ISSN:0975-9646

Design & Analysis of Authentication of Moving Image Using Message Digest

Vijender Kumawat
Computer Science Engineering Department
Kautilya Institute of Technology & Engineering
Jaipur, India

Ms.Palika Jajoo
Assistant Professor
Computer Science Engineering Department
Kautilya Institute of Technology & Engineering
Jaipur, India

***Abstract*— Watermarking has been used time and again for authentication & security of images. Many watermarking Techniques have evolved over a period of last 20 years in the field of information Security. Watermarking embeds identifying information in an image, which is not always hidden, in such a manner that it cannot easily be removed. It can also contain device control code that prevents illegal recording. Another application of watermarking is copyright control, in which an image owner seeks to prevent illegal copying of the image.**

Watermarking techniques can be classified into two types 1. Spatial & 2. Frequency Domain.

In this work we propose to design a new watermarking technique in which Message Digest of a Moving Image will be calculated & then it will be embedded into the Image using LSB technique. So the Message Digest of a Moving Image will act is its own watermark.

Keywords—Watermarking; Image; Message Digest; LSB; styling;

I. INTRODUCTION

With the rapid development and wide use of Internet, disclosure is facing a huge challenge for protection. We require a safe and secure way to transmit information. Encryption is a generalized system that is used to encrypt information. Except for this one is very easy to gain the interest of the attackers because the message cannot be understood directly. The information can be captured, interpreted and yet spread after damage; therefore, the reliability of the information is in ruins. The copying, processing, alteration and copyright security have become very vital concerns with the hasty use of the Internet. Therefore, there is a need to expand corpulent fighting techniques all these problems. Digital watermarking comes to light as a solution to shield the multimedia data. Digital watermarking is a method to hide or embed an undetectable data in the given data. These undetectable data is called watermark or the metadata and the data given is called data coverage.

There has been development of high speed computer networks in terms of Internet over last decades. Internet provides the means of new business, new techniques, leisure, and collective opportunities in the form of electronic publishing and advertising, real-time information release, invention ordering, operation processing, digital repositories and libraries, web e-papers and magazines, network video and audio, personal communication, lots more.

The new opportunities can be broadly grouped under the label “electronic commerce”**.** The expenditure effectiveness of selling software, high class art work in the form of digital images and video sequence by communication over World Wide Web (www) is greatly enhanced consequent to the improvement of technology.

A. *Moving Image*

Amongst various kinds of the carrier media, digital Moving images are the most widely used data on the Internet. Moving image is used to hide the secret data is called the carrier image. When the secret data has got implanted into the cover Moving image, the resultant image is called the stegano image.

B. *Steganography*

Steganography is the ability and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

Steganography includes the camouflage of information within computer files. In digital steganography, electronic communications may include stegano-graphic coding on or above transport layer, such as a document file, image file, program or protocol.

C. *Message Digest*

MD5 is the safest one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1992). When investigative work indicated that MD5's predecessor MD4 was probably to self-doubt.

MD5 processes a variable-length message into an output of fixed-length i.e. 128 bits. The input message is broken up into chunks of the blocks of 512 bits (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than the multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.

Over years, multimedia and interactive promoting services got more cost-effective.

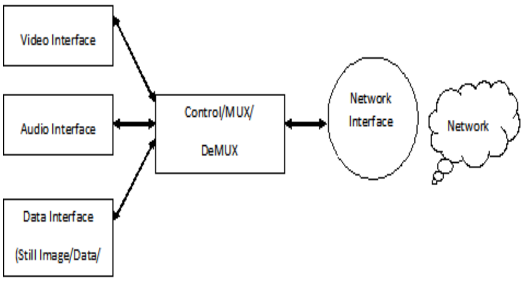


Fig 1.7. Multimedia Communication System

Multimedia is the use of information content and information processing of multiple forms of media (such as text, sound, graphics, animation, video, interactivity) to inform or entertain the user. Multimedia also refers to the use of electronic media to store and experience multimedia content. Multimedia is similar to traditional mixed media art, but a wider range. The term "rich media" is synonymous with interactive multimedia. Multimedia can be broadly divided into linear and nonlinear category. Progress linear activities without any navigation control audience, such as film screenings. Nonlinear content providers for the use of user interaction with a computer game or self-paced computer-based training to control the progress. Nonlinear content is also known as hypermedia content.

II. Types And Characteristics Of Image

Image files can be divided into two distinct categories: **vector-based and bitmap images**. These two are different in the way that how to be processed by computers. In order to decide which format will help you with your multimedia or Web project, you need to have a good understanding of both kinds of images and know their advantages and disadvantages. Then, what is a vector-based image? And what is a bitmap image?

