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.

$$C_x[k] = \begin{cases} \sum_{n=0}^{N-1} 2x[n]cos\left(\left(\frac{\pi}{2N}\right)k(2n+1)\right), 0 \le k \le N \\ 0, otherwise \end{cases}$$

$$x[n] = \begin{cases} \left(\frac{1}{N}\right)\sum_{k=0}^{N-1} w[k]C_x[k]cos\left(\left(\frac{\pi}{2N}\right)k(2n+1)\right), 0 \le n \le N \\ 0, otherwise \end{cases}$$

Figure 4 Images before DCT and after DCT

It is used because Fast algorithm provides high computation speeds and higher compression rates**.**Embedding in low frequency results in poor PSNR. Using low frequency coefficients affects the visual quality of the image significantly. In DCT images are broken into blocks 8x8 or 16x16, these blocks become visible when the image is reduced to higher compression ratios and it is called **block effect**.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

DISCRETE WAVELET TRANSFORM (DWT)

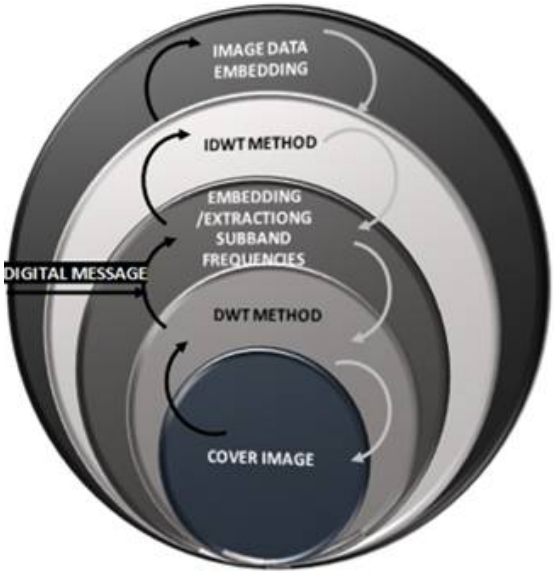


Figure 5 DWT Process

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It decomposes a signal into a set of basic functions, called wavelets. Wavelets are created by translations and dilations of a fixed function called mother wavelet.Wavelet transform provides both frequency and spatial description of an image.

The DWT splits the signal into high and low frequency parts. The low frequency part contains coarse information of signal while high frequency part contains information about the edge components. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges.

Using the quantized DWT based method; we embed secret data into the successive zero coefficients of the medium-high frequency components in eachreconstructed block for 3-level 2-D DWT of cover image.In 2-D applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. Using the quantization factors for DWT, high hiding capacity and preserving the image quality of stego-images are achieved. The original image can be recovered losslessly when the secret data has been extracted from stego-images. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1.

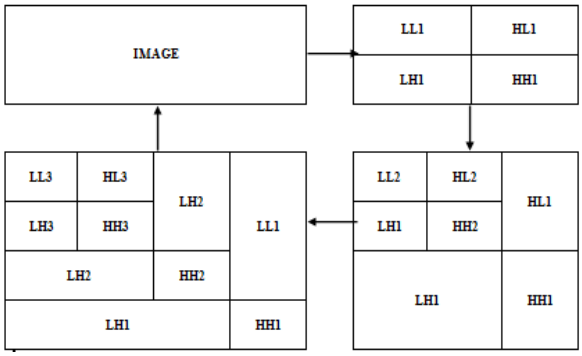


Figure 6 Level Discrete Waveletdecomposition

For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform DWT on 2 level we perform DWT on LL1 & for 3Level decomposition we applied DWT on LL2 & finally we get 4 subband of3 level that are LL3, LH3, HH3, HL3.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Both secret and cover images are divided into disjoint 4x4 blocks. The best match is determined by fitting the blocks of the secret image into the cover blocks. After which, error blocks are generated and embedded into coefficients of the best matched blocks in the HL of the cover image.

Two keys are communicated; one holds the indices to the matched blocks in the CLL (cover approximation) and another for the matched blocks in the CHL of the cover. Note that the extracted payload is not totally identical to the embedded version as only the embedded and extracted bits belong to the secret image approximation while setting all the data in other sub images to 0 during the reconstruction process.

AES METHOD

AES is the advanced version ofdata encryption standard (DES).The encrypted cipher images always display the uniformly distributed RGB pixels.The encrypted image should be different and give no clue to the original one.AES is the most flexible, secure, and fast which can replace Data Encryption standard.

Qualified Algorithm for AES are MARS, RC6, Rijndael, Serpent andtwofish. Characteristics of Rijndael are: High security, mathematical soundness, resistance to all known attacks, high encryption speed, suitability across wide range of hardware and software.

AES ALGORITHM

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14).

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure; the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively.These rounds are governed by the following transformations:

Subbyte Transformation: Is a nonlinear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and Affine Transformation.

Shift rows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

Mix columns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

Add round key transformation: Is a simple XOR between the working state and the round key. This transformation is its own inverse.

