Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 15 Issue 01, 2026

Pixel to DNA: Analysis of Emerging Steganography Techniques for Media Protection

[1]Leena Amol Deshmukh, [2]Maithili Arjunwadkar

[1]*Progressive Education Society's Modern Institute of Business Studies (Autonomous), Nigdi, Pune, Maharashtra India*

[2]*Progressive Education Society's Modern Institute of Business Studies (Autonomous), Nigdi, Pune, Maharashtra India*

Peer Review Information

Submission: 08 April 2026
Revision: 29 April 2026
Acceptance: 11 May 2026

Keywords

Steganography, Spatial and Frequency domain, Spread Spectrum, DNA

Abstract

Steganography is a branch of information hiding where confidential information is hidden inside text, image or any other multimedia. In this paper we analyze different Steganography techniques including DNA steganography. DNA Steganography is an emerging technology. It is more robust. Based on performance parameters, different steganography techniques are studied.

Introduction

In the modern era, information in digital format like text, image, PDF is distributed among multiple users over the internet. When information is transmitted between multiple users, security of information is a major concern. If an unauthorized user or attacker gets access to this digital data, they may modify the content or copy it and create fake copies of digital data and claim as owner of this digital content. This creates ambiguity between authorized and unauthorized user. So, the security of Digital data is important. Different information concealment techniques such as Digital watermarking, Cryptography and Steganography provide security to multimedia data sent over the network. To provide security and authenticity to digital content, copyright information is embedded into it. With Digital watermarking information is added . This data is extracted and verified to prove the ownership of digital data. Watermark can be visible or invisible. In Cryptography, a message to be sent from sender to recipient is translated into another unreadable format. In Cryptography, secret information (called as Plain Text) which is send from sender to receiver is translated into Scrambled text which cannot be understood by unauthorized user whereas the aim of Steganography is that unauthorized user not only understand which secret message is hidden inside cover object but also presence of hidden message. In steganography, information is concealed into another object so that it cannot be easily visible to the human eye. In steganography an unauthorized user is not able to know whether a cover object contains hidden information.

Steganography

Steganography is a branch of information hiding where confidential information is concealed into a cover object. Cover object can be text, images, audio or video. The word Steganography is made up of two Greek words "Stegnos"and "graphia". The meaning of "*Stegno*" is hidden and "*graphia*"

means writing. So Steganography means writing a hidden message into a Cover object [1].

History of Steganography

The utilization of Steganography dates back to ancient Greece. As per Greece records, wax tablet is used to conceal message. Here the wax tablet is melted and a private or confidential message is concealed in underlying wood. After inserting a secret message on wood, wax is reapplied on the wood, showing that it is a new, unused tablet. Then this brand-new tablet is sent without knowing anyone's presence of secret message [2]. Herodotus, the great historian mentioned in his story about a trusted servant who shaved his head and write secret message on the scalp again to re-grow hair and send him on his way [3].

Types of Steganography

In steganography, confidential message is masked into Cover media. Possible Cover media include image, text, audio or video files. Depending on cover media Steganography can be classified as [4].

1. **Text Steganography**: When secret information is concealed into letters of text then it is called Text Steganography.
2. In Text Steganography, secret information is concealed into Text. It can be letter or white spaces or space between two words.
3. **Image Steganography**: In image Steganography, confidential data is masked inside the image. Image is made up of pixel, if a private message is masked inside a pixel, then it is called image steganography.
4. **Audio Steganography**: If a secret message is concealed into audio signal, then it is called audio steganography. Here different audio format is used to conceal secret message.
5. **Video Steganography**: Video is made up of a series of image frames and sound together. If a secret message is inside a video then it is called video Steganography.

Process of Steganography

Steganography is the mechanism of concealing and retrieving confidential message [5].

Terminology of Steganography:

1. Cover Object: Also known as the original image in which confidential message is concealed. Cover image can act like a container in which a secret message is concealed.
2. Secret or confidential message: Confidential message can be in the form of text or image as well. This confidential message is concealed inside the Cover Object.
3. Stego object: When a confidential message is concealed into a cover object, the resultant object is known as Stego object. For example, if secret message is hidden inside cover image, then resultant image is known as Stego image

Hiding private and confidential message into cover object is called an "**embedding process**". For this input are cover object, secret message and key of embedding algorithm. The result of this is Stego-object. An algorithm for hiding private info. is selected to ensure that no one can find out the difference between original object and new object which is created after hiding data. Both cover object and stego object look identical though data is kept inside the stego object.

In the **extraction process**, a secret message is retrieved from the stego object. Input for this process is stego-object, key of extraction algorithm and output is confidential and private information and Cover object.