Vector-based images are defined by mathematical relationships between points and the paths connecting them to describe an image (Doughty, 2002). If a vector-based image, for instance, contains a red dot, then the information, such as the location of the circle's center point, the length of its radius, and the color, red, would be the essential elements for this image file (Mustek, 2000). Graphical elements in a vector file are called objects (PCCafe, 2001). Each object is an independent entity with properties, such as color, shape, size, outline, and position on the screen, by its definition. [7]

Since each object is a self-contained entity, you can easily move and change its properties while maintaining its original clarity, and without affecting other objects in the illustration. These characteristics make vector-based programs ideal for illustration and 3D modeling, where the individual objects usually need to be created and manipulated through the design process (PCCafe, 2001).

Bitmap images are made of individual dots called pixels (picture elements) that are arranged and colored differently to form a pattern (PCCafe, 2001). The individual squares that make up the total image can be seen when zoomed in. However, from a greater distance the color and shape of a bitmap image appear continuous. Since each pixel is colored individually, you can easily work with photographs with so many colors and can create photo-realistic effects such as shadowing and increasing color by manipulating select areas, one pixel at a time (PCCafe, 2001). Bitmap programs are ideal to retouch photographs, editing images and video files and creating original artwork. [8]

Watermarks are classically concealed to avoid their recognition and elimination, they're considered imperceptible watermarks. But that's not the case generally. Watermarks can be utilized and usually get the form of a visual pattern overlaid on an image. The utilization of obvious watermarks is similar to the utilization of watermarks in non-digital types (such as the watermark on English money).

By using human perception it is probable to upload information within a file. Like, with audio files frequency masking happens when two hues with related frequencies are performed at exactly the same time. The listener only hears the louder tone whilst the calmer one is masked. Equally, temporal masking happens when a low-level indication happens instantly before or after a stronger one as it takes time to adjust to the trial of the new frequency. This allows a definite point in the file by which to upload the mark.

But many of the types used for digital media take advantageous asset of retention standards such as for instance MPEG to lessen file dimensions by removing the components that are not observed by the users. Therefore the tag should be entrenched in the perceptually most critical areas of the file to make it survive the retention process.

Clearly embedding the tag in the substantial areas of the file can lead to a loss of quality because number of the information will be lost. A straightforward technique requires embedding the tag at substantial bits that may decrease the distortion. But additionally, it causes it to be relatively simple to discover and eliminate the mark. A marked improvement would be to upload the tag only when substantial bits of randomly opted information within the file.

III. Data Hiding Techniques

Binary File Techniques When we are trying to hide small key data inside a binary file, whether the top key data is a copyright watermark or only simple key text, we face the problem of alteration, i.e. if anyone alters the binary file it can also cause altering the execution. Only introducing a single change can cause the execution to differ and thus this program may not function correctly and might break down the system.

It's quiet surprising why persons wish to introduce data inside binary files, since there are many other types of knowledge design through which data could be introduced. The main cause for this is the need to protect their copyright inside a binary program. One can find different ways of protecting copyright in application, such as sequential secrets, but if we look up on Internet, crucial generators for standard programs are commonly accessible and thus using sequential secrets would not be enough to protect the binary file's copyright.

Using this method, the watermark can be entrenched by creating improvements to the binary signal that doesn't require the execution of the file. To decode and get the watermark, we should have the unique binary file. By comparing the marked and original files, we are able to know from the place the declaration changes and thus take away the stuck watermark. This method really is easy but isn't against to attackers. The opponent needs variety of versions of the marked files to recognize the watermark and thus have the ability to eliminate it.

Text Techniques Although it is very easy to see when we have committed a copyright infringement by photocopying a guide, since the feature is commonly different, it is more challenging when it comes to electronic versions of text. Copies are the exact same and it is difficult to share with if it's an authentic or perhaps a copied version. To introduce data inside a record we are able to clearly transform a number of their attributes. These can be also the text style or faculties of the characters. We may believe when we modify these faculties it can become obvious and clear to next events or attackers. The main element of this issue is that people modify the record in a way that it is simply not visible to the eye however it is probably decoded by computer.

Image Techniques

Simple Watermarking

A very easy however carefully applied process for watermarking images is to add a pattern along with a current image. Frequently this product is a graphic in itself - an emblem or something related, which distorts the underlying image. In an ordinary picture manager it probably will merge both images and get a watermarked image. So long as we realize the watermark, it is possible to change any undesirable effects so that the unique doesn't need to be kept. This process is only actually applicable to watermarking, whilst the product can be viewed and actually with no original watermark, it is probable to eliminate the pattern from the watermarked picture with some energy and skill.

