International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.10 (2016), pp.197-214
http://dx.doi.org/10.14257/ijmue.2016.11.10.20

A Comparative Evaluation of Common Multimedia Steganography Approaches

Mustafa Sabah

AL-Mansour University College
muustafa_bayat@yahoo.com

Abstract

Information hiding techniques have recently turned out to be critical in many applications. Text message, a digital sound recording, movie, as well as images tend to be progressively equipped using distinct nevertheless imperceptible grades, which might include a hidden copyright notice as well as assistance to prevent unauthorized replicating immediately. Many analysts will work in data disappearing techniques employing unique suggestions and regions to cover their secret files. In this paper we present a theoretical performance analysis for some basic method of text based - Steganography techniques, audio files, portable executable files, and digital images, then we compare between them according to their performance using some evaluation parameters to accomplish the goal of reduces the chances of error and enhances security measures.

Keywords*: Information hiding, performance analysis, Multimedia Steganography Approaches*

1. Introduction

Steganography remains on its evolutionary track in this diverse distributed computing domain where most of the applications Internet –based [1]. Therefore, there is a requirement for secret communication [2]. Steganography is the art of hiding information plus an effort to hide the presence of the embedded information [3]. It is not proposed to swap cryptography however supplement it. Hiding a message through Steganography approaches decreases the accidental of a message being detected [4].Cover is the meaning of stego so the image is named as cover image. It assists as a better technique of securing message than cryptography which only hides the content of the message not the presence of the message.

Original message is being hidden inside a carrier such that the modifications so happened in the carrier are not noticeable [5]. The message is inserted in text files, audio, picture also video [6]. Steganography is used in our day today life such as watermarking, ecommerce applications, and for data transfer [7]. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [8]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement [7]. The dialectal steganography is provided for the information hiding. Text steganography is found to be the challenging kind of steganography due to the absence of redundant information in a text file as associated with a picture, otherwise sound file [9].

Audio steganography is attentive in hiding secret information in an acquitted cover audio file or signal securely in addition to strongly. So, communication security and strength are energetic for transmitting significant information to authorized objects while repudiating access to not allowable ones. Through inserting secret information by an

ISSN: 1975-0080 IJMUE

audio signal as a cover medium, the actual presence of secret information is hidden away throughout communication. This is a serious and energetic subject in some applications for instance battlefield communications plus banking dealings. Executable files (EXE) are possibly the greatest normally used one. They are vital part of each application, game, program, and OS. These files enclose exact complex executable code of program, which make it appropriate to performance by way of a cover object [10].

Finally In image steganography, the cover entity is an image. Usually, in this method pixel strengths are used to hide the information. The rest of the paper is organized as follows: Section 2 explains the related works. Section 3 explains the steganography methods. Section 4 shows the evaluation of different methods, and Section 5 concludes the work of this paper.

2. Related Work

V. Lokeswara Reddy *et al*. [11] explains the LSB Embedding technique and Presents the evaluation for various file formats. The Least Significant Bit (LSB) embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format

Swati Gupta and Deepti Gupta [12] discourse several kinds of text -Steganography methods. There are diverse approaches of Text Steganography. The authors designate it one by one for hiding secret information in text. Diverse applications have dissimilar requirements of the Text Steganography method used. In This paper a mutual application that needs together absolute invisibility plus great secret data get hidden was described.

Rana *et al.* [13] inclines to give a summary of image steganography, its use sand methods. It also attempts to recognize the necessities of a respectable steganographical go Richmond briefly reflects on which steganographic methods are further appropriate for which applications.

Bhattacharyya and Gautam Sanyal [14] present a novel transform field image stenographic method DWTDM where secret data is entrenched in contiguous DWT coefficient differences. The dynamic variety of the DWT difference measured while mining of data which results an effective plus strong stenographic method which can evade several image attacks and works effortlessly well for both uncompressed in addition to compressed area.

Bin Li *et al.* [15] provides an investigation on steganography and steganalysis for digital images, mostly covering the essential ideas, the development of steganographic approaches for images in spatial representation and in JPEG format, and the progress of the corresponding steganalytic structures. Some normally used strategies for refining steganographic security and attractive steganalytic ability are summarized.

Gurmeet Kaur and Aarti Kochhar[16] create a relative analysis to establish the efficiency of the future methods. The efficiency of the proposed approaches has been predictable by calculating Mean square error (abbreviation as MSE) in addition to Peak Signal to Noise Ratio (abbreviation as PSNR).

3. Steganography Methods

Steganography can be used for main categories of many file formats like Text, images, audio/video. The main categories of file formats or signals that can be efficiently used for steganography is shown in Figure 1.

