Real Time Simulation Based on Image Protection Using Digital Watermarking Techniques

M.D Imaduddin and Ganji Pullarao

ABSTRACT: There are several Protocol and embedding techniques which are used to hide data digitally for an object in highly sophisticated environment. These protocols and technique must fulfill a number of requirements correctly applied for steganography. The purpose of this experimental Study is to measure quality of embed watermarks in video signals and to hide confidential data Over it without any change and loss of data

The main focus of this paper is that we use two video clips which are bbc.avi and apple.avi. Here we set some parameter value for both clips as mention above. We are varying the quality of referenced image from 100-20% with unit difference 20% and extract the watermarks image with the value of control parameters NC

Key words: Discrete Cosine transform, Watermarking, steganography, least significant bit(LSB),Optical pixel adjustment process(OPAP), Matlab,

Definition: -

A digital watermark is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information
unique to the copyright owner, the creator of the document or the authorized consumer.

Introduction:-

Digital watermarking is a technique which allows an individual to add hidden copyright notices or other Verification messages to digital audio, video, or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking is not a form of steganography, in which data is hidden in the message without the end user's knowledge, although some watermarking techniques have the steganographic feature of not being perceivable by the human eye.

The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this. A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g., to identify the intended recipient), or be common to multiple copies (e.g., to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting where the original file remains intact, but another file is created that "describes" the original file's content. As a simple example, the checksum field for a disk sector would be a fingerprint of the preceding block of data. Similarly, hash algorithms produce fingerprint files.

Difference between Copy protection and Copyright protection

Copy protection attempts to find ways, which limits the access to copyrighted material and/or inhibit the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. A recent example is the copy protection mechanism on DVDs. However, copy protection is very difficult to achieve in open systems, as recent incidents (like the DVD hack - DeCss) show.Copyright protection inserts copyright information into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer along with the identity of the copyright holder, which allows tracing of any unauthorized copies. The most prominent way of embedding information in multimedia data is the use of digital watermarking. Whereas copy protection seems to be difficult to implement, copyright protection protocols based on watermarking and strong cryptography are likely to be feasible.

The Purpose of Digital Water Marking

Two types of digital watermarks may be distinguished, depending upon whether the watermark appears visible or invisible to the casual viewer. Visible

M.D Imaduddin and GANJI PULLARAO M Tech are with Department of Electronics Communication and Engineering, Aurora's Scientific Technological and Research Academy Bandlaguda, Hyderabad.

watermarks are used in much the same way as their bond paper ancestors, where the opacity of paper is altered by physically stamping it with an identifying pattern. This is done to mark the paper manufacturer or paper type. One might view digitally watermarked documents and images as digitally "stamped".

The visible watermarks which appear in Figures 1 and 2 illustrate the technique. The watermark in Figure 1 appears is quite obtrusive because of the high contrast between the background and foreground drawing. There is no place for the watermark to "hide" as it were. The colored image in Figure 2 renders the visible watermark less obvious.

Figure1:-Shows Example of Visible and Invisible Water marking

Invisible watermarks, on the other hand, are potentially useful as a means of identifying the source, author, creator, owner, distributor or authorized consumer of a document or image. For this purpose, the objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute. In the event of illicit usage, the watermark would facilitate the claim of ownership, the receipt of copyright revenues, or the success of prosecution.

Watermarking has also been proposed to trace images in the event of their illicit redistribution. Whereas past infringement with copyrighted documents was often limited by the unfeasibility of large-scale photocopying and distribution, modern digital networks make large-scale dissemination simple and inexpensive. Digital watermarking makes it possible to uniquely mark each image for every buyer. If that buyer then makes an illicit copy, the illicit duplication may be convincingly demonstrated

Image Compression Using Discrete Cosine Transform

JPEG stands for the Joint Photographic Experts Group, a standards committee that had its origins within the International Standard Organization (ISO).JPEG provides a compression method that is capable of compressing continuous-tone image data with a pixel depth of 6 to 24 bits with reasonable speed and efficiency.JPEG may be adjusted to produce very small, compressed images that are of relatively poor quality in appearance but still suitable for many applications. Conversely, JPEG is capable of producing very high-quality compressed images that are still far smaller than the original uncompressed data.

JPEG is primarily a lossy method of compression.JPEG was designed specifically to discard information that the human eye cannot easily see. Slight changes in color are not perceived well by the human eye, while slight changes in intensity (light and dark) are. Therefore JPEG's lossy encoding tends to be more frugal with the gray-scale part of an image and to be more frivolous with the color.