LSB Least Substantial Bit Hiding (Image Hiding) -This approach is probably the best means of hiding information in a graphic and however it is remarkably effective. It operates using the least substantial pieces of every pixel in one single picture to hide the absolute and most substantial components of another. So in a JPEG picture as an example, the following measures should be used.

1. First stock up both the sponsor picture and the picture we need to hide.
2. Next chose the number of pieces we wish to hide the trick picture in. The more the number of pieces used in the sponsor picture, the more it deteriorates. Increasing the number of pieces applied however demonstrably features a valuable reaction on the trick picture raising its clarity.
3. We now have to produce a new picture by mixing the pixels from equally images.

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. Also while in this example an image has been hidden, the least significant bits could be used to store text or even a small amount of sound. All we need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data.

Direct Cosine Transformation

Yet another means of covering knowledge is through a primary cosine change (DCT). The DCT algorithm is among the primary elements of the JPEG pressure process works as follows

1. First the picture is separated into 8 x 8 squares.
2. Next all these sections are altered with a DCT, which results in a multidimensional array of 63 coefficients.
3. A quantized unit of all these coefficients, which basically is the pressure stage as that, is where knowledge is lost.
4. Small insignificant coefficients are spherical to 0 while greater types eliminate some of the precision.
5. As of this stage we should have numerous streamlined coefficients, which are more squeezed with a Huffman encoding scheme or similar.
6. Decompression is performed via an inverse DCT.

Hiding with a DCT pays to as somebody who only looks at the pixel prices of the picture would be ignorant that any such thing is amiss. Also the hidden knowledge can be distributed more equally over the entire picture in such a way as to create it more robust.

One process hides knowledge in the quantize stage. If we need to encode the bit price 0 in a certain 8 x 8 sq of pixels, we could try this by ensuring all the coefficients are actually, as an example by fine-tuning them. Bit price 1 can be stored by fine-tuning the coefficients so they are odd. In this way a sizable picture may keep some knowledge that's quite difficult to identify in comparison to the LSB method. This can be a quite simple process and while it is effective to keep down disturbances, it is at risk of noise. Other practices, which use DCT transformations, occasionally use different formulas for holding the bit. One employs pseudo noise to incorporate a watermark to the DCT coefficients while still another employs an algorithm to scribe and acquire a bit from them. These other practices are generally more technical and are more robust compared to strategy described.

Original Image

Watermarked Image

JPEG compressed

Wavelet Change

While DCT transformations support covered watermark data or normal data, they don't perform good job at larger retention levels. The blocky search of squeezed JPEG documents is as a result of 8 x 8 prevents utilized in the transformation process. Wavelet transformations on one other are far better at large retention levels and ergo improve the amount of robustness of the information that is concealed, something which will be crucial in a location like watermarking.

That strategy works by getting several wavelets to scribe a complete image. They allow photos to be squeezed at an extent by holding the large volume “details” in the image separately from the lower volume parts. The low volume places will then be squeezed which will be adequate because they are sensible for compression. Quantization will then get spot to decrease points more and the entire method will start again if needed.

IV. HASH FUNCTIONS/ MESSAGE DIGEST

Message digest functions also called *hash functions*, are used to produce digital summaries of information called message digests. Message digests (also called *hashes*) are commonly 128 bits to 160 bits in length and provide a digital identifier for each digital file or document. Message digest functions are mathematical functions that process information to produce a different message digest for each unique document. Identical documents have the same message digest; but if even one of the bits for the document changes, the message digest changes. Figure shows the basic message digest process.

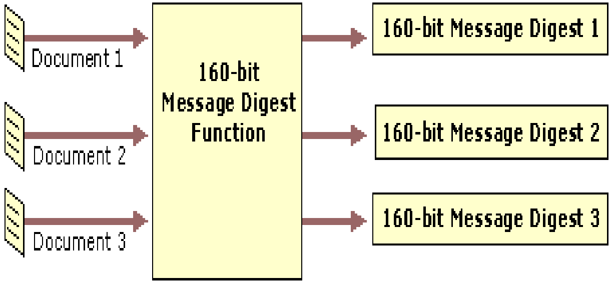


Figure. Example of the Message Digest Process

Because message digests are much shorter than the data from which the digests are generated and the digests have a finite length, duplicate message digests called *collisions* can exist for different data sets. However, good message digest functions use one-way functions to ensure that it is mathematically and computationally infeasible to reverse the message digest process and discover the original data. Finding collisions for good message digest functions is also mathematically and computationally infeasible but possible given enough time and computational effort. However, even if an attacker discovers a collision, it is highly improbable that the collision could be useful. For example, assume that an English message produces a message digest with a value of *n*, and an attacker somehow manages to computationally generate a second set of data that also produces a message digest of *n* . The second set of data would have to be in the English language and form a coherent and germane message for an attacker to be able to use it for an illicit purpose, such as sending a counterfeit message in the place of the original message. With the best message digest functions in use today, the probability that a second set of collision data would be in a known language or form a coherent message is minuscule.