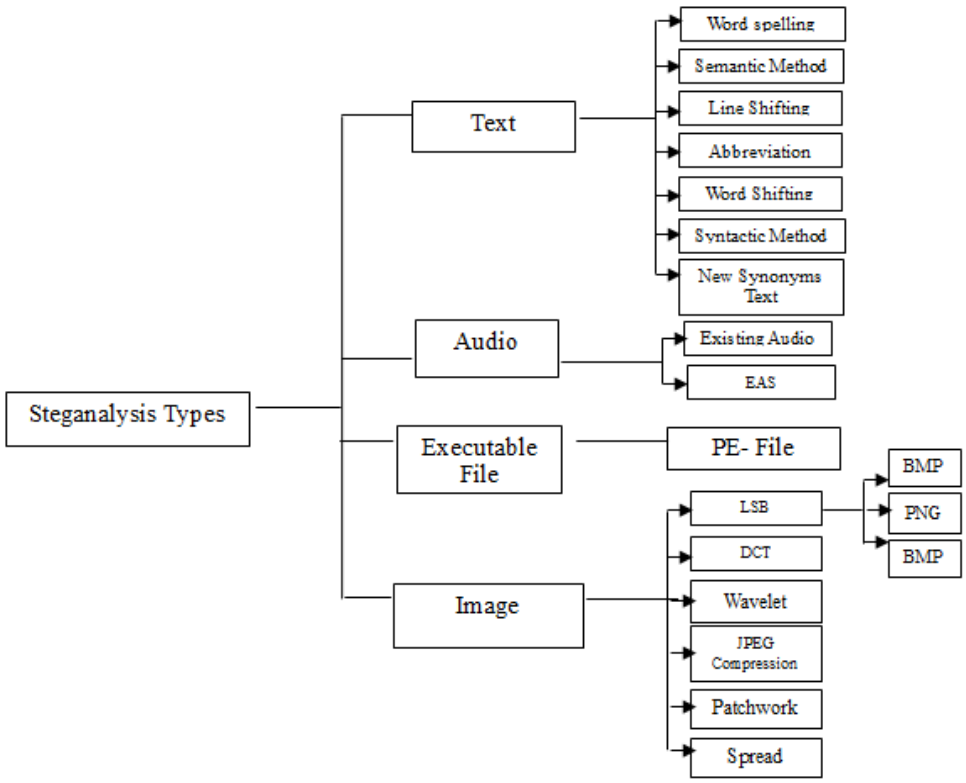

Figure 1. Steganographic Techniques

3.1. Text Steganography Methods

Text -Steganography is most difficult kind of – Steganography, This is due to the lack of redundant information in a text file, while there is a lot of redundancy in a picture or a sound file.

A. Word Spelling

This process can be used pertaining to disappearing files inside British Word. With this technique term punctuation inside United States usually are intended completely different from UK British. As an example: “Center” have different words inside United States (Center) and also UK (Centre). This process pays to for that location where by both equally all of US &UK sort terms punctuation a smaller amount applied. With this technique, our files obtain hide in the event that no person recognize both equally technique, however effortlessly detectable. This is because there is small difference involving word punctuation associated with United states and also UK, like inside all of US (Dialog) and also BRITISH (Dialogue), small difference associated with “u” and also "e" simply, which often obtain effortlessly detectable[17]. Table.1 List of some words which have different spelling in UK and US.

Table 1. List of Some Words which have Different Spelling in UK and US

American English	British English
Favorite	Favourite
Criticize	Criticise
Fulfill	Filfil

Center	Centre
Dialog	Dialogue
Medieval	Mediaeval
Check	Cheque
Defense	Defence
Tire	Tyre

B. Semantic Method

Using this method resembles concept punctuation technique. But small modify is usually, in this particular technique you can use synonym connected with words and phrases is employed for sure words and phrases in so doing the knowledge is usually disguised inside texting[18].

C. Line Shifting

In this process, the particular traces regarding wording tend to be vertically moved to some extent (and data will be concealed by setting up a one of a kind shape of some sort of wording.

This specific instrument regarding range analysis and also needed changes will probably is presented to eliminate the particular concealed data [19].

D. Abbreviation

Yet another method for hiding details with Text message Steganography is actually the use of abbreviation. Within this approach, almost no details hidden in the word, as an example, just few bytes involving files can be hiding in the word [20].

E. Word Shifting

Within this procedure, by means of shifting words flat and also by means of adjusting mileage between words, details tend to be disguised within this word [21].

F. Syntactic Method

In this technique, by Positioning a few punctuation symptoms such as whole quit (.) along with comma (,) in appropriate place, it's possible to disguise details in a very wording document. This process involves determining appropriate place or even positioning punctuation symptoms [22].

G. New Synonym Text

Simple thought of this process is based on Expression Spelling approach in some degree however different also. Throughout Expression spelling approach, there is little change with spelling however in Brand new Synonym Technique, different phrase used by same dat. throughout the English language several phrases possess different expression with US and also UK. As an example, “rubber” possesses different expression with UK (eraser) and also US (rubber)[20]. This kind of process is actually much more effective next phrase spelling approach, due to the fact within this approach phrases possess different terms, which in turn are unable to identify easily. Throughout phrase spelling approach, phrases are usually associated with different spelling like with US (tire) and also UK (tyre). This big difference is actually of a single mail just, easily detectable next Brand new Synonym Word Technique [23]. Table 2 lists some of words which have different terms in UK and US

Table 2. List of Some Words which have Different Terms in UK and US

American English	British English
Account	Bill
Candy	Sweets
Closet	Cupboard
Faculty	Staff
Fall	Autumn
Gas	Petrol
Incorporated	Limited
Mail	Post
Movie	Film
Package	Parcel
Soccer	Football
Stove	Cooke

Finally, each one of the previous strategies has its own advantages and disadvantages that can be summarized in Table 3.