OBSERVATIONS:

1. Concludes that any normal text along withsymbol in both key as well as input can be easily encrypted and decrypted.
2. Concludes that any same number sequencewritten in key as well as input produces the decryptedmessage which contains encrypted message also.
3. Concludes that any number different typesof number sequence written as a key and input producedencrypted output along with encrypted message. It meansthat if we write numbers in key and input message at thattime decrypted message contains original message alongwith input message.
4. Concludes that if we write same textmessage in input as well as key it will perform normalencryption and decryption.
5. Concludes that AES is casesensitive algorithm if case of input message only or keyonly or both input message and key are change then itwill produces a different encrypted messageandexpected decrypted message.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

6. If we write letters along with symbols inplace of key and if input provided is in number form itwill perform normal encryption and decryption andprovide input message as a decrypted message.
7. If we write key in the form of numbersand input message in the form of letters it provides at thattime decrypted message contains original message alongwith input message.

STRENGTHS:

- AES is extremely fast compared to other block ciphers. (Though there are tradeoff between size and speed).
- The round transformation is parallel by design. This is important in dedicated hardware as it allows even faster execution.
- AES was designed to be amenable to pipelining.
- The cipher does not use arithmetic operations so has no bias towards big or little endian architectures.
- AES is fully self-supporting.

WATERMARKING – THE RUDIMENTS

The increasing amount of applications using digital multimedia technologies has accentuated the need to provide copyright protection to multimedia data. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data.It means that it remains present within the data after any decryption process. In short,"Hiding of a secret message or information within an ordinary message and the extraction of it at its destination." Complementary to encryption, it allows some protection of the data after decryption. As we know, encryption procedure aims at protecting the data during its transmission.
Both classical steganography and digital watermarking are based on a fundamental assumption: it is quiteeasy to foil the human senses.

This leads to a simple formula: given an original piece of data *d*, there is a threshold *t* below which any changes to the data won't be spotted by a person where *t*depends on the experience of the observer, but there is a minimum that's beyond the capabilities of the human senses. Thus, we can always afford to make a change *c* on *d* without being spotted.

When the attacker is technically tenacious, we can then rephrase the formula using the entropy function H(): assuming that the message we insert is perfectly encrypted, then it is indistinguishable from random data, so the entropy will be strictly additive. The entropy of the stego-medium S will be given by the sum of the entropy of the cover C and of the embedded message M:

$$H(S) = H(C) + H(M)$$

And the embedded message would be undetectable if:
1. The entropy H(M) is much less than the uncertainty in the attacker's measurement of H().
2. H(C) is reduced by some means before processing, so it is restored by adding H(M).

Once decrypted, the image is not protected anymore. By adding watermark, we add a certain degree of protection to the image (or to the information that it contains) even after the decryption process has taken place. The goal is to embed some information in the image without affecting its visual content. In the copyright protection context, watermarking is used to add a key in the multimedia data that authenticates the legal copyright holder and that cannot be manipulated or removed without impairing the data in a way that removes any commercial value.

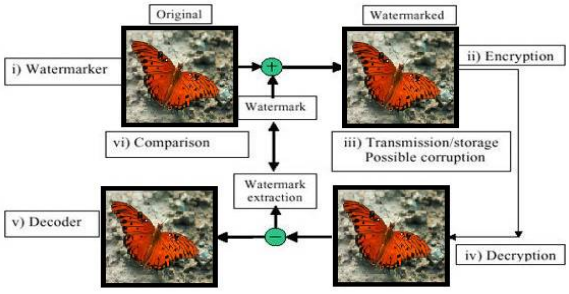


Figure 7 Watermarking Procedure

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

The purpose here is to forbid any unauthorized use of an image by adding an obvious identification key, removing the image's commercial value. While, invisible watermarks are used for content and/or author identification in order to determine the origin of the image. The purpose of invisible scheme is not to forbid any access to an image but to tell whether a specified image has been used or altered without the owner's formal consent in any way.

WATERMARKING FRAMEWORK

An image watermarking system needs to have at least the following two components:

1. A watermark embedding system
2. A watermark extraction (recovery) system

The watermark embedding system takes as input the watermark bits, the image data, and optionally a secret or public key. The output of the watermark embedding system is the watermarked image. The watermark extraction system takes as input an image that possibly contains a watermark and possibly a secret or public key. Depending on the type of watermarking system used, it may also take as input the original image or the watermark. The watermark extraction system determines whether a watermark is present or absent in the image. It may also output a confidence measure that indicates the probability with which the watermark is present in the image.

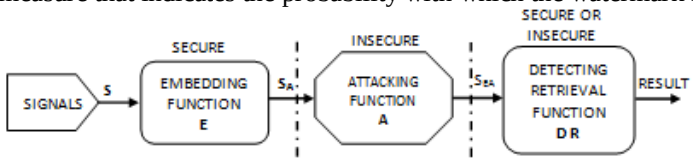


Figure 8 Overall Framework of Watermarking

WATERMARKING TECHNIQUES

The most widely used transforms include LSB method of Watermarking in Spatial domain and DWT method of Frequency domain.