Message digests are commonly used in conjunction with public key technology to create digital signatures or "digital thumbprints" that are used for authentication, integrity, and nonrepudiation. Message digests also are commonly used with digital signing technology to provide data integrity for electronic files and documents.

For example, to provide data integrity for e-mail messages, message digests can be generated from the completed mail message, digitally signed with the originator's private key, and then transmitted with e-mail messages. The recipient of the message can then do the following to check the integrity of the message:

- Use the same message digest function to compute a digest for the message.
- Use the originator's public key to verify the signed message digest.
- Compare the new message digest to the original digest.

If the two message digests do not match, the recipient knows the message was altered or corrupted. Figure below shows a basic integrity check process with a digitally signed message digest.

Because the message digest is digitally signed with the sender's private key, it is not feasible for an intruder to intercept the message, modify it, and create a new valid encrypted message digest to send to the recipient. Another method of ensuring the integrity of data is to use message digests with a Hashed Message Authentication Code (HMAC) function.

Two of the most commonly used message digest algorithms today are MD5, a 128-bit digest developed by RSA Data Security, Inc., and SHA-1, a 160-bit message digest developed by the National Security Agency. The SHA-1 algorithm is generally considered to provide stronger cryptographic security than MD5, because it uses a longer message digest and it is not vulnerable to some attacks that can be conducted against MD5.

Message Digest 5

The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input. MD5 is used in many situations where a potentially long message needs to be processed and/or compared quickly. The most common application is the creation and verification of digital signatures.[13]

V. PROPOSED WORK MODEL

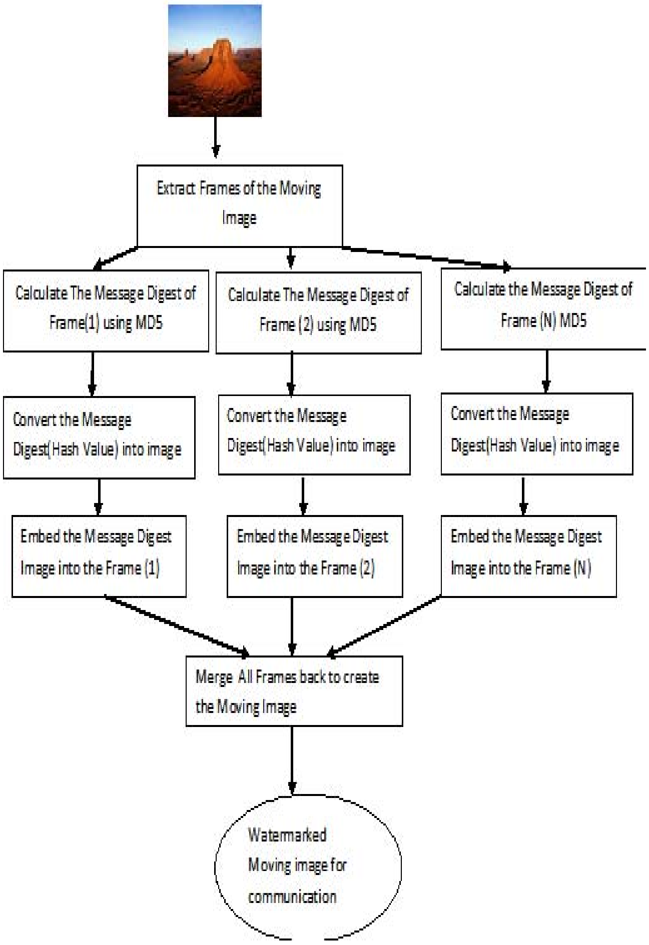
Many techniques exist for watermarking an image using text, image or any other media as the watermark is embedded in the cover image.

There are also many techniques of watermarking involving, Least Significant bit, Discrete Wavelet Transformation, Discrete cosine Transformation and many more, which effectively and more importantly they ensure and protected communication of the cover object which delivers the result of watermarking to the receiver with minimum redundancy.