Table 3. Comparative Analysis of Text Steganography Strategies

Strategy	Merits	Demerits
Word Spelling	A good technique for data hiding not only for electronic document but moreover for printing text ,In this technique, hidden data is not damaged	It is less secure than new synonyms text technique since little modification in spelling not hides data accurately
Semantic method	This technique is better than other approaches, because that cannot distinguish through retyping or by OCR programs	Clever reader which has enormous information of words their synonyms or antonyms can realize it
Line shifting	This technique is appropriate only for printed text .In printed text OCR (character recognition) not ever used	As soon as OCR applies the hidden information gets damaged
Semantic method	This technique is better than further approaches, because that cannot distinguish through retyping or using OCR programs	Clever reader which has massive information of words their synonyms or antonyms can notice it
Word shifting	It is better and further operative for use with files because they are less good-looking to the reader's Consideration. It's size is around on bit per word	it have a large problem which is the capability to destroy the watermark is very high when retyping or printing besides they are obvious through OCR
Syntactic Method	The quantity of evidence to hidden the method is small	Clever reader can discover hidden data simply
New Synonym Text	This is best technique between above approaches because in this technique it use diverse terms of words that hide data correctly	This kind of technique is slight bit time consuming because it gets exploration word through word besides substitute it until the result will be gotten.

3.2. Audio-Steganography

In audio steganography it's captivating to offer a respectable, effectual technique for hiding the data from hackers and sent to the destination in a safer method [24].

3.2.1. Least Significant Bit (LSB) Coding

Least significant bit coding is the easiest and humblest technique to hide secret data in a digital audio. Through substituting the least significant bit of every sample words by a bit of the secret data, this technique licenses a big size of secret data to be entrenched. Using LSB is probable, as alterations will naturally not generate noticeable deviations to the sounds. Additional technique includes taking benefit of human sound system boundaries. It is probable to encode messages via frequencies that are inaudible to the human ear. Using several frequencies exceeding 20.000 Hz, messages can be hidden inside sound files and will not be detected by human authorizations [25].

3.2.2. Parity Coding

In this method, audio signal is broken down into distinct parts of samples and hide the secret message in the parity bit of every sample part. If the parity bit of a sample part does not match the secret message bit to be embedded, the LSB of one of the samples in the part is inverted. Consequently, this will give a extensive range of choices on where to hide the secret bit, and will preserve the modification in the signal further unobservable [26].

3.2.3. Phase Coding

This method is based on the realism that, unlike noises, audio phase components are invisible to the human ear. Relatively than adding noises, this method encodes the secret data bits to phase shifts in the phase spectrum of the audio signal, achieving inaudible encodings in terms of signal-to-noise ratio [27]. In this method, the phase of an initial audio part is replaced with a reference phase that denotes the data. Following segments phase is changed back to preserve the comparative phase among parts. This method, when appropriate, is one of the greatest effective audio steganographic approaches in terms of SNR. When the phase relation among every frequency component is melodramatically altered, obvious phase dispersion will happen. In contrast, on condition that the modification of the phase is small enough, an inaudible steganography can be talented [28].

3.2.4. Spread Spectrum

In the arena of audio steganography, essential spread spectrum abbreviation as (SS) methods attempts to allocate secret data through the frequency spectrum of the audio signal to the extreme possible level. This is alike to applying LSB coding through spreading the secret data bits over the whole audio signal. Yet, different from LSB coding, this method spread the secret bits over the frequency spectrum of the audio media through using a code that is not dependent on the honest signal. Therefore, the consequential signal will exploit a bandwidth wider than what is fundamentally needed for communication [29].

3.2.5 Echo Hiding

In this method, secret data is inserted into an audio medium via presenting an echo into the discrete signal. Comparable to SS method, it also suggestions benefits as it permits high data communication rates plus suggestions greater toughness compared to the earlier noise-inducing methods[30].

3.2.6. Existing Audio Steganography Systems

Existing audio steganography systems have poor interface, very low level execution, difficult to comprehend and legal only for certain audio formats through limited message size. The problems of the existing system can be summarized [31]:

1. The LSB algorithm in the existing system is not effective since it hides the message in successive bytes received from audio files.
2. Assortment of audio formats is limited to one (merely wave file).
3. Non-Provision in term of encryption key plus sending the file to the destination.
4. Length of the message is restricted to 500 characters.
5. Nonappearance of frequency charts to demonstration the distinctions.
6. Absence in good user interface.
7. Consume much time to encode in addition to decode.
8. Operator needs to realize better to recognize the procedures.
9. It difficulty get up when more message to be encoded

3.2.7. Enhanced Audio Steganography (EAS) system

These drawbacks in the existing system can be overwhelmed by Enhanced Audio Steganography abbreviation as (EAS) which is an audio Steganography plus cryptography based system that guarantees secure data transfer between the source and destination. EAS uses most influential encryption procedure in the first level of security, which is very multifaceted to break. In the second level it uses a further influential adapted LSB procedure to encode the message into audio. It achieves bit level operation to encode the message.

However it is well controlled software it has been restricted to certain limitations. The superiority of sound depends on the size of the audio which the user chooses besides length of the message. However it demonstrations bit level nonconformities in the frequency chart, as a whole the modification in the audio cannot be determined [32]. The chief two features of this scheme are, File size doesn't modification after encoding in addition to it is bit level management; henceforth the sound differences cannot be determined via some present software. This system has the following benefits [33]:

1. Diverse Audio formats are supported via this system.
2. Provision of encryption key besides achieves simple encryption procedure.
3. The encryption key is adapted by a strong procedure to get a novel key, which is used to encrypt the message. Consequently even if the key is known for an intruder, he cannot disruption the code with that key.
4. Presence of frequency chart to demonstration the differences that assistances the operator to control.
5. Ingesting of time to encode and decode is reduced.
6. Provision of sending the file to the destination is given so that after encoding the operator can send the file by giving destination IP address.

