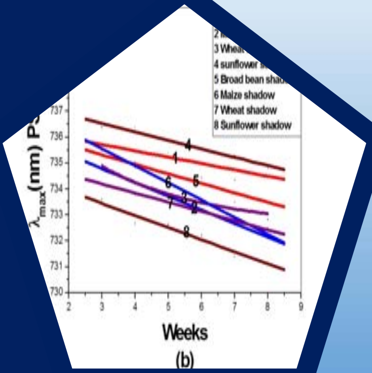
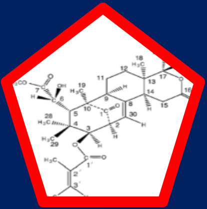
Journal of Faculty of Sciences

A Refereed Scientific Journal
Faculty of Pure and Applied Sciences
International University of Africa
Volume No. 5 , December , 2018





ISSN: 1858 – 513x

Journal of Faculty of Sciences

Refereed Scientific Journal

Faculty of Pure and Applied Sciences

International University of Africa

Volume No. 5, December, 2018

Survey of Steganography Techniques

Mohammed Salah AbdalazizKhaleel[1*],SaifEldinFattoh Osman[2*]

IUA –Computer Science Department, Khartoum,Sudan
Emirates College of Technology, Khartoum, Sudan
**Corresponding address: Mohammedkh33@hotmail.com,Saifefatoh@hotmail*

ABSTRACT

Digital communication has become major means of communication today. However a lot of applications are internet-basedwithhigh risk of attacks, if they are not secured. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to be protected against unauthorized access. Thus, and these are some of the reason that has led to development of data hiding or data encryptions.Steganography was created as a technique for securing the secrecy of communication and many different methods have been developed to hide data in order to conceal their very existence.The goal of this paperis to survey different steganography techniqueswhich are usedto enhance communication security over an open channel.

Keywords: Steganography, plaintext, integrity, Steganalysis, Confidentiality.

1. INTRODUCTION

Due to the development of computers and the increasing of theirneeds in different areas of life and work; the issue of information security has become very importantto the users. Accordingly, many techniques have involved such as Cryptography, Steganography usually abbreviated as(stego), Watermarking ,coding, etc…which are used to hide the data and we are now seeing every day means a new technique or a modern method. Steganography is among the technique that has been receiving attention in recent past years[1].

Steganography and Watermarking are considered as the two main branches of information hiding, theyshare many characteristics,and both describe methods to embed information transparently into a carrier media. They are also differ in a number of ways, Steganography communication is a method that establishes a covered information channel in point-to-point connections (between sender and receiver), While watermarking does not necessarily hide the fact of secret transmission of information from third persons and is usually one –to-many. In addition, the existence of a watermark is often declared openly, and after any attempt to remove or invalidate embedded content, the host become useless. So robustness against malicious attack is the primary Concern is for watermarking. Finally, the most fundamental difference is that watermarking techniques is the host signal, with the embedded are for providing copyright protection. Whereas steganography is about concealing the existence of hidden data in the host signal must be undetectable by human vision. Steganography and Cryptography are closely related. ButSteganography differs fromcryptography, whichis about protecting the content of messages and provides privacy by scrambling message. Both Steganography and Cryptography can be combining to achieve additional security and better protection of the messages. When the steganography fail; the hidden information is revealed and themessage is detected, its content is still of no use and cannot be extracted as it is encrypted using cryptography techniques[2].

Table 1. Comparison of secret communication techniques [3].

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes / No	Yes / No	Yes

Table 1 matches between different data hiding techniques, from this table; Steganographyis more confidential has more integrity and also Unremovability.It is the more powerful.

1.1 HISTORY

Steganography can be defined as the hiding of information by embedding messages. The first steganography technique was developed in ancient Greece around 440 B.C[4].