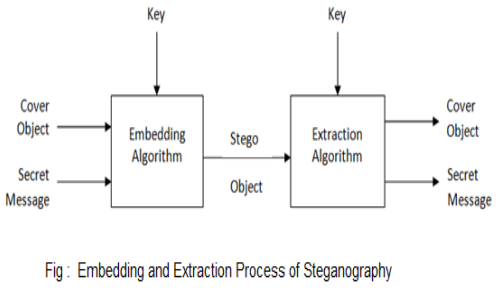

Figure 1: Embedding and Extraction Process of Steganography

Performance evaluation parameter of Steganography is as follows [6] [7]

1. **Payload Capacity**: It is defined as how much secret information is concealed into a cover object without losing the quality of the cover object. i.e. number of bits is concealed into a cover object. Payload capacity depends upon which steganography technique is being used. If payload capacity is large then good steganography is used.
2. **Robustness**: Irrespective of multiple attacks on stego object to obtain a secret message, if an attacker has failed to obtain a secret message, then the steganographic technique is called roust.
3. **Imperceptible**: Stego object should be imperceptible. i.e. changes made in cover object to embed secret message that cannot be identified by the naked eye. After inserting a secret message, stego-object and cover object should

look identical and changes cannot easily be visible. Imperceptivity can be measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

a) PSNR : It is calculated in terms of decibel (dB). Higher the PSNR value indicates lower the MSE value. PSNR is used to calculate how much quality of an image is changed after confidential information is kept inside it .

If PSNR value > 40dB is good and acceptable. PSNR is calculated as follows

PSNR = $10 *$

$log\ log\ 10 \frac{(maximum\ Pixel\ \ Intensity)^2}{MSE}$ dB

Pixel intensity for 8 bit image = 255

After putting above value,

PSNR = $10 * log\ log\ 10 \frac{255*255}{MSE}$ dB

b) Mean Square Error (MSE). It is the average square difference among original image known as cover image and steganographic image called stego image. If the original image and steganographic image are the same, the MSE is 0. Lesser the MSE value shows original image and steganographic image are nearly identical. i.e. in term of pixel difference, stego image is closer to cover image. It means there is less distortion among original image and steganographic image. It is calculated as follows

$$MSE = \frac{1}{m*n} \sum_{i=1}^{m} \quad \sum_{j=1}^{n} \quad (cij - sij)^2$$

Where

cij = Cover mage pixel value at i^{th} row and j^{th}column

sij = Stego mage pixel value at i^{th} row and j^{th} column

m = number of rows

n = number of columns

Application of Steganography

1. Digital watermarking:

Steganography is used in digital watermark to conceal copyright information or ownership details into another digital medium like text, images, audio or video. This approach is used to verify originality of the content and prevents unauthorized sharing [6.1].

2. Secret Communication:

Criminals use Steganography to do secret communication among them. Here criminals send secret message on digital media like image, text, audio or video. Normal people when see image or text containing secret message inside it, cannot find difference between original image and stego image an only criminal at receiver end know how to retrieve secret message. By this communication happens between them. Digital expert who has knowledge of how to retrieve this secret information is used to identify information and stop criminal activity [8] .

Steganography Techniques

A number of steganography techniques are used to ensure high robustness and better imperceptibility. They can be categories as follows:

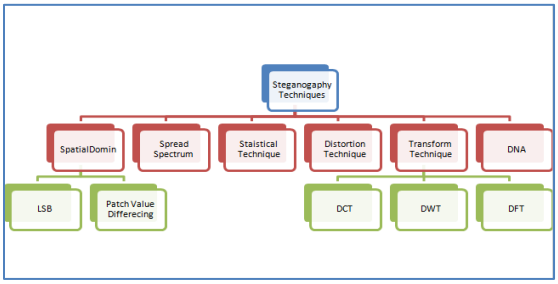

Figure 2: Different techniques of Steganography

Based on domain, Image Steganography is classified as Spatial Domain and Transform domain.

In the Spatial domain, a confidential message is concealed inside an image by modifying the pixel of an image. This is an easy and simple technique. It has a high capacity to conceal confidential message but it is not robust again Image manipulation attacks. In the transform domain, the first image is transformed to frequency domain and the confidential message is concealed by changing the coefficient of frequency domain. This technique offers greater robustness and efficiency and sustains image manipulation attacks [9].

1. Spatial Domain

a. LSB

Least Significant Bit (LSB) is to conceal confidential message inside an image. In this technique, a confidential message is transformed to binary sequence and then a bit of confidential message is added to the right most bit of the image. Implementation of this technique is very easy but the technique is very sensitive to image manipulation attacks. [10].

b. Pixel Value differencing (PVD)

In pixel value differencing, difference *d* between two adjacent pixel values is calculated and private or confidential message is concealed into difference. If pixel difference is larger, then more bits of private or confidential message is concealed into it and if the difference is less then only a limited amount of data is secreted into difference. Pixel value differencing has high capacity and good imperceptivity [11].