3.3. Executable File Steganography

The (EXE files) are one of the greatest vital files in operating systems besides systems designed via developers , therefore hiding information in these types of file is the basic objective for this approach, because most users of several system cannot adjust or adapt the content of this type. In this method, it's probable to hide information inside image page of execution file to make sure modifications made to the file will not be noticed through universe then the functionality of this type of file is still functioning after hiding procedure. Temporarily, since the cover file might be used to recognize hiding information, overwhelming this dilemma can be done via using this type of file as a cover file [35].

3.3.1. Portable Executable File (PE-FILE)

The Program Loader that is a subclass of the Windows System assumes the loading executable files keen on a virtual memory, thus the executable files have the format that the Program Loader can recognize, and then the format is named PE (Portable

Executable). It is essential to recognize the PE format in order to recognize the new approaches for hiding information in this type [36].

3.3.2. Characteristics of Executable Files

The features of the Executable file does not have a standard size, like other files, for instance the image file (BMP) the size of this file is among (2-10 MB), Other example is the text file, the size frequently is less than 2 MB. The features of files can be used as a cover; it found that lacks satisfactory size to aid as a cover for information to be hidden. For these types of the Executable file, it has indeterminate size; it can be 650 MB similar as window setup File or 12 MB for instance installation file of multi-media players. For taking benefit of this feature (disparity size) make it a appropriate setting for secreting information deprived of detect the file from attacker in addition to realize hidden information in this type of file[37].

3.3.3. Executable Files System Concept

The chief idea of this system can be summarized as hiding the password or some information beyond the end of an executable file so there is no function or routine such as (open, read, write, and close-file) in the operating system to excerpt it. This operation can be achieved in two substitute approaches:

First approach achieved by building the file handling process individually of the operating system file handling routines. Yet, in this situation, canceling the existing file handling routines and developing a new function will be performed. This approach needs the customer to install the system application manually [35].

Second approach achieved by emerging the file handling functions subject on the existing file handling routines. This approach can be achieved remotely. The merit of the first method is it doesn't need some further functions, which can be recognized through the analysts while the drawback is that it needs to be installed. The merit of the second method is it can be implemented remotely and appropriate for networks plus the internet applications [38].

3.3.4. Executable Files System Features

This file system type has the following features:

First, The hiding operation inside image page of EXE file using the statistical procedure growths the level of security for the information hiding since the data which is entrenched inside the this file is not embed straight of EXE file, it will be hiding inside image page of this file. Consequently the attacker cannot be predicting the information hidden [39]. Secondly, a cover file can be implemented generally after hiding operation. Since the hidden information previously hide in the image page inside (.exe file) and so cannot be operated as the (.exe file), consequently, the cover file still usual, working usually and not effected [40]. Finally, a virus detection programmer' can't distinguish such as files, the attitude of antivirus check is examination from beginning to end [35]. When examination this type of files through antivirus, will checked it from beginning to end of it [36].

3.4. Image Steganography

Image steganography emphases on several approaches to apply on the images. Different types of images Depending on the number of bits in a pixel (such as black and white, gray and color images) are used to hide the message [41].

3.4.1. Data Hiding by LSB

One of the mutual procedures is based on deploying the least-significant-bit (LSB) through straight substituting the LSBs of the cover-image through the message bits. This approach naturally realizes high capacity but inappropriately LSB insertion is susceptible to minor image employment such as cropping besides compression [42].

3.4.1.1 LSB in BMP

The BMP file an image file format used to store bitmap images. Since this type of image is not extensively used the suspicion might arise, if it is conveyed with an LSB stego. This type of image is accomplished of hiding quite a great message. LSB in BMP is most appropriate for applications, where the emphasis is on the amount of information to be conveyed and not on the privacy of that information. If further number of bits is changed, it can result in a larger opportunity that the changed bits can be seen through the human eye. Nevertheless with the LSB the chief objective of Steganography is to permit a message to a receiver without an intruder even knowing that a message is being approved is being accomplished. The chief drawback regarding LSB in this type of image is confidently the distrust that might arise from a very large BMP image being conveyed among parties [43]. LSB in BMP is most suitable for applications where the focus is on the amount of information to be transmitted and not on the secrecy of that information.

3.4.1.2. LSB in PNG

Portable Network Graphics abbreviation as (PNG) is bitmapped images format that occupations lossless data compression. PNG was generated to advance upon and substitute GIF. Meanwhile this type of image is extensively used the distrust might not arise if it is communicated with an LSB stego. This type of image is accomplished of hiding quite a large message. LSB in PNG is most appropriate for applications where the emphasis is on the amount of information to be communicated and not on the privacy of that information [44].

3.4.1.3. LSB in GIF

Graphics interchange format also recognized as GIF is one of the machine independent compressed formats for packing images. Since this type of image only have a bit depth of 8, amount of information that can be hidden is less than with BMP. LSB in this type of image is a very effective algorithm to use when embedding a sensible amount of data in a grayscale image [45].

Most applications that use LSB methods with this type of image have low security because it is probable to detect even reasonable alteration in the image. Explanations to these difficulties could be as following:

1. Category the palette so that the color variance among successive colors is minimized
2. Supplement new colors, which are visually like to the current colors in the palette.
3. Custom Gray scale images.