In this paper we are not intend to cover the whole history of steganography, rather just giving the important land marks. The Greek leaderHistaeus employed an early sortof steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to releasethe secret message, and sending the slave on his way to conveythe message. The receiverwould have the slave’s head to uncover the message. The recipient would reply in the same wayof steganography. In the same period of time, another early versionof steganography was employed. This method involved Demerstus, who wrote a message to the Spartans warning of eminent attacksfrom Xerxes. The message was carved on the wood of wax tablet, and then covered with a fresh layer of wax. This seemingly blank tablet was delivered with its hidden message successfully. Steganography continued development in the early 1600s as Sir Francis Bacon used a variation in type face to carry each bit of the encoding. In the 20th century, invisible inks were widely used techniques. In the Second World War, people used milk, vinegar, fruit juices and urine to write secret messages. When heated, these liquids become shadier and the message could be recited. More recently, the Germans established a technique called the microdot. Microdots arephotographs with the size of a printed period but have the clearness of a standard typewritten page. The microdots where then printed in a letter or on an envelope and being so small, they could be sent unnoticed and intended for transportation by pigeons[4].

1.2 DEFINITIONS

***1.2.1 Steganography*:** is the process of hiding secret messages in an ordinary document. Secrets can be hidden inside all sorts of digital covers such as: text, images, audio, video, Deoxyribonucleic Acid (DNA) for biological data, and more. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the media**.**

***1.2.2 Steganalysis*:** could be simply defined as the methods and processes that are used to detect and defeat steganography by a third party.

***1.2.3 Plaintext*:** is message or databefore it gets encrypted .Data in their normal and readable form.

***1.2.4 Confidentiality*:** Assuring that only authorized parties are able to understand the data.It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm and biometric verification is an option as well. In addition, users can take precautions to minimize the number of places where the information appears, and the number of times it is actually transmitted to complete a required transaction.

***1.2.5 Integrity*:** Ensuring that when a message is sent over a network, the message that arrives is the same as the message that was originally sent. Data must not be changed in transfer, and rules must be followed to ensure that data cannot be modifiedby unlicensedpeople .Also someadditional stepsmust betakento detect any changes in data that might occur as an effectof non-human-caused events such as an ElectroMagnetic Pulse (EMP) or server crash. If an unpredictedchange arises, a backup copy must be existingto return the affected data to its correct state.

1.2.6 Unremovability**:** involve to the file of transmit file can't be remove[3]-[4].

1.3 Steganography

Thetermsteganography derives from the Greek word Stego, which mean covered or secret and graphy means writing or drawing. Therefore, steganography means, plainly, covered writing. The coreobjectiveof steganography is to communicate securely in a completely undetectable mode and to avoid drawing doubtto the transmission of a hidden data. During the process, characteristics of these methodsare to change in the structure and features so as not to be detectableby human eye. Digital images, videos, audio, text files, and other computer files that are usually contain some redundant bytes of information which aren't important; these files can be used as “hosts” or carriers to hide secret messages. After insertinga secret message into the cover-image, a so-called stegoimage is attained. The simplemodel of steganography involvesof Carrier, Secretmessage, embedding with Detectors algorithms and Stego key. The model of steganography is shown in (Fig 1).

Carrier is also recognizedas a cover-object, which embeds the message and works to mask and hide its existence[5].

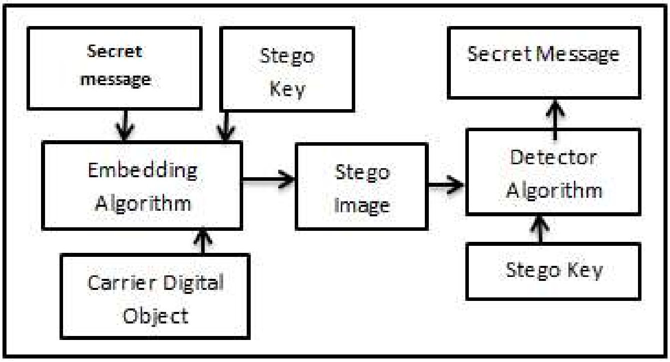


Fig 1.A model of Steganography[5]

2. STEGANALYSIS

Steganalysis in its simplest definition is the process of detecting hidden information inside of a file and identifying steganography by examining various factors of a stego media. The main step of this process is to identify a suspected stego media. Thus if an attacker cannot confirm a hypothesis that a secret message is embedded in a cover, then a system is theoretically secure.