LEAST SIGNIFICANT BIT WATERMARKING TECHNIQUE

LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Considering a basic grayscale image, the pixel and its values can be sliced up into significant and irrelevant levels. Because the significant levels merely represent a digital noise pattern, it could be easily used for digital watermarking. By changing selected pixel values of the noise pattern using a special or key-based algorithm, the watermarking information can be easily integrated. However, such a technique is very insecure as the watermark can be easily destroyed. But on the other hand, it can also be useful in copy control and authenticity applications.

Steps of Least Significant bit

Step 1: Convert RGB image to gray scale image.
Step 2: Make double precision for image.
Step 3: Shift most significant bits to low significant bits of watermark image.
Step 4: Make least significant bits of host image to zero.
Step 5: Add shifted version (step 3) of watermarked image to modified (step 4) host image.

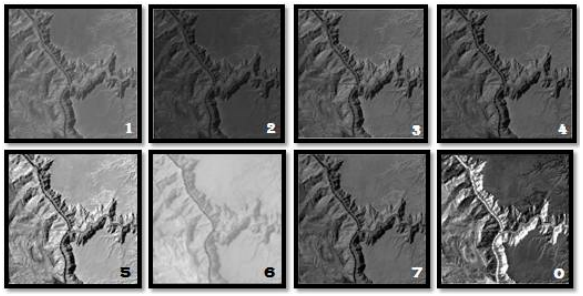


Figure 9 **7-0:**8 Bit Planes of the Image
(The number identifies the bit plane)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

In LSB watermarking of images, the concept of bit-plane splicing is used. Any 8-bit image can be represented as a combination of 8-bit planes, categorized from lest significant bit plane to the most significant bit plane.

LIMITATIONS OF SPATIAL DOMAIN WATERMARKING

This method is comparatively simple, but lacks the basic robustness that may be expected in any watermarking applications. It can survive simple operation such as cropping and any addition of noise. However lossy compression is going to defeat the watermark.

An even better attack is to set all the LSB bits to '1' fully defeating the watermark at the cost of negligible perceptual impact on the cover object. Furthermore, once the algorithm isidentified, it would be very easy for an intermediate party to alter the watermark.

DISCRETE WAVELET TRANSFORM WATERMARKING

The basic idea in the DWT for a 1D signal is as follows. A signal is split into two parts, usually high frequency and low frequency. The edge components of the signal are largely to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times, which is usually determined by the application at hand.

STEPSOFDWTWATERMARKING

Embedding Algorithm

Step 1: The first step is to decompose the image into four frequency bands using first resolutions of Haar wavelets at first level by applying DWT.
Step2: The next operation is to add a pseudo random sequence N, to the coefficients of the medium and high frequency bands.
Step3: Perform IDWT on the image and then convert back to unit8.

Extraction Algorithm

Step 1: Read in the watermarked object.
Step2: Determine size of watermarked image.
Step3: Read in original watermark.
Step 4: Determine size of original watermark
Step 5: Decompose the image into four frequency bands using first resolutions of Haar wavelets at first level by applying DWT.
Step 6: Add pn sequences to H1 and V1 components.
Step 7: Reshape the message vector and display recovered watermark.

ADVANTAGES

- With the DWT, the edges and textures are usually to the high frequency subbands, such as HH, LH, HL etc. Large frequencies in these bands usually indicate edges in an image.
- The watermarking method robust to wavelet transform based image compressions, such as the embedded zero-tree wavelet image compression scheme, and as well as to other common image distortions, such as additive noise, rescaling/stretching, and half toning. This is advantage over DCT.

ATTACKS

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

The chosen attacks are listed below.

JPEG Compression attack	Salt and Pepper noise attack
Image Resize attack	Speckle or Multiplicative noise attack
Image Cropping attack	Gamma Correction
Image Rotation attack	De-Gamma Attack
Histogram Equalization or Contrast Enhancement	Low- pass filter attack
Gaussian Noise attack	High-pass filter attack
Poisson Noise attack	Median filter attack

Figure 10 Types of Attacks

Figure 11 Lossy JPEG Compression

The various noise types that cause attacks along with PSNR values implemented using LSB Algorithm are:

NOISE TYPE	NC	PSNR
Gaussian	0.9824	19.5862
Poisson	0.9965	26.6987
Speckle	0.9767	18.3554
Salt & Pepper	0.9752	18.0862

Figure 12Various Noise and their parameters using LSB

APPLICATION OF DIGITAL WATERMARKING There is a wide variety of applications for watermarking

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

(a) Effects of Gaussian Noise

1) Owner identification: It is similar to copyright protection to establish ownership of the content.
2) *Copy protection*: It prevents people from making illegal copies of Copyrighted content.
3) Content authentication: To detect modifications of the content, as a sign of invalid authentication.
4) Fingerprinting: To trace back illegal duplication and distribution of the content.
5) Broadcast monitoring: Specifically for advertisements and in entertainment industries, to monitor content being broadcasted as contracted and by the authorized source.
6) Medical applications: It is used to provide both authentication and Confidentiality in a reversible manner without affecting the medical image.