This consequence in gradual variations in the colors and it is hard to notice. The robust and weak points concerning embedding information in this type of image using LSB are more or less the similar as those of using LSB with BMP. The chief variance is that since this type of image only has a bit depth of 8, the quantity of information that can be hidden is less than with BMP [46]. This type of image is specifically susceptible to statistical – or visual attacks – since the palette processing that has to be done leaves a very sure signature on the image. This method is reliant on the file format as well as the image itself, since an incorrect choice of image can result in the message being visible. LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a greyscale image.

3.4.2. Data Hiding by DCT

DCT based data hiding used in the JPEG compression procedure to transform succeeding 8x8-pixel blocks of the image from spatial domain to 64 DCT coefficients each in another domain called frequency domain. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The alteration of a single DCT coefficient disturbs all 64 image pixels. Since this alteration occurs in the frequency domain and not the spatial domain, there are no obvious visual changes. The merit DCT has over other transforms is the capability to minimize the block-like appearance resulting when the limits between the 8x8 sub-images become visible. The statistical properties of this type of image are also preserved. The difficulty is that this technique only works on JPEG files since it assumes a certain statistical distribution of the cover data that is normally found in this type of image [47].

3.4.3. Data Hiding by Wavelet-based Steganography

It's a new knowledge in the application of wavelets. Yet, the standard procedure of storing in the least significant bits (LSB) of a pixel still applies. The only variance is that the information is stored in the wavelet coefficients of an image, instead of altering bits of the real pixels. The impression is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually destroy the image. Though this thought procedure is essential in most steganographic techniques, the change here is that through storing information in the wavelet coefficients, the modification in the intensities in images will be unnoticeable [48].

3.4.4. Data Hiding by DWTDM Steganography

DWTDM based steganographic image has been confirmed on several attack like noise addition and image compression. Two types of noise specifically Gaussian noise happens from electronic noise in image acquisition system and most difficult with poor lighting circumstances or vary high temperatures and Salt & Pepper noise which is naturally produced by malfunctioning pixel element in camera sensors, defective memory locations, or timing errors in digitization procedure has been added to the Stego images before the extraction process happen and the last results is quite promising and has given a satisfied performance[49]. Table 4 shows contrast of DWTDM through further spatial domain approaches, while Table 5 shows contrast of DWTDM through further DCT domain.

Table 4. Contrast of DWTDM through Further Spatial Domain Approaches

LSB	DWTDM
• All are spatial domain methods. Data can be simply tractable from raw pixel intensities besides falter from greatest kinds of image attacks.	• Transform domain technique, extraction from wavelet coefficients which is far more complex but robust against some type of image attacks.
• Works only on uncompressed image type.	• Works on together uncompressed besides compressed image types.
• For assessing performance only MSE and PSNR has been combined.	• Except MSE and PSNR several other image similarity metric parameters has been combined.
• Security of the hidden data not verified.	• Security of the hidden data is very high.

Table 5. Contrast of DWTDM through further DCT Domain

DCT	DWTDM
• All are transform domain methods works via adjust the DCT coefficients.	• Transform domain technique works via adjust wavelet coefficients.
• 1 bit mapping method means embedding capacity is lower.	• 2 bit mapping method means embedding capacity is high.
• Works only on uncompressed image type.	• Works on together uncompressed and compressed image type.
• Security of the hidden data not verified.	• Security of the hidden data is very high.
• Not verified against several image attacks	• Tested against several image attacks such as noise addition, compression, … *etc.*

3.4.5. Data Hiding by JPEG Compression

The procedure of embedding information throughout JPEG compression results in a stego image with a high level of invisibility, meanwhile the embedding happen in the transform domain. JPEG is the greatest general image file format on the Internet and the image sizes are small because of the compression, therefore making it the least suspicious procedure to use. Yet, the procedure of the compression is a very mathematical procedure, making it further difficult to implement.

The JPEG file format can be used for most applications of steganography, but is especially suitable for images that have to be communicated over an open systems environment like the Internet [50].

3.4.6. Patchwork

The major difficulty of this method is the small quantity of information that can be hidden in one image. This property can be altered to accommodate further information but one may have to expense the secrecy of the information. Patchwork's chief benefit, however, is its strength in contrast to malicious or accidental image manipulation. A stego image using patchwork be cropped or rotated, certain of the message data may be missing but since the message is frequently embedded in the image, greatest of the information will survive. Patchwork is most suitable for transmitting a small amount of very sensitive information [51].

3.4.7. Spread Spectrum

This technique satisfies greatest necessities and is especially robust in contrast to statistical attacks, since the hidden information is scattered through the image, while not altering the statistical properties. This technique can be used for greatest steganography applications, although it's highly mathematical and intricate method may evidence too much [52].