DCT separates images into parts of different frequencies where less important frequencies are discarded through quantization and important frequencies are used to retrieve the image during decompression. Compared to other input dependent transforms, DCT has many **Advantages**:

(1) It has been implemented in single integrated circuit;

(2) It has the ability to pack most information in fewest coefficients;

(3) It minimizes the block like appearance called blocking artifact that results when boundaries between sub-images become visible [11].

Technologies in particular type of water marking.

1) Techniques for Texts

1. Line Coding: Change the spacing between lines.
2. Word-shift Coding: Change the spacing between words.
3. Character Encoding: Alter the shapes of characters.

2) Techniques for Images

1. Spatial Watermarking: Just change some of the values of the pixels in the lower bit plane; e.g., Change some of the bits from 1 to 0 or 0 to 1.

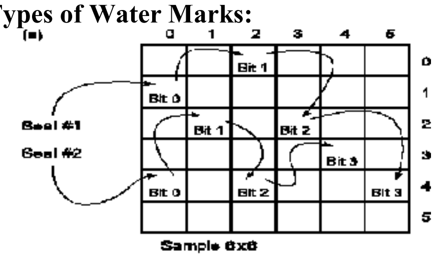
2. Frequency Domain Watermarking: First convert the image to the frequency domain and then apply the watermark in the low frequency regions.

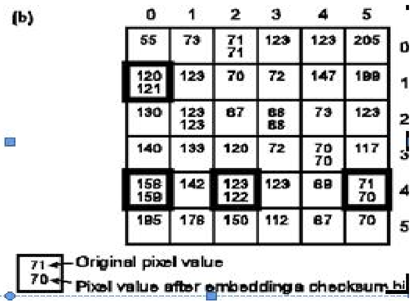
3. Checksum Technique for images

.Watermark is formed from the 7 most significant bits of each pixel. .Eight 7-bit segments (from eight different pixels) are concatenated and the final checksum is thus 56-bit. .Locations of the pixels that are to contain one bit each of the checksum are randomly chosen.

.These pixel locations along with the checksum form the watermark, W. Last bit of each pixel is then changed to the corresponding checksum bit.

Types of Water Marks:





There are lots of techniques to overcome digital water marking. That all techniques are described below.

Visible watermarks:

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image. Further, such watermarks are protected against attacks such as statistical analysis. The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, is not possible to detect them by dedicated programs.

.

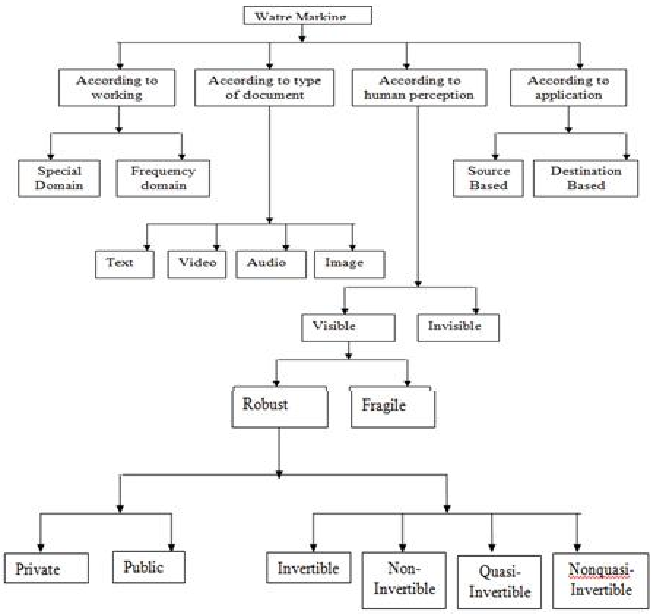


Figure2:-Hierarchy of Water marks

Watermarks have applications in maps, graphics and software user interface.

Invisible watermark:

Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copier.

Public watermark:

Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information. They are good alternatives to labels.

Fragile watermark:

Fragile watermarks are also known as tamper-proof watermarks. Such watermarks are destroyed by data manipulation.

Private Watermark:

Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.

Perceptual watermarks:

A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

Bit-stream watermark:

The term is sometimes used for watermarking of compressed data such as video.