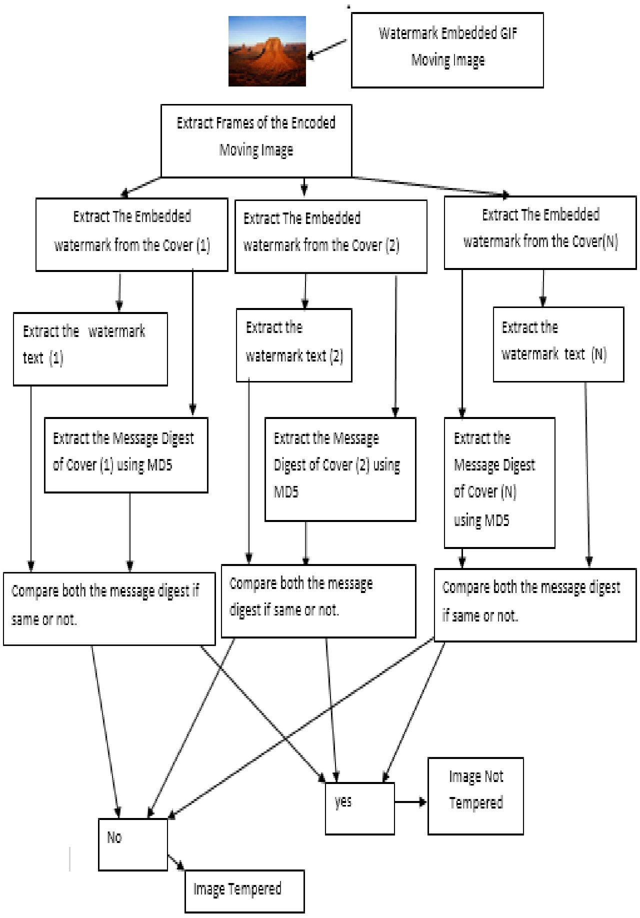
One of the arts of watermarking for copyright protection is Cover Generation Technique, in this technique the message which user wants to send the end user converts itself into the image and then the receiver cracks the image to obtain the secret message hidden inside.

Here in this work we propose an art of message Generation technique, in which the Cover Moving image is used to create the secret message and then that secret message is embedded into the cover image.
For implementing the same the Message Digest using MD5 algorithm is calculated of the cover image, which is converted into a image then this MD5 image is embedded into cover image using 1 LSB(Least Significant Bit).
Our work comprise of two stages:

Stage 1:
It is done at the sender end; the sender first extracts the various frames of the moving image and then he calculates the Message Digest of each individual frame using MD5 algorithm, which is then converted into a binary image then this MD5 image is embedded into cover image using 1 LSB (Least Significant Bit).
The flow chart at the sender end is as follows:

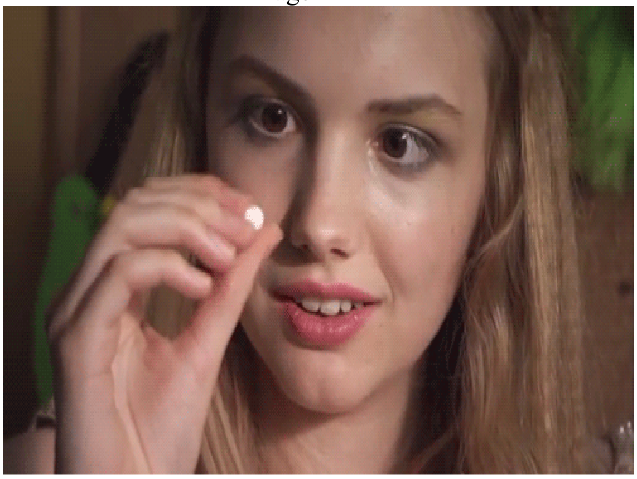

Extract Frames of the Moving Image
Calculate The Message Digest of Frame(1) using MD5
Calculate The Message Digest of Frame (2) using MD5
Calculate the Message Digest of Frame (N) MD5
Convert the Message Digest(Hash Value) into image
Convert the Message Digest(Hash Value) into image
Convert the Message Digest(Hash Value) into image
Embed the Message Digest Image into the Frame (1)
Embed the Message Digest Image into the Frame (2)
Embed the Message Digest Image into the Frame (N)
Merge All Frames back to create the Moving Image
Watermarked Moving image for communication

Stage 2:
It is done at the receiver end; the receiver extracts all the frames of the Watermarked Moving image, then he decomposes the watermarked Frames and extracts their respective hash images and finds the hash value of cover frames and compares both of them