4. Evaluation Criteria

So as to rationally evaluate the performance of several types of steganographic and steganalytic approaches, it is essential to discuss certain criteria that are suitable to the popular. Furthermore, the evaluation criteria may also lead us to the correct way to improve the techniques [45].in this part a brief description for some criteria will be description:

1. **Invisibility:** The invisibility of a steganography procedure is the first and primary obligation; meanwhile the strength of steganography lies in its capability to be unobserved through the human eye. The instant that one can see that an image has been interfered with, the procedure is cooperated [49].
2. **Payload capacity:** Distinct from watermarking, which desires to embed only a small amount of copyright information, steganography purposes at hidden communication and consequently requires adequate embedding capacity. Information through applying statistical tests on image data. Several steganography procedures leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to permit via a warden deprived of being detected, a steganography procedure must not leave such a mark in the image as be statistically important [51].
3. **Robustness against image manipulation:** In the communication of a stego image via trusted systems, the image may undergo variations via an active warden in an effort to remove hidden information. Image operation, for instance cropping or rotating, can be achieved on the image before it reaches its destination. Subject on the manner in which the message is embedded, these operations may destroy the hidden message [51].
4. **Independent of file format:** With several different image file formats used on the Internet, it might seem doubtful that only one type of file format is unceasingly connected among two parties. The greatest influential steganography procedures possess the capability to embed information in several type of file. This moreover solves the problem of not always being able to discovery appropriate image at the correct instant, in the correct format to use as a cover image [50].
5. **Unsuspicious files:** This condition contains all features of a steganography procedure that may result in images that are not used usually and may cause distrust. Irregular file size, for instance, is one property of an image that can result in further examination of the image via a warden [47].
6. **Peak Signal-to-Noise Ratio (PSNR):** is the ratio amid a signal's maximum power and the power of the signal's noise. Engineers normally use the PSNR to measure the quality of reassembled signals that have been compressed. Signals can have a varied dynamic range, so PSNR is frequently expressed in decibels [48]. This type of criteria measures the quality of the image via associating the cover image with the stego-image

$$PSNR = 20 \log_{10} \frac{255}{\sqrt[2]{MSE}} \quad (1)$$

The PSNR is used to evaluate the quality of the stego-image after embedding the secret message in the cover [45].

7. **Mean-Squared Error:** In statistics, the mean squared error abbreviation as (MSE) of an estimator is one of several methods to quantify the variance among values implied via an estimator and the true values of the quantity being estimated. This type of criteria is a risk function, corresponding to the predictable value of the squared error loss or quadratic loss. The mean-squared error (MSE) among two images $I_1(m, n)$ and $I_2(m, n)$ can be agreed in:

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

Where *M* and *N* are the number of rows and columns in the input images, correspondingly [48].

8. **Perceptibility:** It defines the capability of a third party (not the intended recipient) to visually detect the attendance of hidden information in the stego image. The embedding procedure is unnoticeable when used on a specific image if an innocent third party, concerned in the content of the cover image, is ignorant of the presence of the payload. Fundamentally this requires that the embedding procedure not destroy the visual quality of the cover image [50].

9. **Security:** Steganography may undergo from several active or passive attacks, congruently in the prisoner's problem when Wendy entertainments as an active or passive warden. If the presence of the secret message can only be estimated with a probability not higher than random predicting in the presence of some steganalytic systems, steganography may be measured secure under such steganalytic systems [52].
10. **Imperceptibility:** Stego images should not have plain visual relics. Below the same level of security and capacity, the higher the reliability of the stego image is the better. If the ensuing stego image seems innocuous enough, one can trust this requirement to be satisfied well for the warden not having the original cover image to compare [53].

5. Evaluation of Different Techniques

For text steganography, Table 6 summarizes these methods with their benefits and drawbacks.

Table 6. Evaluation of Text Steganography Methods

Strategy	Robustness by OCR	Security	Visibility
Word Spelling	Medium	Low	High
Semantic method	High	Low	Medium
Line shifting	Low	Low	Medium
Semantic method	High	Low	Medium
Word shifting	High	Low	High
Syntactic Method	Medium	Low	High
New Synonym Text	High	High	Low

For audio steganographic approach, Table 7 tabularizes the comparison of audio signal steganographic techniques based on the proposed evaluation criteria.

Table 7. Evaluation of Audio Steganography Methods

Technique	Payload capacity	Imperceptibility	Robustness
LSB	High	Medium	Low
Parity coding	Medium	Medium	Low
Phase coding	Low	High	High
Spread spectrum	High	Low	High
Echo hiding	High	Low	Medium

In executable file format the characteristics of executable file can be summarized in Table 8.

Table 8. Executable File Characteristics

Benefit	Limitation
• The hidden information will be avoiding explanations because most anti-virus system do not permit direct write in executable file. • The cover file immobile natural, working ordinarily. • Growing the degree of security (the attackers cannot be predicting the information).	• Insertion of data maybe damaged because of file is very multifaceted depend on multi header and addressing. • It's essential to know the PE format besides RVA which is an addressable type used in the PE in order to recognize the new approaches for hidden information in the PE.

• Flexible and very useful in hiding several type of data. • The characteristic of excitable file does not have standard size.	

The analysis of LSB based and DCT based steganography has been done on basis of restrictions like PSNR, MSE, Processing time and security as shown in Table 9.

Table 9. Contrast of LSB through DCT Domain

Features	LSB	DCT
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	High	Medium
MSE	Less	Medium

From the results it is clear that as PSNR in LSB is the best but as we know that security is much more significant in today's communication system. So security wise DCT is the best. As shown in Table 10.

Table 10. Contrast of DWTDM through Other DCT Domain

	LSB in BMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

*Depends on cover image used

The stages at which the procedures satisfy the necessities are distinct as high, medium and low. A high level means that the procedure wholly satisfies the obligation, whereas a low level shows that the procedure has a weakness in this obligation. A medium level specifies that the obligation depends on outside effects, for instance the cover image used. LSB in GIF images has the possible of hiding a large message, but only when the most appropriate cover image has been selected.