(b) Effects of Poisson Noise

Figure 14 Effects of various Noises in Images

VII. PROPOSED WORKSTEGANOGRAPHY IMAGE AS CARRIERUSING LSB ALGORITHM

In our paper, we first attempted a simple implementation of steganography using LSB algorithm. We have used image as the carrier and the data embedded is a cipher text. The enciphering is achieved by random key generation. This key adds additional security as only with this key can the intended receiver unlock the ciphered data. The data is encrypted (digitized) and then stored in the image. This is done by altering the LSBs of the image pixels so that the overall aesthetic quality of the image is unaltered and non-detectable by the human eye.
Though simple to implement, this method suffers a disadvantage that the cipher text can be decrypted once the type of

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

algorithm is discovered.

VIDEO STEGANOGRAPHY

The cover medium here is a video. The factor to consider is the frame size. The sender should specify the frame to in which the data should be hidden. The usage of any other frame by the receiver counteracts the process and throws an error thereby achieving integrity and authenticity.

DIGITAL WATERMARKING

As discussed earlier, watermarking is responsible for revealing the ownership of the information. This makes the image static and immobile, eventually preventing it from being intercepted. However, the very presence of data is prone to arouse suspicion. This makes itimperative to combine the concepts of watermarking and steganography. While watermarking makes the data immobile, Steganography takes care of the suspicion.

The image is initially converted into bit plane (gray scale). Secondly, on the application of DWT algorithm, the data to be used as watermark is chosen. The image or data is now secure and can be reconstructed at the receiver side.

STEGANOGRAPHY EMBEDDED WITH WATERMARKING

Steganography is accomplished by choosing a cover image and a secret text to embed in it. Now the watermark image is chosen. As we have used visible watermarking, this image (logo image) is visible in the stego image. This marks the fact that no adversary will be able to snatch the image

PROPOSED DESIGN TO SWAMP SECURITY ISSUES

A serious problem with watermarking technology is the insufficient robustness of existing watermarking algorithms against geometrical distortions for example translation, rotation, scaling, cropping, change of aspect ratio and shearing. These geometrical distortions cause the loss of geometric synchronization that is necessary in watermark detection and decoding. Vulnerable to geometric distortion is a major weakness of many watermarking methods.Therefore, in this project, a watermark algorithm based on dividing image into blocks is proposed and DCT with sandwiching the watermark data in between pseudorandom sequences is applied.Also we have attempted to make it arduous for an attacker to willfully destroy the watermark.

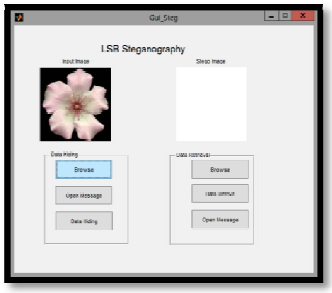
Conclusively, we have chosen an image as the watermark rather than a sequence of numbers because then it might be possible to visually identify the watermark in case it reached a reasonably advanced state of degradation after attacks (for instance if the extracted watermark after the attack had 50-60% correlation with the original watermark).

VIII. SIMULATION AND EXPERIMENTAL RESULTS

8.1 STEGANOGRAPHY USING LSB ALGORITHM:

STEP 1:

Browse through and get the required input image.



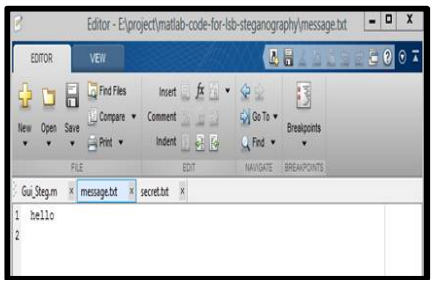
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

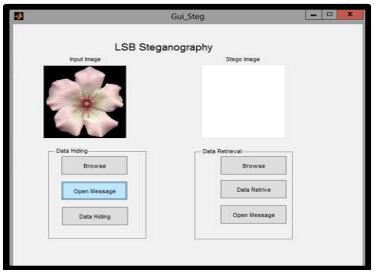
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

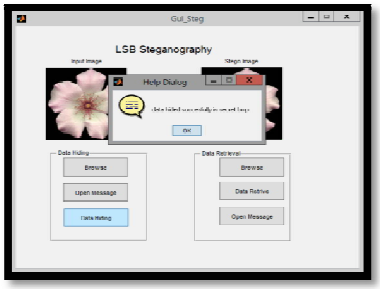
STEP 2:
The next step is to embed the secret message.Our secret message is “hello”.
This is now embedded in the input message



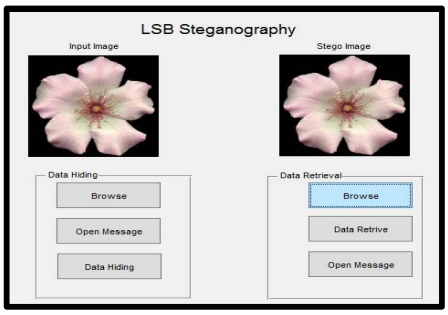
STEP 3:
Data hiding encrypts the data inside the image on successful compilation.