Watermark Embedded GIF Moving Image
Extract Frames of the Encoded Moving Image
Extract The Embedded watermark from the Cover (1)
Extract The Embedded watermark from the Cover (2)
Extract The Embedded watermark from the Cover(N)
Extract the watermark text (1)
Extract the watermark text (2)
Extract the watermark text (N)
Extract the Message Digest of Cover (1) using MD5
Extract the Message Digest of Cover (2) using MD5
Extract the Message Digest of Cover (N) using MD5
Compare both the message digest if same or not.
Compare both the message digest if same or not.
Compare both the message digest if same or not.
No
yes
Image Not Tempered
Image Tempered

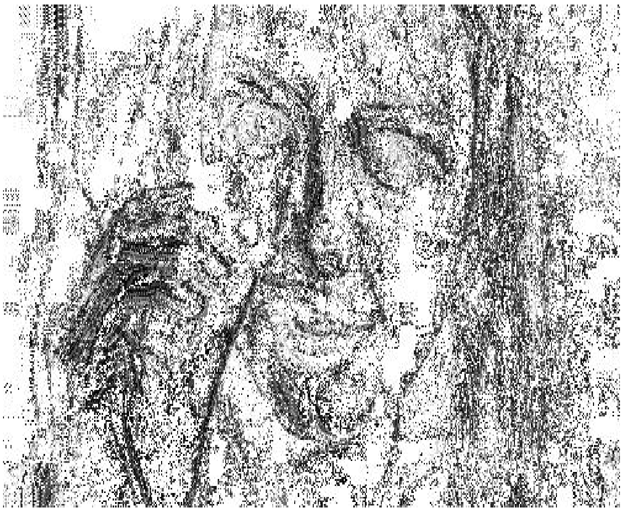
Implementation
We have taken three different GIF images and perform above said process on the images here we show the snapshots of original GIF image, its frames and their Message Digest, and recovered watermark image for every image separately, which are as follows:

Image LADY



Frame 1 of LADY GIF

Frame 2 of LADY GIF



Frame 3 of LADY GIF

Hash value of Frame 1

b0944794ea7906ef91abf1241defbdc9

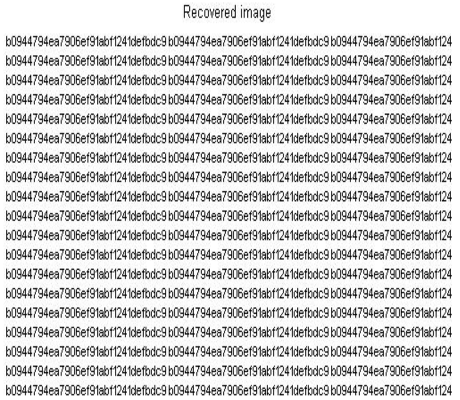
Hash value of Frame 2

b29b6419894d1e8b3f9823545d90d867

Hash value of Frame 3

97f0e09dbbd48cefb0d6219bba36c05f

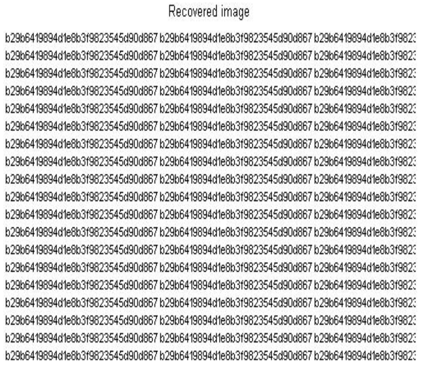
Recovered Hash value from Encoded Frame 1



Recovered image

```
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf1241defbdc9 b0944794ea7906ef91abf124
```

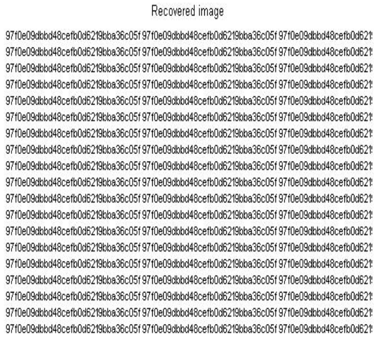
Recovered Hash value from Encoded Frame 2



Recovered image

```
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823545d90d867 b29b6419894d1e8b3f9823
```

Recovered Hash value from Encoded Frame 3



Recovered image

```
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d6219bba36c05f 97f0e09dbbd48cefb0d621
```

Figure 1 Lady Frames, Message Digest as Watermarks and Recovered Watermarks

Results & Analysis

We analyses the outcome of efforts made by the sender and results of watermarked image

Table: PSNR of Original Frames compared with Watermarked Frames and finally of whole GIF

S. No.	Name of Image	Size of Image	PSNR Frame 1	PSNR Frame 2	PSNR Frame 3	PSNR of both GIF
1	Lady	500 X 282	51.2962	53.0814	52.9207	52.35506

The above table shows the name of each frame its size and respective PSNR values PSNR of individual frames and their respective GIF Files too. The PSNR's are calculated by comparing extracted cover frames from Original GIF and embedded cover Frames and then we also compare Original GIF with the New designed GIF .