2. Spread Spectrum

In Spread Spectrum, noise is required to conceal private data and after this noise is added to image to transmit data. Here data is transmitted over wide range of frequencies so it makes it almost impossible for an unauthorized user to detect. For detecting secret message, the recipient must possess proper decoding technique. In other word, secret message called communication is spread over a wide frequency range using pseudo-random sequence also called as noise [12]. The spread spectrum is resistant to statistical attack because in the spread spectrum a secret message is spread all over the cover image.

3. Statistical technique

In statistical technique, important secret message is hidden inside an image by changing the statistical properties of image. In this technique, image is split into smaller parts, which represents 1 or 0 bit of private message which need to be hidden. If bit is "1", then the statistical properties of the image are changed slightly. If bit is "0", then no change in image The modifications are minor so that variations go unnoticed by humans. This technique is prone to geometric attack like cropping, scaling or rotating an image [13].

4. Distortion Technique

In distortion technique the secret message is concealed within the cover image by performing a limited number of incremental alterations in the host image known as cover image. Here source image called original image is required at the time retrieving confidential message from stego image and that is the main challenge. Here the sender needs to send a stego image along with a cover image to the receiver. In between clever intruders get access to both the message and if the intruder knows the cover image, then performing some set of cropping, scaling, manipulation on stego image they can easily know the secret message [14] **.**

5. Transform domain

a. Discrete Cosine Transform (DCT):

It is image compression technique. Here image is transformed from spatial domain to frequency domain and hide confidential message in it. DCT divides image into two frequency bands : low and high where low frequency shows general features of image and high frequency shows better details of image like edge, texture etc.

In this jpeg image is segmented into 8 * 8 block and DCT is performed to each block and then secret message in binary format is concealed into least significant bit (LSB) of each DCT coefficient. The capacity to conceal confidential message is high in DCT. DCT is affected by high compression rates and it requires more complex processing [15].

b. Discrete Wavelet Transform (DWT)

In this technique image is segmented into non-overlapping sub bands called LL, HH, HL and LH. DWT (Discrete Wavelet Transform) is Transform domain Steganography technique in which the original image is decomposed into high and low frequency components and confidential message is hidden by changing wavelet coefficient in different frequency bands. Here original image is called as cover

image and after applying DWT image is called stego image. It has good performance under compression but implementation cost is high. So, it is expensive [16].

6. DNA Steganography

DNA stands for Deoxyribonucleic acid. DNA is a complex molecule found in all living organisms. Nucleotides are the smallest unit of DNA. DNA is A,T,C,G where 'A' stands for Adenine,, 'T' stands for Thymine , 'G' stands for Guanine, and 'C' stands for Cytosine .

Different techniques are used in DNA steganography to conceal secret message into DNA stands (sequence) [17] [18]

a. Insertion Based – DNA stand is divided into equal parts and then secret message is embedded inside DNA sequence after each part.

b. Substitution based - In this technique, secret message is concealed in DNA sequence by modifying specific nucleotides in a DNA sequence.

c. Complementary Rule based – In this, first transmitter and recipient agree on complementary rule confidential information is concealed into DNA stand before the longest complimentary substring. At the receiver side the same complementary rule is applied by the receiver to extract a secret message.

Study of different Steganography Techniques

Table 1: Comparative Analysis of Steganography Techniques

Ref.	Technique	PSNR (dB)	MSE	Payload Capacity	Robustness
[19]	LSB Substitution	40–55	Low	High	Low
[20]	DCT-Based	48–57	Low	Medium	High
[21]	DWT-Based	48–65	Very Low	Medium	Very High

[22]	DNA Insertion	NA	High	High	High
[23]	DNA Substitution	NA	High	Very High	Medium
[24]	DNA Complementary Rule	NA	Very High	Very High	High

Conclusion

Steganography is a robust technique used from ancient times. It is used in various applications like invisible watermarking. Different techniques are reviewed. In terms of capacity, robustness and imperceptivity, each technique offers certain advantages. Study shows combining DNA and Image Steganography together makes stego image more robust.