STEP 4:
Now that data is hidden, on the receiver side the same image is supplied.



STEP 5:



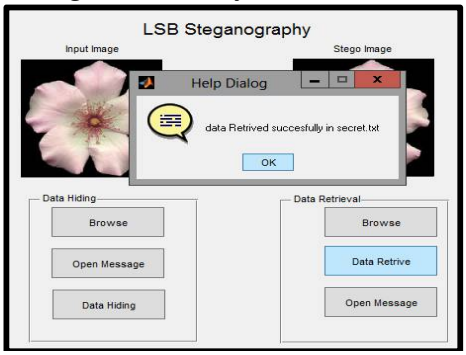
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

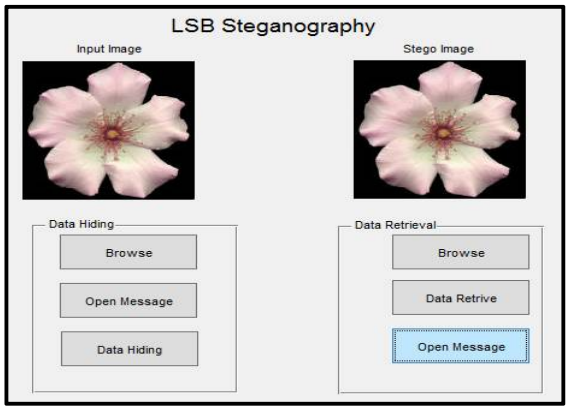
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

On clicking the “data retrieve” box, the data gets successfully retrieved and stored in secret.txt.



STEP 6:
The secret data can thus be viewed by thereceiver.
This shows the process of Steganography with encrypted secret message with image as carrier.



8.2 DIGITAL WATERMARKING

STEP 1: Browse through and get the required input image.

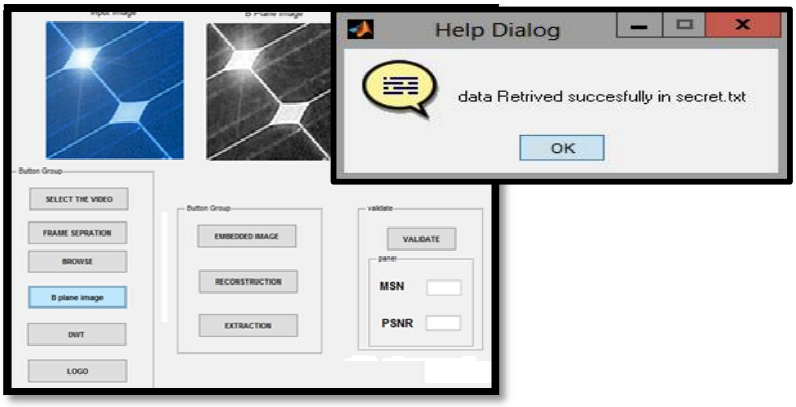
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

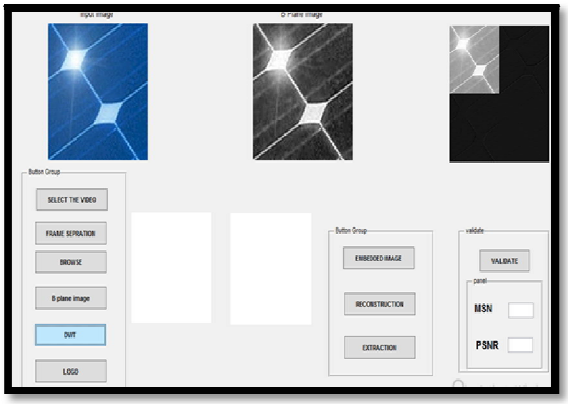
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

STEP 2:
Develop the bit plane image.



STEP 3:
Apply DWT to the B Plane image.



STEP 4:
Select the image to be watermarked using logo option.