In developing a formal security model for steganography we must assume that an attacker has unlimited computation power and after he has determined whether that media contains hidden message or not and he is able and willing to perform a variety of attacks- as discussed later- in order to recover the message from it.

In the cryptanalysis it is clear that the captured message is encrypted and it definitely contains the hidden message. But in the case of steganalysis this may not be true. The suspected media mayor may not be with a secret message. The steganalysis process starts with a set of suspected information streams. Then the set is summarized with the help of progress statistical methods [6].

2.1 Steganalysis Techniques

The characteristics of electronic media are being altered after hiding any object into that. This can result in the form of degradation in terms of quality or unusual of the media: Steganalysis techniques based on un usual form in the media. For example in the case of Network Steganography unusual pattern is presented in the TCP/IP packet header. If the packet analysis technique of Intrusion Detection System of a network is based on white list pattern (common pattern), then this method of network steganography can be overcome. In the case of Visual detection steganalysis technique a set of stego images are matched with original cover images and note the observable difference. Signature of the hidden message can be derived by matching plenty full images. Cropping or padding of image also is a visual sign of hidden message by cropping or padding blank spaces to fit into fixed size. Variance in file size between cover image and stego images and growth or reduction of unique colors in stego images can also be used in the Visual Detection steganalysis technique [6].

2.2 Steganography Attacks

Steganography attacks involve detecting, extracting and destroying hidden object of the stego media. Steganography attack is followed by steganalysis. There are numerous types of attacks centered on the information available for analysis. Some of these areas shown:

- Known carrier attack: The original cover media and stego media both are existing for analysis.

  Steganography only attack: In this type of attacks, only stego Media is existing for analysis.
- Known message attack: The hidden message is known in this case.
- Known steganography attack: All the cover media, stego media as well as the steganography tool or algorithm, are known [6].

2.3 Tyes of steganography

Steganography can be split into two types:

Steganography can be existing in one of these two categories:

a) Fragile: This category of steganography involves embedding information into a file which is ruinedif the file is modifiedby changing its format or by compression.

b) Robust: Robust marking objects to embed information into a file which cannot effortlessly bedestroyed [6].

3 STEGANOGRAPHY TECHNIQUES

Steganography systems can be congregated by the nature of media used for communication, or by the procedures used for embedding process and extraction process; in this paper we don't care about extraction techniques. As mentioned earlier in this III there are many sorts of media and techniques can be used in order to hide the existence of a secret message, some of these techniques are:

3.1 Imagefile Techniques

Image file is simply a file that displays different colors and intensities of light on different areas of an image.

Using digital images for coding secret messages in is by far the most widely used of allmethods in the digital world of today. This is because it can take advantage of the limited power of the Human Visual System (HVS) and the capability to work on a larger range of image formats. To hide a message within an image file two files are required:

- The file having the image into which the message is supposed to be put in it.
- The file holding the secret message itself.

The implementation of this technique is to select the image file and write the plaintext, which is then hidden behind the image[6].

There are four methods to hide messages in images, they include:

3.1.1 Simple Watermarking[6]

A very simple yet widely used technique for watermarking images is to add a pattern on top of an existing image. Usually this pattern is an image itself - a logo or something similar, which alters the original image.

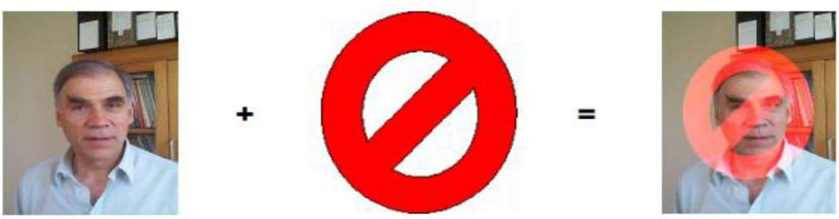


Fig 2.Visible watermarking[6].