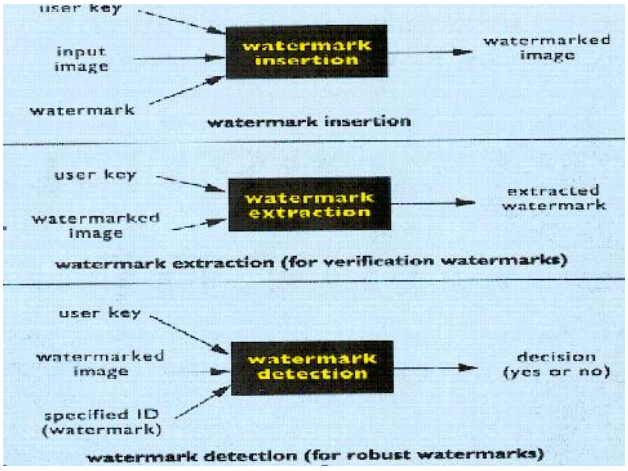
Text document watermark

Text document is a discrete information source. In discrete sources, contents cannot be modified. Thus, generic watermarking schemes are not applicable. The approaches for text watermarking are hiding watermark information in semantics and hiding watermark in text format. In semantic-based watermarking, the text is designed around the message to be hidden. Thus, misleading information covers watermark information. Such techniques defy scientific approach. By text format, we mean layout and appearance. Commonly used techniques to hide watermark information are line shift coding, word shift coding and feature coding.

Types of Water Marking

Video watermarking

Video watermarking can be considered as a superset of normal image watermarking. As such, all the techniques applicable to static images can be applied to video images. However, due to the high frame rate of video, the embedding process must occur almost in real time for live transmissions (it takes a finite time to embed the watermark, which might influence the transmission rate). If the content is generated off-line, this limitation does not exist. A very popular form of on-line (live) video watermarking is the usage of a visible watermark (normally a logo or other distinguishing sign placed in an unobtrusive place on each frame of video footage)..



The following two sequences of images demonstrate a typical watermark embedding and extraction process applied to a static image. It is notable that a slight degradation of the original image occurs when the watermark is embedded. However, the retrieved watermark is very close to the original watermark, which can help resolve ownership issues.

Requirements of Water Marking:

To be effective in the protection of the ownership of intellectual property, the invisibly watermarked document should satisfy several criteria: the watermark must be difficult or impossible to remove, at least without visibly degrading the original image,

1. the watermark must survive image modifications that are common to typical image-processing applications (e.g., scaling, color requantization, dithering, cropping, and image compression),
2. an invisible watermark should be imperceptible so as not to affect the experience of viewing the image, and
3. for some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decidability without requiring the original, un-watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

One can understand the challenge of researchers in this field since the above requirements compete, each with the others. The litmus test of a watermarking method would be that it is accepted and used on a large, commercial scale, and that it stands up in a court of law. None of the digital techniques have yet to meet these tests.

DigitalWatermarkingApplications:

- **Ownership Assertion**

.'A' uses a private key to generate a watermark and embeds it in the document
.'A' makes the watermarked image publicly available
.'B' claims that he owns the image derived from the public image
.'A' produces the unmarked original and establishes the presence of 'A's watermark

Fingerprinting

.Used to avoid unauthorized duplication and distribution.
.A distinct watermark (a fingerprint) is embedded in each copy of the data.
.If unauthorized copies are found, the origin of the copy can be determined by retrieving the fingerprint.

Authentication & integrity verification

Watermarks should be able to detect even the slightest change in the document.
.A unique key associated with the source is used the create the watermark and then embed in the document.
.This key is then used to extract the watermark and the integrity of the document verified on the basis of the integrity of the watermark.

- **Usage control & Copy protection**

.Digital watermark inserted to indicate the number of copies permitted.
.Every time a copy is made the hardware modifies the watermark and at the same time it would not create any more copies of the data.
.Commonly used in DVD technology.
:

- **Unobtrusiv:**

Invisible enough not to degrade the data quality and to prevent an attacker from finding and deleting it.
copyright of the data. Moreover, removal of it should cause a considerable degradation in the quality of the data.

- Visible watermarks should be visible enough to discourage theft.

Advantages/Disadvantages:

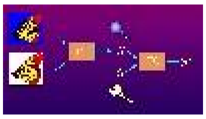
- Embedding the checksum only changes (on average) half the number of pixel. So less visual distortion.
- Can hold multiple watermarks as long as they don't overlap.
- Extremely simple and fast.