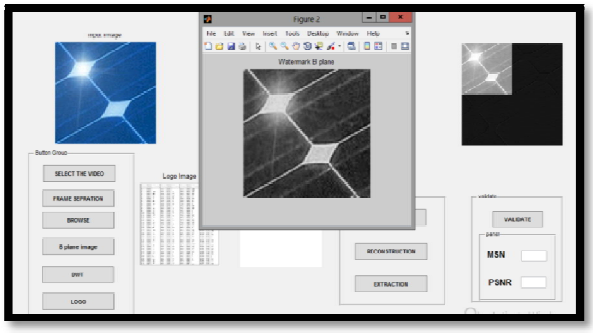
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

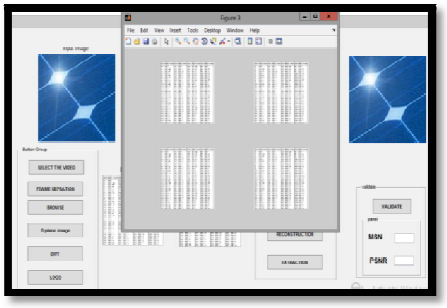
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

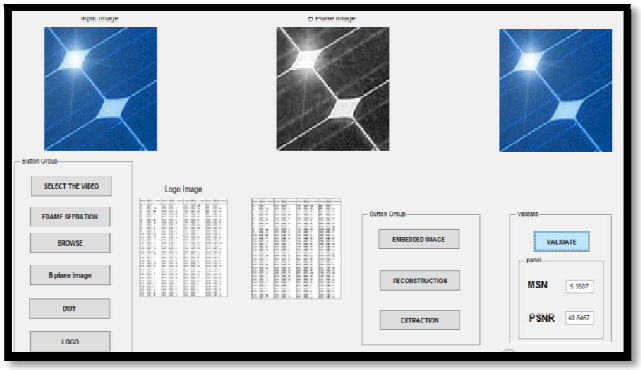
STEP 5:
The water marked image is highlighted with hidden logo.



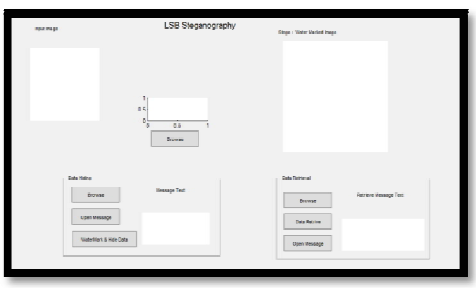
STEP 6:
At the receiver end the data is reconstructed and the secret message is retrieved.

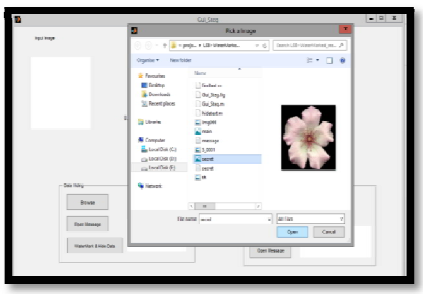


STEP 7:
The PSNR and MSN levels are validated and displayed.



STEGANOGRAPHY EMBEDDED WITH WATERMARKING
STEP 1: Browse through to get the required input image.





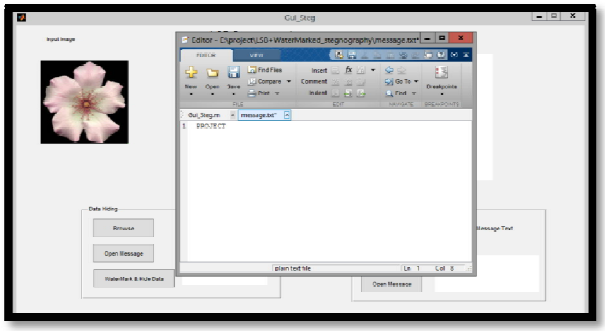
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

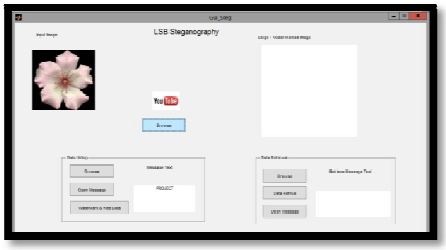
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

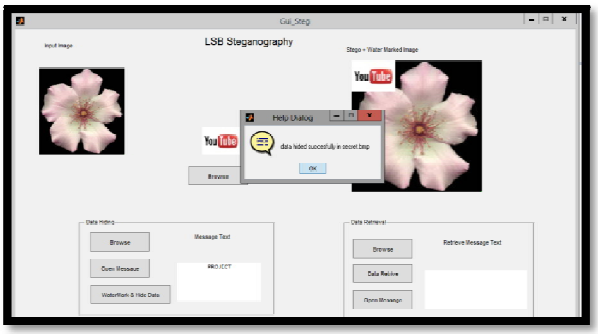
STEP 2: Open the message to be hidden – E.g.: 'Project'



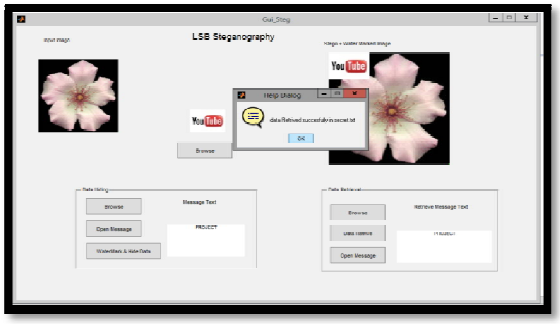
STEP 3:
Browse to get the water mark logo[here it's you tube logo].