In the (Fig2): the pattern is the red middle image while the portrait picture of Dr. Axford is the image being watermarked. In a standard image editor it is possible to merge both images and get a watermarked image. As long as you know the watermark, it is possible to reverse any adverse effects so that the original doesn't need to be kept. This method is only really applicable to watermarking, as the pattern is visible and even without the original watermark, it is possible to remove the pattern from the watermarked image with some effort and skill.

3.1.2 LSB – Least Significant Bit Hiding (Image Hiding)

This method is doubtlessthe easiest way of hiding information in an image and yet it is amazinglyeffective. It serves by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in a JPEG image for example, the following steps would need to be followed:

1. First prepareboth the host image and the image you need to hide.

2. Next indicate the number of bits you desireto hide the secret image in. The host image is more deteriorated when increasing the number of bits used.
3. Now you have to builda new image by mergingthe pixels from both images.

If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types).

Host Pixel: 10110011

Bits used: 4

New Image: 00110000

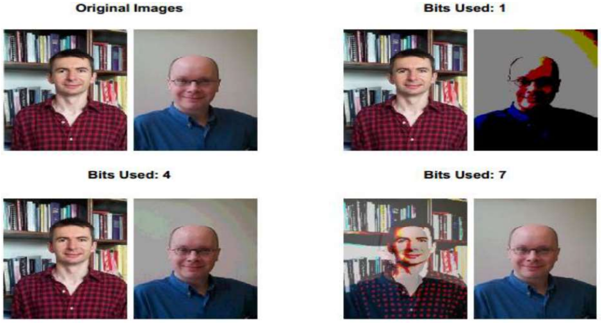


Fig 3.LSB (Image Hiding)[6]

In (Fig3): This method works well when both the host and secret images are given equivalentpriority. When one has significantly has priority than the other, the quality is lost. 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 you need to do is change how the least significant bits are packed into the host image. This technique makes it very easy to find and remove the hidden data [6].Howeverthere is a problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG).

3.1.3 Direct Cosine Transformation

Another steganography technique is to hide data using mathematical functionsfor example Direct Cosine Transformation (DCT). The DCT Algorithm is one of the main components of the JPEG compression technique [7, 8] , it is a losscompression transform.Indeed, JPEG images are becoming abundant on the Internet and JPEG images are high quality color images with good compression .So, it is desirable to use JPEG images across networks such as the Internet. DCT transforms an image from the spatial domain to the frequency domain. It separates the image into portions (or spectral sub-bands) of differing importance (with respect to the image's visualQuality). DCT Algorithm followsnext steps:

1. First the image is dividedinto 8 x 8 squaresof pixels.
2. Next each of these squares is transformed via a DCT, which outputs a multi-dimensional array of 63 coefficients.
3. A quantizes rounds each of these coefficients, which is the compression stage as this is where data is lost.
4. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision.

5. At this stage you should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar.

6. Decompression is done via an inverse DCT .

Hiding via a DCT is useful as someone who just looks at the pixel values of the image would be unaware that anything is amiss. Moreover, a difference between the original data and the recovered data depends on the values and methods used to calculate the DCT.Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust. If you wish to scramblethe bit value 0 in a specific 8 x 8 square of pixels, you can do this by making sure all the coefficients are even, for example by tuningthem. Bit value 1 can be stored by tuningthe coefficients so that they are odd. Thus, a large image can stocksome data that is quite difficult to noticein comparison to the LSB method. This is a very simple method and while it works well in keeping down distortions, it is vulnerable to noise. It can be implemented in the Fig 4[7,9,10].

Original Image Watermarked Image JPEG Compresses

Fig 4. Direct Cosine Transformation[7].

Images can also be processed using fast Fourier transformation and wavelet transformation. While DCT transformations help hide watermark information or general data, they don't do a great job at higher compression levels. The blocky look of highly compressed JPEG files is due to the 8 x 8 blocks used in the transformation process. Wavelet transformations on the other hand are far better at high compression levels and thus increase the level of robustness of the information that is hidden.