Unfortunately in the algorithms that are evaluated here, there is not one algorithm that satisfies all of the requirements. Thus a trade-off will exist in most cases, depending on which requirements are more important for the specific application, as shown in Table 11.

Table 11. Contrast of LSB Method for Several File Formats

	LSB in BMP	LSB in GIF	LSP in PNG
Percentage distortion les resulting image	High	Medium	High
Invisibility	High	Medium	Medium
Steganalysis detection	Low	Low	Low
Image manipulation	Low	Low	Low
Amount of embedded data	High	Medium	Medium

Payload capacity	High	Medium	Medium
Independent of file format	Low	Low	High

In Table 12 we show the evaluation of different image file format.

Table 12. A Contrast of LSB in BMP, GIF, GPEG Compression, Patchwork, and Spread Spectrum

	LSB in BMP	**LSB in GIF**	**JPEG compression**	**Patchwork**	**Spread spectrum**
Invisibility	High	Medium	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

6. Conclusion

Information hiding is a subdivision of computer science which contracts with hiding data object or function details. Numerous researchers are working in this part to advance the effectiveness of steganographic procedures.

In this paper, a comparative study of the current-state-of-the-art literature in common multimedia steganography techniques and approaches is obtainable. In an attempt to disclose their capabilities in ensuring secure communications, we discussed their strengthes as well as limitations.

A comparison as well as a performance evaluation (*i.e*., imperceptibility and steganalysis) for the reviewed techniques has been also obtainable.

From our point of view, the diversity and large number of existing common multimedia steganography techniques expand application possibilities. The advantage on using one technique over another one depends on the application constraints in use and its requirement for hiding capacity, embedded data security level and encountered attacks resistance.

References

[1] J. T. L. Philjon and N. V. Rao, ‘‘Metamorphic Cryptography - A Paradox between Cryptography and steganography Using Dynamic Encryption’’, IEEE -International Conference on Recent Trends in Information Technology, ICRTIT, **(2011)**.
[2] G. C. Kessler, “Steganography: Hiding Data within Data”, http://www.garykessler.net/library/steganography.html, **(2001)**.
[3] M. M. Amin, M. Salleh and S. Ibrahim, “Information Hiding Using Steganography”, 4th National Conference on Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, **(2003)**, pp. 21-25.
[4] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information hiding—A Survey,” Proceeding IEEE (Special Issue on Identification and Protection of Multimedia Information), vol. 87, **(1999)**, pp. 1062-1078.
[5] P. Moulin and J. A. O’sullivan, “Information-theoretic analysis of information hiding”, preprint, **(2001)**.
[6] T. Moerland, “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf, **(2013)**.

[7] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, **(1999)**, pp. 1062-1078.
[8] B. Mehboob and R. A. Faruqui, "A Steganography Implementation", IEEE, **(2008)**.
[9] K. Alla and R. S. R. Prasad, "A New Approach to Telugu Text Steganography", IEEE Symposium on Wireless Technology and Applications, **(2011)**, pp. 25-28.
[10] S. K. Bandyopadhyay, D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, **(2008)**, pp. 105-114.
[11] V. L. Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications, vol. 2, no. 5, **(2011)**, pp. 868-872.
[12] M. S. Rana, B. S. Sangwan and J. S. J. Souvik, "Art of Hiding: An Introduction to Steganography", International Journal of Engineering and Computer Science, vol. 1, no. 1, **(2012)**, pp. 11-22.
[13] S. Gupta and D. Gupta, "Text -Steganography: Review Study & Comparative Analysis", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 2, no. 5, **(2011)**, pp. 2060-2062.
[14] S. Bhattacharyya and G. Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)", International Journal Computer Network and Information Security, vol. 7, **(2012)**, pp. 27-40.
[15] B. Li, J. He, J. Huang and Y. Q. Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, **(2011)**.
[16] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging Technologies with Latest Trends, vol. 4, no. 1, **(2012)**, pp. 35-41.
[17] M. H. S. Shahreza and M. S. Shahreza, "A new approach to persian/arabic text steganography", Proceeding 5th Int. Conf. Computer and Information Science, Washington, **(2006)**, pp. 310-315.
[18] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm Based On Word Classification And Inter-Word Space Statistiocs", Proceeding Of The Seventh International Conference On Document Analysis And Recognition, **(2003)**, pp. 775-779.
[19] M. S. Shahreza and M. H. S. Shahreza, "Text Steganography in Chat", 1-4244-1007/07 ©, IEEE, **(2007)**.
[20] M. S. Shahreza, "Text Steganography by Changing Words Spelling", ISBN 978-89-5519-136-3, 2008, ICACT, **(2008)**.
[21] M. Shirali-Shahreza, M. H. Shirali-Shahreza, "Text steganography in SMS," Proc. Int. Conf. Convergence Information Technology, Washington, **2007**, pp. 2260-2265.
[22] K.F. Rafat, "Enhanced text steganography in SMS," Proc. of the 2nd Int. Conf. Computer, Control and Communication, Karachi, **2009**, pp.1-6.
[23] Shraddha Dulera, Devesh Jinwala and Aroop Dasgupta, "EXPERIMENTING WITH THE NOVEL APPROACHES IN TEXT STEGANOGRAPHY" , International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November **2011**.
[24] Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography" FIN-90014 University of Oulu, Finland ,**2002**.
[25] Nutzinger, M., C. Fabian, and M. Marschalek,"Secure Hybrid Spread Spectrum System for Steganography in Additive Media", in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. **2010**.
[26] Shahreza, S.S. and M.T.M. Shalmani,"High capacity error free wavelet Domain Speech Steganography in Acoustics", Speech and Signal Processing, IEEE International Conference on **2008**.
[27] Bhattacharyya, D., et al., "Hiding Data in Audio Signal, "Advanced Communication and Networking **2010**, Springer Berlin Heidelberg, pp. 23-29.
[28] Chungyi, W. and W. Quincy,"Information Hiding in Real- Time VoIP Streams",In Multimedia ISM Ninth IEEE International Symposium on. **2007**.
[29] Kumar S. B., D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, **2008**, pp. 105-114.
[30] Bender, W., W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques for data hiding", IBM Systems Journal, Volume 39, Issue 3-4, July **2000**, pp. 547 – 568.
[31] Vapnik, V.N. "Statistical Learning Theory". John Wiley and Sons, New York, USA,**1998**.
[32] Dutta, P. Bhattacharyya, D. and Kim, T.,"Data Hiding in Audio Signal: A Review" ,International Journal of Database Theory and Application Vol. 2, No. 2, June **2009**.
[33] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream", Technical report of IEICE, ISEC, vol.106 pp.15-22, September **2006**.
[34] Min Wu, Bede Liu. "Multimedia Data Hiding", Springer- Verlag New York, **2003**.
[35] A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "New Technique of Hidden Data in PE-File with in Unused Area One", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198,**2009**, pp 669-678.