STEP 4: The logo and message are embedded successfully at transmitting end.



STEP 5:
The data can be retrieved using the 'Data Retrieve' option.



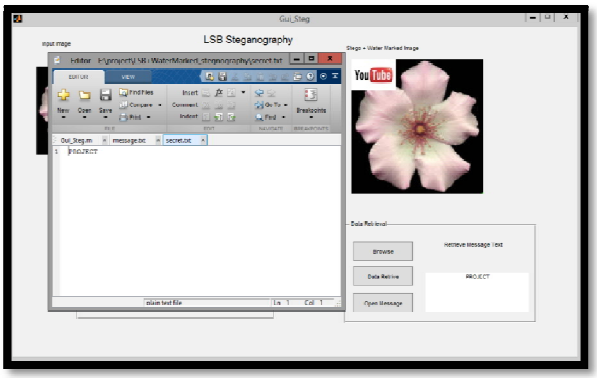
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

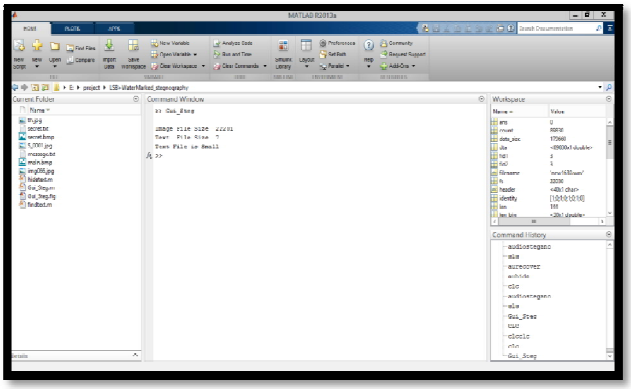
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

STEP 6: The message can be read using 'open message option'.

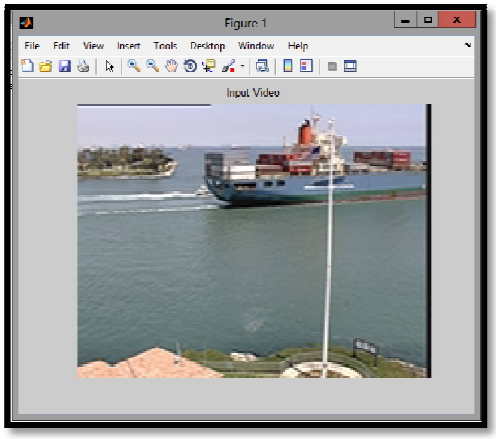


STEP 7: The size of the image file and text file is displayed in the command window.



VIDEO STEGANOGRAPHY

STEP 1: Select the required video.



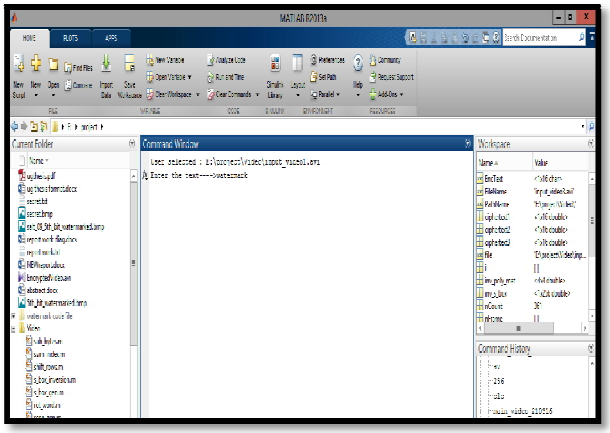
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

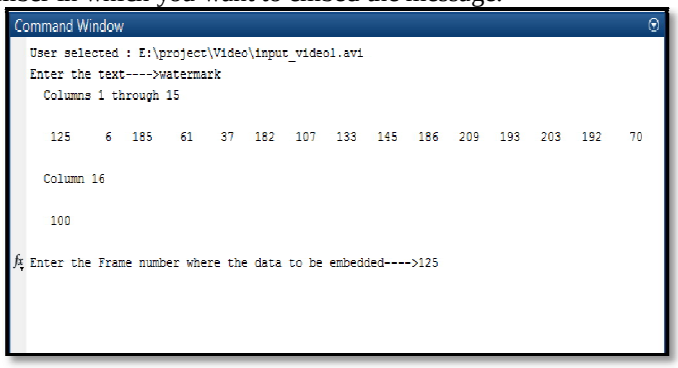
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

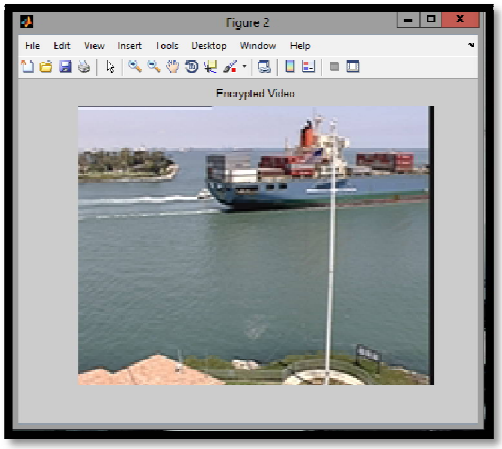
STEP 2:
Type in the secret message in the command window.