3.2 Sound Techniques

The Human Auditory System (HAS) identifies over a range of power greater than one billion to one and range of frequencies greater than one thousand to one. Also, the auditory system is very sensitive to additive random noise. So, data hiding in audio signals is especially challenging.

Hiding messages in audiothrough sound can be done as the figure below shows[8]

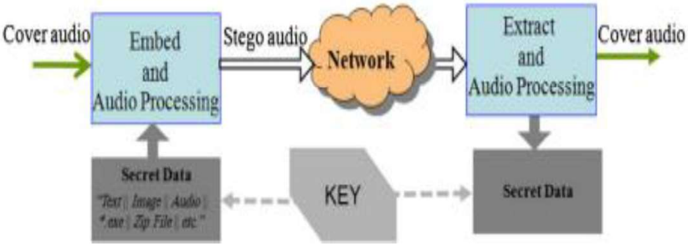

Cover audio
Embed and Audio Processing
Stego audio
Network
Extract and Audio Processing
Cover audio
Secret Data
"Text | Image | Audio | *.exe | Zip File | etc"
KEY
Secret Data

Fig5. Audio steganography workflow[8].

3.2.1 Spread Spectrum

Spread spectrum systems has been used by the military since the 1940s.This techniqueencode secretdataacross frequency spectrum as a binary sequence which sounds like noise but can be recognized by a receiver with the correct key.

Twoschemes:

Direct Sequence

Frequency hopping

Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.

3.2.1.1 Musical Instrument Digital Interface (MIDI)

MIDI files are good places to hide information due to the revival this format has had with the rushof mobile phones, which play MIDI ring tones. There are also techniques which can embed data into MIDI files easily. MIDI files are ended of a number of different messages. Some of these messages control the notes you hear while others are silent and make up the file header or change the notes being played .The Program Change (PC) is said to the message we are interested in [11]-12].

A PC basically changes the type of instrument being played on a certain channel. If there is multiple PC messages in succession the instrument played will be the one selected at the very end of the message chain and due to the fact these messages happenso frequently, there are no noticeable side effects to the sound. Each PC message can contain a number from 0 to 127, which corresponds to the number of different instruments that can be played. What you need to do is seriestogether the necessary number of PC messages to enclosethe hidden data. Obviously this method doesn’t permit enormous amounts of data to be stored nor is it a very simpleway of hiding data as it can be easily seen[9]-[10]-[11].

3.2.1.2 Motion Picture Experts Group Layer-3 audio (MP3)

The MP3 format is doubtlessthe most commoncompression format that is used for music files. Due to this reason it happens to be very good for hiding information inside it. The more inconspicuous format, the more easily the concealeddata may be unnoticed. There are very limitedworking examples of hiding information in MP3 files but one freely offeredprogram isMP3Stego [12]. The technique used, is similar to the frequency transformations. Basically the data to be hidden is stored as the MP3 file is created, that is during the compression stage [13]. As the sound file is being compressed during the Layer 3 encoding process, data is selectively lost depending on the bit rate the user has specified. The hidden data is encoded in the parity bit of this information. As MP3 files split up into a number of frames each with their own parity bit, a reasonable amount of information can be stored. To retrieve the data all you need to do is uncompressingthe MP3 file and read the parity bits as this process is done. This is an operativetechnique which leaves little trace of any distortions in the music file [14]-[15].

3.3 Video Techniques

Video files are generally a collection of images and sounds, so combination of the presented techniques on images and audio can be applied to video files. The great advantages of video are the large amount of data that can be hidden inside and that it is a moving stream of images and sounds.

This is due to the fact that video generally has separate inner files for the video (consisting of many images) and sound. Therefore the probabilities of hidden data being discovered arerelativelylow.

3.4 Text files Techniques

We can use Steganography in text file, it works by simply adding white space and tabs to the ends of the lines of a document.The advantage of this method is that white space and tabs is not visible to the human eye. Since white space and tabs arise naturally in documents, so using this method of steganography wouldn't cause somebody to be suspicious. But it is very challenging task. This is because text files have a very small quantity of redundant data to substitute with a secret message.There are other methods to hide secret message in text files:

3.4.1 A-Line-shift encoding:

This method works by shifting every single line of text vertically up or down by as little as 3 centimeters.Reliant on whether the line was up or down from the standing line would equate to a value that would or could be encoded into a secret message.