[36] Ramanpreet Kaur, Prof.Baljit Singh "Survey and Analysis of Various Steganographic Techniques" international Journal Of Engineering Science & Advanced Technology Volume-2 , Issue-3, May-June **2012**.
[37] A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "New Technique of Hidden Data in PE-File with in Unused Area One", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, **2009**, pp 669-678.
[38] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Academic and Scientific Research Organizations (WASET), International Conference on Computer, Electrical, and Systems Science, and Engineering (CCESSE09), ISSN:2070-3724,**2009**.
[39] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "New Approach of Hidden Data in the portable Executable File without Change the Size of Carrier File Using Distortion Techniques", Academic and Scientific Research Organizations (WASET), International Conference on Computer, Electrical, and Systems Science, and Engineering(CCESSE09), , ISSN:2070-3724,**2009**.
[40] B. B. Zaidan, A. A. Zaidan, F. Othman and A. Rahem, "Novel Approach of Hidden Data in the (Unused Area 1 within EXE File) Using Computation Between Cryptography and Steganography", Academic and Scientific Research Organizations (WASET), International Conference on Cryptography, Coding and Information Security (ICCCIS09), Session 24, ISSN: 2070-3740, Vol.41, **(2009)**.
[41] A. A. Shejul and U. L. Kulkarni, "A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform", International Journal of Computer Theory and Engineering, vol. 3, no. 1, **(2011)**, pp. 16-22.
[42] D. Yan, R. Wang, X. Yu and J. Zhu, "Steganography for MP3 audio by exploiting the rule of window switching", Computers & Security, Elsevier publications, vol. 31, **(2012)**, pp. 704-716.
[43] Z. Wang, A. C. Bovik and H. R. Sheikh, "Image Quality Assessment: From Error Visibility to Structure Similarity",IEEE Transactions on image processing, Vol. 13, No. 4, **2004**. pp. 600-612.
[44] C. S. Varnan, A. Jagan, J. Kaur, D. Jyoti and D. S. Rao, "Image Quality Assessment Techniques in Spatial Domain", IJCST, vol. 2, no. 3, **(2011)**, pp. 177-184.
[45] M. I. Khalil, "Image steganography: Hiding short messages within digital images", JCS & T, vol. 11, no. 2, pp. 68-73.
[46] Y. Yalman and Đ. Ertürk, "A new color image quality measure based on YUV transformation and PSNR for human vision system", **(2011)**, pp. 1-18.
[47] J. J. G. Hernandez, R. P. Michel, C. F. Uribe and R. Cumplido, "High payload data-hiding in audio signals based on a modified OFDM approach", Expert Systems with Applications, Elsevier publications, vol. 40, **(2013)**, pp. 3055–3064.
[48] V. Kumar and D. Kumar, "Performance Evaluation of DWT based Steganography", IEEE 2nd International Advance Computing Conference, **(2010)**, pp. 223-228.
[49] A. Kanso and H. S. Own., "Steganographic algorithm based on a chaotic map", Communication Nonlinear Science Numerical Simulation", vol. 17, **(2012)**, pp. 3287–3302.
[50] S. Geetha, V. Kabilan, S. P. Chockalingam and N. Kamaraj, "Varying radix numeral system based adaptive image steganography", Information Processing Letters, vol. 111, **(2011)**, pp. 792–797.
[51] T. C. Lu, C. C. Chang and Y. H. Huang, "High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting", Springer, **(2013)**.
[52] K. H. Jung and K. Y. Yoo, "Data hiding using edge detector for scalable images", Springer, **(2012)**.
[53] Shivani, V. Yadav and S. Batham, "An Approach to Image Steganography using Strength of Indexed Based Chaotic Sequence", SSCC (Springer), **(2014)**.