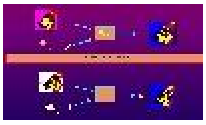
Limitation of Digital Water Marking:

As of this writing, a counterfeiting scheme has been demonstrated for a class of invertible, feature-based, frequency domain, invisible watermarking algorithms. This counterfeiting scheme could be used to subvert ownership claims because the recovery of the digital signature from a watermarked image requires a comparison with an original. The counterfeiting scheme works by first creating a counterfeit watermarked copy from the genuine watermarked copy by effectively inverting the genuine watermark.

This inversion creates a counterfeit of the original image which satisfies two properties: (a) a comparison of the decoded versions of both the original and counterfeit original yields the owner's (authorized) signature, and (b) a comparison of decoded versions of both the original and counterfeit original yield the forged (inverted) signature. This, the technique of establishing legitimate ownership recovering the signature watermark by comparing a watermarked image with the original image breaks down. It can be shown that both the legitimate signature and counterfeiter's signature inhere in both the watermarked and counterfeit watermarked copies. Thus, while it may be demonstrated that at least one recipient has a counterfeit watermarked copy, it cannot be determined which it is.This research suggests that not all watermarking techniques will be useful in resolving ownership disputes in courts of law. There will likely be non-commercial applications, or those with limited vulnerability to theft, where "good enough watermarking" will suffice. More sensitive applications may require non-invertable or non-extracting watermarking techniques. These issues are under consideration at this writing.

Standard watermarking involves the creation of a watermarked image by encoding a signature into an original image. Authentication proceeds in two stages. First, the watermarks signature is "removed" from the watermarked copy. The watermark signature is the "difference" between the original (white) and the watermarked copy of the original (blue). Next, the extracted signature (blue) is compared against the original signature (gold). Identity signifies authenticity of the copy.





Watermarking Attack

- Iterative progress
  - Attacks will lead to more robust systems
- Idea is to be able to produce images very similar to the original except that it has the watermark removed.
- Another way of saying - Hacking!!

Attacks on video watermarking

Problem: attacker digitizes video from analog source, distributes over Internet.

- Solution model one: control digitizing.
- Solution model two: control playback of digitized video in display devices.
- Is there a "common case" in either model?

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack*. While the modification may not be malicious, the term attack arises from copyright protection application, where *pirates* attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during Employed to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified. Accordingly, the MSE is when payload is 1 bpp. In contrast, the MSE obtained by LSB is 0.5. In the same year, Zhang and Wang [10] proposed an exploiting modification direction (EMD) method. EMD improves Mielikainen's method in which only one pixel in a pixel pair is changed one gray-scale unit at most and a message digit in a 5-ary notational system can be embedded. Therefore, the payload is. LSB matching and EMD methods greatly improve the traditional LSB method in which a better stego image quality can be achieved under the same payload. However, the maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively. Hence, these two methods are not suitable for applications requiring high payload.

Another group of rather practical data-hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These methods may either be implemented by avoiding embedding the message into the conspicuous part of the cover image, or by improving the embedding efficiency, that is, embed more messages per modification into the cover. The former can be achieved, for example, using "the selection channel" such as the wet paper code proposed by Fridrich *et al*. The latter can be done by encoding the message optimally with the smallest embedding impact using the near-optimal embedding schemes. In these methods, the data bits were not conveyed by individual pixels but by groups of pixels and their positions.

This paper proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency.

The image quality obtained by the proposed method not only performs better than those obtained by OPAP and DE, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

Least significant bit:

In computing, the least significant bit (lsb) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the *right-most bit*, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the *ones* (right-most) position.

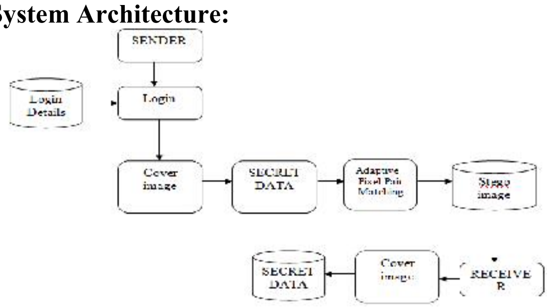
It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31}\ldots2^{0}$). Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different endianness), the term *lsb* (of course) remains unambiguous as an alias for the unit bit.By extension, the least significant bits (plural) are the bits of the number closest to, and including, the lsb.

The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums.