References

Mohammed A. Saleh, "Image Steganography Techniques - A Review Paper", International Journal of Advanced Research in Computer and Communication Engineering", Vol. 7, Issue 9, PP:52-58, 2018

Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Volume 9– No.7,PP:19-23,2010

JAMMI ASHOK, Y.RAJU, S.MUNISHANKARAIAH, K.SRINIVAS, "STEGANOGRAPHY: AN OVERVIEW",

International Journal of Engineering Science and Technology ,Vol. 2(10), 2010, 5985-5992, 2010

Jasleen Kour, Deepankar Verma, "Steganography Techniques –A Review Paper", International Journal of Emerging Research in Management &Technology , Volume-3, Issue-5, PP:132-135, 2014

Ritu Sindhu, Pragati Singh, "Information Hiding using Steganography", International Journal of Engineering and Advanced Technology, Volume-9 Issue-4, PP:1549:1554, 2020

C.P.Sumathi , T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey, Vol.4, No.6, PP:9-25, 2013

Alaa A. Jabbar Altaay, Shahrin Sahib, Mazdak Zamani, "An Introduction to Image Steganography Techniques", International Conference on Advanced Computer Science Applications and Technologies, At: Kuala Lumpur, MalaysiaVolume: ACSAT'12 , 2012

Nujud Alabdali , Sabah Alzahrani, "An Overview of Steganography through History", International Journal of Scientific Engineering and Science, Volume 5, Issue 2, PP: 41-44 , 2021

Sami Ghoul, Rossilawati Sulaiman, Zarina Shukur, "A Review on Security Techniques in Image Steganography", International Journal of Advanced Computer Science and Applications, Vol. 14, No. 6,PP:361-385, 2023

Sabah Abdulazeez Jebur, Abbas Khalifa Nawar, Lubna Emad Kadhim, Mothefer Majeed Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique", International Journal of Interactive Mobile, Vol. 17, No. 07,PP:167-178 , 2023

JayeetaMajumder, Chittaranjan Pradhan, "IMAGE STEGANOGRAPHY TECHNIQUES USING PIXEL VALUE DIFFERENCING: AREVIEW", International Journal of Creative Research Thoughts, Volume 6, Issue 1, PP:1042-1046 , 2018

Lisa M. Marvel, Charles G. Boncelet, Charles T. Retter, "Spread spectrum image steganography", IEEE Transactions on Image Processing, Vol-8, issue -8, PP: 1075-1083 , 199

Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi , "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3),2012,PP:168-187 , 2012

Vinita Haridas, "Steganography-A Data Hiding Technique", Steganography-A Data Hiding Technique, Volume 3, Issue 30,2015, PP:1-4 , 2015

Humbe Rupesh, Khond Pranesh, Ukirde Rohan, Prof. Dere K. D. , "Discrete Cosine Transform Technique in Steganography", International Journal of Research Publication and Reviews, Vol 4, no 5, 2023, PP: 6028-6034, 2023

ASHOK KUMAR BALIJEPALLI & L.SRINIVAS, "STEGANOGRAPHY BASED SECRETE COMMUNICATION USING DWT", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 5, 2012,PP:1-8,2012

Omar Haitham Alhabeeb, Fariza Fauzi , Rossilawati Sulaiman, "A Review of Modern DNA-based Steganography Approaches", International Journal of Advanced Computer Science and

Applications,Vol. 12, No. 10, 2021, PP:184-196, 2021

Ghada Hamed, Mohammed Marey, Safaa El-Sayed and Fahmy Tolba, “DNA Based Steganography: Survey and Analysis for Parameters Optimization”, Intelligent Systems Reference Library, 2016, PP: 47-89, 2016

Marghny H. Mohamed Loay M. Mohamed, “High-Capacity Image Steganography Technique based on LSB Substitution Method”, Applied Mathematics & Information Sciences, Vol. 10, No. 1,2016, 259-266, 2016

Dr. Ekta Walia, Payal Jain, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, Vol. 10 Issue 1, 2010, PP:4- 8 , 2010

Della Baby, Jitha Thomas, Gisny Augustine, Elsa George, Neenu Rosia Michael, “A Novel DWT Based Image Securing Method Using Steganography”, International Conference on Information and Communication Technologies, 2015, PP:612-615, 2015

Malathi P, Manoaj M, Manoj R, Vaikunth Raghavan,Vinodhini R E, “Highly Improved DNA Based Steganography”, 7th International Conference on Advances in Computing & Communications, PP:651 -659, 2017

Ashish Gehani, Thomas H. LaBean and John H. Reif, “DNA-based Cryptography”, chapter in "Aspects of Molecular Computing", Springer Verlag series in Natural Computing (edited by N. Jonoska, G. Paun and G. Rozenberg) LNCS 2950 Festschrift, Springer, PP: 167-188, 2004

Amal Khalifa, Ahmed Elhadad, Safwat Hamad, “Secure Blind Data Hiding into Pseudo DNA SequencesUsing Playfair Ciphering and Generic Complementary Substitution”, Applied Mathematics & Information Sciences, Vol. 10, No. 4, PP: 1483-1492 ,2016

Abdullah Ahmed Abdullah1, Sardar Hasen Ali1, Ramadhan J. Mstafa1, Vaman Mohammed Haji, “Image steganography based on DNA sequence translation properties”, UKH Journal of Science and Engineering Vol. 4 Issue-6, PP:15-26, 2020