STEP 3: Enter the frame number in which you want to embed the message.



STEP 4: The encrypted video is displayed.



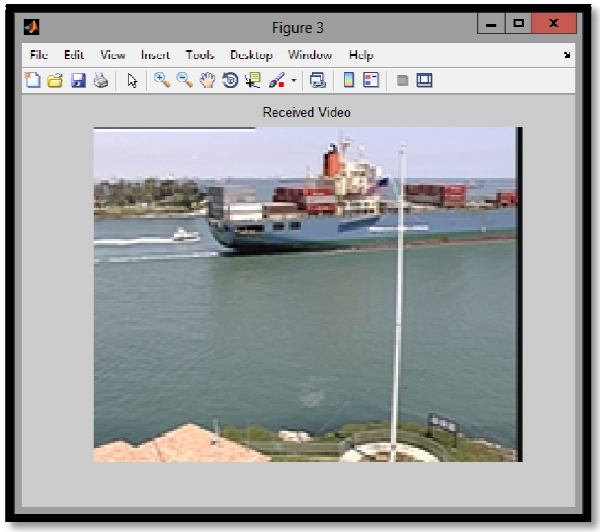
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

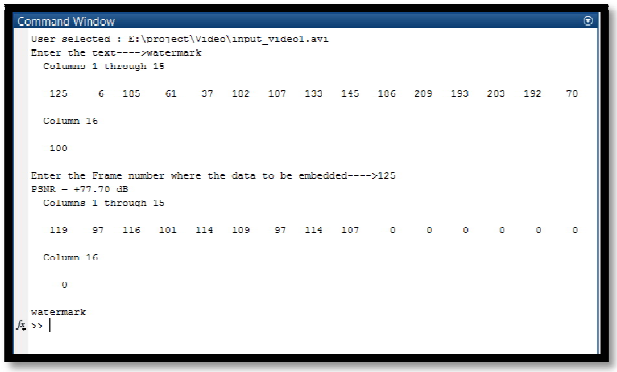
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

STEP 5:
The video is reconstructed at the receiver end.



STEP 6:
The encrypted message is received in the form of ASCII values and the corresponding PSNR values are displayed.



IX. FUTURE SCOPE

In this paper, combinedfunctions of both cryptography and steganography are explored to provide dynamic method of cloaking data from any unwarranted users. We have used audio as medium for steganography and employed LSB algorithmto encode the message inside the audio file. This proposed system does not tinker the original size of the file even after encoding,irrespective of audio file format. The encryption and decryption techniques used with this system make its aegis more robust.

The system is therefore, a brain waveforthe internet users to institute a more secured communication. This is strengthened by the digitization of media assets, the rapid growth of the Internet, and the speed of file transfers. Thus, it is necessary to have mechanisms to protect these digital assets and its associated rights,where the concept of watermarking takes its place.

We expect some commercial and effective schemes to be come-at-able in the near future. If an intelligent watermarking application softwaresystem that barricades all essentialscan be built and be implemented in a high performance DSP processor, it has a huge potential market commercially.

REFERENCES

[1] AditiGhosh, SoumenBhowmik, Arup KumarBhaumik, “High Level of Perceptibility and Security in Color Image Steganography”, International

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 2, February 2016.
[2] AbikoyeOluwakemi C, AdewoleKayode S, OladipupoAyotunde J, "Efficient Data Hiding System using Cryptography and Steganography",International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.11, December 2012.
[3] Dr. T. Ravichandran, "A New Level of Image Processing Technique Using Cryptography and Steganography", International journal of Science, Engineering and Technology Research (IJSETR), March 2013.
[4] Fengyong Li, "Steganalysis over large scale social networks with high order joint features and clustering ensembles", IEEE transactionson information forensics and security, Vol. 11,No. 2, February 2016.
[5] Gerhard C. Langelaar, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine 2000.
[6] Jan Kodovsky, "Effect of Image Downsampling on Steganographic Security", IEEE transactions on information forensics and security, Vol. 9, No. 5, May 2014.
[7] PallaviPatil and D.S. Bormane, "DWT Based Invisible Watermarking Technique for Digital Images", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.
[8] Pratibha Sharma and Shanti Swami, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform".Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).
[9] P. SunithaKency Paul, P.FascaGilgy Mary, and J.Dheeba, "Data Hiding in the Internal Dynamics of Video", ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 5, May 2013.
[10]Vahidsedighi, "Content Adaptive Steganography by Minimizing Statistical Detectability", IEEE transactions on information forensics and security, Vol.11, No.2, February 2016.