As seen in the table and below given graph the PSNR of individual frames are varying, but when it comes to the Final GIF comparison the GIF with smaller frame size has more losses and thus has less PSNR while the GIF with larger frame size has less loss and thus has higher PSNR value. But the PSNR of approx. 50db for all the GIF frames and GIF indicate that the quality of Watermarking technique developed here is very good and thus it incurs minimum losses.

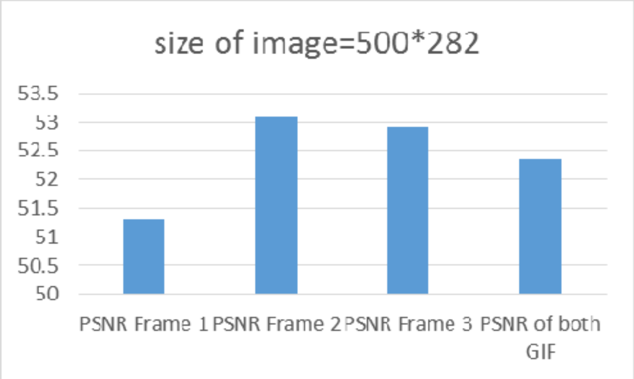


Figure PSNR Values of all the test GIF images

CONCLUSION & FUTURE WORK

There are also many techniques of watermarking involving, Least Significant bit, Discrete Wavelet Transformation, Discrete cosine Transformation and many more, which effectively and more importantly they ensure and protected communication of the cover object which delivers the result of watermarking to the receiver with minimum redundancy.

One of the arts of watermarking for copyright protection is Cover Generation Technique, in this technique the message which user wants to send the end user converts itself into the image and then the receiver cracks the image to obtain the secret message hidden inside.

Here in this dissertation we propose an art of message Generation technique, in which the Cover Moving image is used to create the secret message and then that secret message is embedded into the cover image.

For implementing the same the Message Digest using MD5 algorithm is calculated of the cover image, which is converted into a image then this MD5 image is embedded into cover image using 1 LSB(Least Significant Bit).

As our results show that the PSNR of final output watermarked GIF image is very good in terms of input GIF image and the work done for securing the GIF image for communication has also been achieved.

We also achieved the goal of ensuring authentication of the watermark GIF image by verifying the Message Digest.

Future Work

In future one can perform the further task to enhance better results and good security:

1. Use embedding techniques like DCT or DWT
2. Use various kind of images formats.
3. Use other multimedia formats like moving images & video.
4. Use other types of Message digest for high quality authentication.
5. Use encryption techniques in tandem to the above work for better security too.

REFERENCES

[1]. Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, “Image Captcha Based Authentication Using Visual Cryptography”, Ijreat, Issn: 2320 – 8791, April 2013

[2]. Mr. A.Duraisamy, Mr.M.Sathiyamoorthy, Mr.S.Chandrasekar, “Protection Of Privacy In Visual Cryptography Scheme Using Error Diffusion Technique Using Error Diffusion Technique”, Ijcsn Issn (Online) : 2277-5420 April 2013

[3]. Ankita Gharat, Preeti Tambre, Yogini Thakare, Prof. S.M. Sangave “Biometric Privacy Using Visual Cryptography” Ijarcet, Issn: 2278 – 1323, January 2013

[4]. Vilma Petrauskiene, Rita Palivonaite, Algiment Aleksa, Minvydas Ragulskis “Dynamic Visual Cryptography Based On Chaotic Oscillations”, Elsevier, 2013.

[5]. Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam And Tanveer Al Jami, “An Exploitation Of Visual Cryptography To Ensure Enhanced Security In Several Applications”, Ijca Issn: 0975 – 8887, 2013

[6]. Anushree Suklabaidya, “Visual Cryptographic Applications”, Ijcse, Issn: 0975- 3397, June 2013

[7]. M. L. Miller, I. J. Cox, And J. A. Bloom, "Informed Embedding: Exploiting Image, Digital Watermarking, Morgan Kaufmann Publishers Inc., San Francisco, Ca, 2001.

[8]. Jitao Jiang, Xueqiu Zhou And Xiaohong Liu, “An Improved Algorithm Based On Lsb In Digital Image Hidden”, Journal Of Shandong University Of Technology (Science And Technology), Vol. 20(3), 2006, Pp. 66-68, Issn: 1672-6197.0.2006-03-018.