3.4.2 B-Word-shift encoding:

This method works in greatly the similar way that line-shift encoding works; only we use the horizontal spaces between words to equate a value for the hidden message. This method is less noticeable than line-shift encoding but involves that the text format provides variable spacing.

3.5 Executable Files Techniques

Executable files (EXE) are probably the most commonly used one. They are indispensable part of every application, game, program, or OS. These files contain very complicated executable code of program. In these files also, information about window structure, and other required information has their place.Every file contains a markup called EOF (End of File). Every data after this markup are ignored and aren't analyzed by system, so they don't disturb the application. We can use that fact to place hide able data right behind this markup, and bystanders won't notice it. Used algorithm is called as placing method, its defect is that, after using this algorithm, file is much bigger than original.

3.6 DNA Techniques

A quitenew area for information hiding is within DNA.This technique was explained by Peterson a message"JUNE6_INVASION: NORMANDY"was hidden inside some DNA. This was done in a scheme relativelysimilar to some of the text techniques discussed earlier. A single threadof DNA consists of a sequence of simple molecules called bases, which protrude from a sugar-phosphate backbone. The four varieties of bases are known as Adenine (A), Thymine (T), Guanine (G), and Cytosine (C). To generatethe secret message, DNA was producedfollowing this table with the bases in the right order. Then it was sandwiched between another two threadsof DNA which acted as markers to point the sender and recipient of the message to the message. The final step taken was to add in some arbitraryDNA threadsin order to further avoidthe revealingof the secret message. As DNA is extremelysmall, it can be hidden in a dot in a book or magazine much like the old microdot technique used in World War II. It is also robust enough to be forwardedthrough the mail and still be decoded. This could demonstrateto be a very operativetechnique in thefuture [16].

4. SUMMARY OF SOME STEGANOGRAPHY METHODS

For each technique that mentioned before, Carrier, CoverMedia, Embedding method withadvantages that Distinguish each techniques and give it strong points in specificapplications. In the flowing table we illustrate and summarize the advantages and disadvantages for each steganographytechniques:

Table 2: SUMMARIESOF SOME STEGANOGRAPHY METHODS[17]

No	Steganography Techniques	Cover Media	Embedding Technique	Advantages
1	Executable Binary File Technique	Binary File	Data can be embedded by making changes to the binary code that does not	Simple to implement

			affect the execution of the file	
2	Tex File Technique	Document	To embed information inside a document we can simply alter some of its characteristics .i.e. either the text formatting or characteristics of the characters	Alterations not visible to the human eye
3	Image File: 1) LSB (Least Significant Bit)	Image	It works by using the least significant bits of Each pixel in one image to hide the most significant bits of another.	Simple &easiest Way of hiding information.
	2) DCT (Direct	Image	Embeds the information by	Hidden data can

	Cosine Transform)		altering the transformed DCT coefficients	be distributed more evenly over the whole Image in such a way as to make it more robust.
	3) Wavelet Transform	Image	This technique works by taking many wavelets to encode a whole image	Coefficients of the wavelets are altered with the noise within tolerable levels
4	Sound Technique	MP3 files	Encode data as a binary sequence which sounds like noise but which can be recognized by a receiver with the correct key	Used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium
5	Video		Combination of sound & image	The scope for adding lots of

	Technique	Video Files	techniques can be used	data is much greater
6	DNA Technique	threads of DNA	DNA is produced following a table withbases in the right order. Then it was sandwiched between two threads of DNA	DNA is extremely small, so it is robust enough to be sendingthrough mails. This very effective technique.