RELATED WORKS:

OPAP effectively reduces the image distortion compared with the traditional LSB method. DE enhances the payload of EMD by embedding digits in a B-ary notational system. These two methods offer a high payload while preserving an acceptable stego image quality. In this section, OPAP and DE will be briefly reviewed.

System Architecture:



Existing System:

The least significant bit substitution method, referred to as LSB in this paper, is a well-known data-hiding method. This method is easy to implement with low CPU cost, and has become one of the popular embedding techniques. However, in LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the imbalanced embedding distortion emerges and is vulnerable to steganalysis.

Optimal pixel adjustment process (OPAP) method to reduce the distortion caused by LSB replacement. In their method, if message bits are embedded into the right-most LSBs of an -bit pixel, other bits are adjusted by a simple evaluation. Namely, if the adjusted result offers a smaller distortion, these bits are either replaced by the adjusted result or otherwise kept unmodified.

Disadvantages of Existing System:

- Imbalanced embedding distortion emerges and is vulnerable to steganalysis.
- The existing technique can be easily cracked.

Proposed System:

The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit.

This paper proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency. The image quality obtained by the proposed method not only performs better than those obtained by OPAP and DE, but also brings higher payload with less detect ability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

Advantages of Proposed System:

The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads. Experimental results reveal that the proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well-known steganalysis techniques.

Modules:

- Extraction Function and Neighborhood Set
- Embedding Procedure
- Extraction Procedure
- Statistical Analysis of the Histogram Differences

Optimal Pixel Adjustment Process (OPAP):

The OPAP method proposed by Chan *et al.* in 2004 greatly improved the image distortion problem resulting from LSB replacement. The OPAP method is described as follows. Suppose a pixel value is *v*, the value of the right-most **r** LSBs of . Let be the pixel value after embedding message bits using the LSB replacement method and be the decimal value of these message bits. OPAP employs the following equation to adjust so that the embedding distortion can be minimized

$$v'' = \begin{cases} v' + 2^r, & v^{(r)} - s > 2^{r-1} \text{ and } v' + 2^r \leq 255 \\ v' - 2^r, & v^{(r)} - s < -2^{r-1} \text{ and } v' - 2^r \geq 0 \\ v', & \text{otherwise} \end{cases}$$

Where v'' denotes the result obtained by OPAP embedding. Note that v'' and v' have the same right-most *r* LSBs and thus, the embedded data can be extracted directly from the right-most *r* LSBs. Here is a simple example. Suppose a pixel value $v=160=10100000_2$ and the bits to be embedded are 101_2. In this case, $r=3$ and $s=5$. After is embedded, we obtained $v' = 165$. Because we obtained $v'' = v' - 2^3 = 165 - 8 = 157 = 10011101_2$. Thus, after embedding 101_2, the pixel value 160 is changed to 157. To extract the embedded data, we simply extract the right-most three LSBs of 157.

INPUT:

COVER IMAGES:

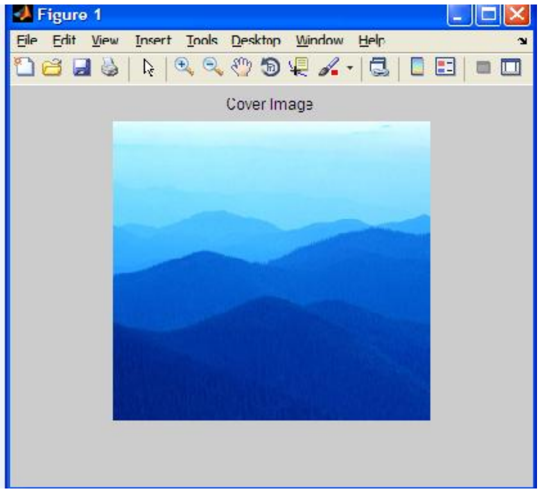


Figure 1: Input of Cover Images

SECRETE DATA IMAGE:

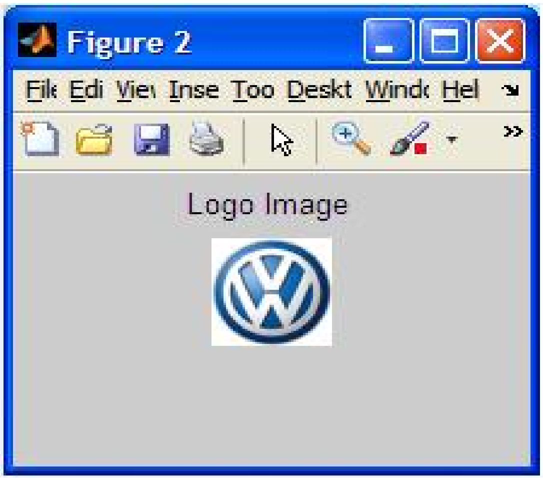


Figure 2: Input of Secrete Data Image

OUTPUT:

WATERMARKED IMAGE:

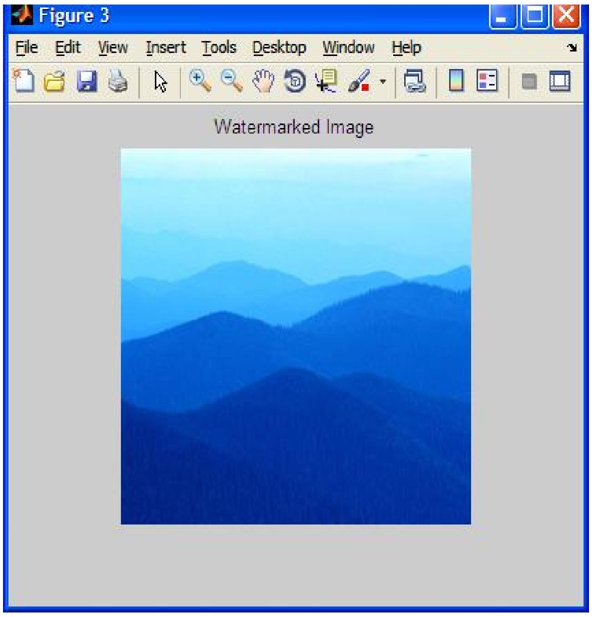


Figure 3: output of Watermarked Image:

EXTRACTED SECRETE IMAGE:

Figure 4: Extracted Secrete Data Image

CONCLUSION:

The results of our simulations are analyzed and discussed in this section. Our study provides an optimal result which is fully based on simulation and analysis. The results are analyzed and discussed in case of varying quality of image and respectively we determine values add the least significant bit in optimal pixel adjustment process of extracted image. The purpose of this experimental study is to measure the quality of embed watermarks in video signals and to hide confidential data over it without any change and loss of data.

REFERENCES:

[1] W.hong is with the department of information management. Yu Da University.Tanwen village, ChaochiaoTownship,Miaoli country 361,Taiwan(e-mail:wienhong@ydu.edu.tw)

[2] T.S.Chen with, the department of computer science and information Engineering. National Taichung University of Science and Technoiogy. Taichung404,Taiwan(e-mail:tschen@ntit.edu.tw)

[3] color versions of one more of the figures in this paper are available online at Http://ieeexplore.ieee.org

[4] A Video Watermarking Algorithm Based on the Human Visual System Properties Ji-Young Moon and Yo-Sung Ho Samsung Electronics Co., Paldal-gu, Suwon-si, Gyenggi-do,Korea Kwangju Institute of Science and Technology(K-ST) Kwangju,500-712,Korea.

[5] An Efficient Digital Image-in-Image Watermarking Algorithm Using the Integer Discrete Cosine Transform (IntDCT) . J. Zhang, Anthony T. S. Ho ICICS-PCM 2003 15-18 December 2003 Singapore IEEE 2003

[6] C. Cachin, An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on information Hiding, MIT Laboratory for Computer Science, May 1998

[7] M. D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Image, IEEE Digital Signal Processing Workshop, pp. 37-40, Department of Electrical Engineering, University ofMinnesota, http://www.assuredigit.com/tech_doc/more/Swanson_dsp96_robust_datahiding.pdf, September 1999

[8] Voloshynovskiy Sviatolsav, Joachim J. and Su Jonathan K., Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks, Proceedings of IEEE Communications Magazine, vol. 39, pages 118--126, August 2001.

[9] C. I. Podilchuk and W. Zeng, Image-adaptive watermarking using visual models, IEEE J. Select. Areas Common. vol. 16, pp. 525539, May 1998.

GANJI PULLARAO S/O KANNAIAH *M.Tech*

ADDRESS:

C/O H.NO.4-100
NEAR CPM OFFICE
KUSUMANCHI (MANDAL) POST
KHAMMAM (DIST)
ANDHRAPRADESH (STATE)
PIN: 507159

E-MAIL: pulla.ganji@gmail.com