[9]. Juan Zhou, Shijie Jia, “Design And Implementation Of Image Hiding System Based On Lsb”, Computer Technology And Development, Vol. 17 (05), 2007, Pp. 114-116, Doi: Cnki: Issn: 1673-629x.0.2007-05-034.

[10]. Jianwei Zhang, Xinxin Fang, Junhong Yan, “Implement Of Digital Image Watermarking Lsb”, Control & Automation, Vol. 22(10), 2006, Pp. 228-229, Doi: Cnki:Issn:1008-0570.0.2006-10-083.

[11]. Qian-Lan Deng Jia-Jun Lin, “A Steganalysis Of Lsb Based On Statistics”, Modern Computer, No.1, 2006, Pp. 46-48, Doi: Cnki: Issn: 1007-1423.0.2006-01-010.

[12]. Jian-Quan Xie, Chun-Hua Yang. “Adaptive Hiding Method Of Large Capacity Information”, Journal Of Computer Applications, Vol. 27(5), 2007, Pp.1035-1037, Doi: Cnki: Issn: 1001-9081.0.2007-05-001.

[13]. Hongwei Lu, Baoping Wan, “Information Hiding Algorithm Using Bmp Image”, Journal Of Wuhan University Of Technology, Vol.28(6), 2006, Pp. 96-98, Doi: Cnki: Issn: 1671-4431.0.2006-06-027.

[14]. Shaik. Basheera, P. V. Naganjaneyulu & N. Renuka, 2013, Distortion Free Fragile Watermarking Technique For Medical Images, International Journal Of Computer Science Engineering And Information Technology Research, Vol 3. No. 2, Pp 187-192

[15]. Harish Nj, Kumar Bbs, Kusagur A (2013) Hybrid Robust Watermarking Techniques Based On Dwt, Dct, And Svd. Int J Adv Electric Electron Eng 2(5):137–143

[16]. R. HovančÁk, P. Foriš, And D. Levický, "Steganography Based On Dwt Transform", Available On: Www.Urel.Feec.Vutbr.Cz/Ra2007/Archive/Ra2006/Abstracts/038.Pdf

[17]. Rathod Jigisha D, Rachana V.Modi ,2013, A Hybrid Dwt-Svd Method For Digital Video Watermarking, International Journal Of Advanced Research In Computer And Communication Engineering Vol. 2, Issue 7, July 2013

[18]. Md. Maklachur Rahman, “A Dwt,Dct And Svd Based Watermarking Technique To Protect The Image Piracy”, International Journal Of Managing Public Sector Information And Communication Technologies (Ijmpict)Vol. 4, No. 2, June 2013

[19]. Chia-Chen Lin Et. Al. 2014 , A Novel Svd-Based Watermarking Scheme For Protecting Rightful Ownership Of Digital Images, Journal Of Information Hiding And Multimedia Signal Processing, Vol. 5 No. 2

[20]. Dmitri Jarnikov, Et. Al. 2014, Forensic Watermarking, Iarjj, Vol.3 No. 5

[21]. Burman Et. Al., 2013, “Histogram Based Color Image Authentication By Digital Image Watermark Technique”, International Journal Of Engineering Research And Applications Issn: 2248-9622 Vol.3 No. 4.Page No. 321-326

[22]. Gil-Je Lee, Eun-Jun Yoon, Kee Weng Yoo "A New Lsb Based Digital Watermarking Scheme With Random Mapping" In 2008 International Symposium On Ubiquitous Multimedia Computing

[23]. N. Askari et.al, "Visual Cryptography", 2007, IJCRSSE, Vol. 2., No. 3

[24]. P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Weng , (2008) "A New Copyright Protection Scheme With Visual Cryptography", Second International Conference On Future Generation Communication And Networking Symposia. Pp. 60-63.

[25]. J.J. Eggers, J.K. Su And B. Girod, "A Blind Watermarking Scheme Based On Structured Codebooks," Iee Colloquium: Secure Image And Image Authentication, London, Uk, April 2000

[26]. A. Westfield, A. Pfitzmann. "Attacks On Steganographic Systems". In Proceedings Of 3rd. International Workshop Computer Science (Ih '99) Germany, 1999.

[27]. M. C. Padma et.al Wavelet Packet Based Texture Features for Automatic Script Identification

[28]. Ge Xiuhui and Tian Hao," Research on application of Immune digital Water marking Algorithm", International conference on computer Science and Software Engineering",2008,pp 806-809.