5. LIMITATIONS OF STEGANOGRAPHY

There are limitations on the use of steganography. As with encryption, if Alice wants to communicate secretly with Bob they must first agree on the method being used. Demeratus, a Greek at the Persian court, sent a warning to Sparta about an imminent in vision by Xerxes by removing the wax from a writing tablet, writing the message on the wood and then covering it in wax again [17]. The tablet seemedto be blank and trickedthe customs men but almost misleadthe receivertoo since he was unaware that the message was being concealed. With encryption, Bob can be reasonably sure that he has received a secret message when a seemingly worthlessfile arrives. It has either been ruinedor is encoded. It is not so clear with hidden data, Bob simply receives an image, for example, and needs to know that there is a hidden message and how to locate it. Another restrictionis due to the size of the medium being used to hide the data. In order for Steganography to be useful the message should be hidden without any main alterations to the object it is being inserted. This makes limited room to embed a message without noticeably changing the original object.

This is most clear in compressed files where many of the obvious candidates for embedding data are lost. What is left is likely to be the most significant portionsof the file and although hiding data is still possible it may be difficult to avoid changing the file[18].

6. CONCLUSION

As steganography becomes more widely used in computing, because the high development of communication and network, that is the environment of transmit data through it .There are some challenges that needs to be resolved. There are some different techniques with their own advantages and disadvantagesthere are some issues must be aware for any stego design:

a) The quality of the media should not be easy to decryptby third parties for a secret data.

b) Secret data should be undetectable without secret knowledge, typically the key.

c) If multiple data are present they should not interfere with each other.

d) The secret data should survive attacks that don't degrade the perceived quality of the work.

This paper presents DNA techniques as a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties. And compare between several of steganography techniques. When the data will be sent throw unprotected area, the future work for more secure transmit data we must use the power full steganography algorithms with cryptography for the plaintext to let the data difficult to attacked by third parties.

REFERENCES

Artz, D., (2001) "Digital steganography: hiding data within data," internet computing, IEEE, vol. 5, pp. 75-80,

Djebbar, F, B. Ayad, K. A. Meraim, and H. Hamam,(2012) "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing, vol., pp. 1-16,.

Chao, A. K. and C. Chao,(2000) "Robust Digital Watermarking & Data Hiding", Image Systems Engineering Program, Stanford University, http://ise.stanford.edu/class/ee368a_proj00/project7/index.html,.

Channalli and A. Jadhav S. (2010), "Steganography an art of hiding data," International Journal on Computer Science and Engineering,.

Hacker, S, MP3(2000): The definitive guide: O'Reilly Sebastopol, CA,.

J.Blasco, J. C. Hernandez-Castro, J. M. de Fuentes, and B. Ramos,(2012) "A framework for avoiding steganography usage over HTTP," Journal of Network and Computer Applications, vol. 35, pp. 491-501,.

James P. Cavanagh(2004) ,"Introduction to steganography ",Brigitte Si Athabasca University, COMP607 Project,July,

Manoj, I. V. S. "Cryptography and steganography," International Journal of Computer Applications (0975–8887), vol. 1,.

Peter, W. (1996), "Disappearing Cryptography," Massachusetts, AP Professional,.

Sehgal, N. and A. Goel, "Evolution in Image Steganography".

Swanson, M. D., B. Zhu, and A. H. Tewfik,(1996) "Robust data hiding for images," in Digital Signal Processing Workshop Proceedings,., IEEE, , pp. 37-40.

ShashikalaChannalli ,(2009)"Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), , 137-

Shirali-Shahreza, M.(2006), "A new method for real-time steganography," in Signal Processing, 2006 8th International Conference on,.

Rajyaguru, M. H., (2012) "Crystography combination of cryptography and steganography with rapidly changing keys," Int J EmergTechnol Ad Eng, vol. 2, pp. 329-332,.

Thakur, R. S. and R. D. Jadhav, "Advance Data Concealing By Digital Steganography and Watermarking".

Thakur, R. S. and R. D. Jadhav, "Advance Data Concealing By Digital Steganography and Watermarking.

Zaidan, B, A. Zaidan, A. Al-Frajat, and H. Jalab,(2010) "On the differences between hiding information and cryptography techniques: An overview," Journal of Applied Sciences, vol. 10, pp. 1650-1655.