A Modified High Capacity Image for Communicating Multimedia Data using Steganography Algorithms

Apoorva Mishra[1] and Dr. Prateek Mishra[2]

[1]M. Tech., Student, Electronics & Communication Department, Baderia Global Institute of Engineering and Management Jabalpur, Madhya Pradesh
[2]Assosiate Professor, Electronics & Communication Department, Baderia Global Institute of Engineering and Management Jabalpur, Madhya Pradesh

ABSTRACT- In today's world, there is a desire to transmit and publish information secretly, especially where it is readily available. Information disclosure and exchange occur for many reasons. In this document, to conceal information, the information is locked in the form of numbers, as this is the most popular method on the internet. There are many ways to hide information; some are simple, some are more complex than others, and all have their advantages, disadvantages, and limitations. Pixel power methods are used for hiding information. If it is an image, shutter objects are used. Frequency domain techniques: In this technique, the different algorithms and transformations created to encode the data are considered as methods depending on the number of transformations. The process of hiding data and information is called steganography, which is done to provide secure communication. In today's world, there is a need to transmit and present data secretly, especially when information and data are being exchanged publicly, and for this reason, many methods have been proposed for hiding data and information.

Keywords: Digital Image; Steganography; Hiding security information:

1. INTRODUCTION

Steganography comes from the Greek words steganós, meaning covered, and graphein, meaning to write. It avoids suspicion when sending secret messages. When suspicion arises, the purpose is defeated. Steganography is a method where sensitive information is hidden in images, and it is extracted when the message reaches the recipient.

If someone tries to view the message, they will not be able to see the complete information. Steganography is used to counter corporate espionage attempts in the competitive world, and terrorist organizations also use steganography. It is mostly for confidential information. It is rumored that some terrorist organizations are using steganography by posting images on certain websites and sharing them secretly. The key design of steganography is based on Kerckhoffs' principles of steganography. It is a way to hide personal information or concerns that might seem unusual. Steganography is often confused with encryption because they are similar in the way they store sensitive information. The internet is one of the most popular and easiest mediums for transmitting digital data between individuals, but one of the common threats during transmission is that someone can access this data, and the internet itself does not provide any security on this data. [2]. The term steganography originates from the Greek words steganos, meaning covered or concealed, and graphic, meaning writing or drawing. Its purpose is to hide secret data within another unsuspecting cover medium. [3] Steganography and cryptography are major fields in security and information concealment. [4]

2. LITERATURE REVIEW

Sanjeev Tyagi et al. (2018) have proposed a novel model for PDF-based text steganography. Confidential information is embedded in the spaces between text characters in a PDF format to enable covert communication. The stego text format is designed to improve embedding capacity and reduce the size of the stego cover PDF file. This method can be used to develop a variety of mounting power systems designed to meet needs ranging from standard mounting capacity to general mounting capacity. The editing and classification of the encrypted text are performed using a quadratic hashing model, creating a four-'creative manual' that delivers effective performance under complex time constraints. The research results indicate that the established method provides useful algorithms for modern security and a high level of hidden data. The performance and testing of the model method and other simulations provide significant information demonstrating that it outperforms existing methods and does not require shadows, languages, word lists, pronunciation, etc.

Security is a vital part of our lives to ensure that information is protected in a way that prevents unauthorized individuals from stealing it. For this reason, various strategies are available to protect information through security statements, secret keys, fingerprint security, and much more. However, today, in the era of digital communication on the global web, activities such as illegal access, exploitation, and copyright infringement are increasing. Therefore, there is a need to protect sensitive information using cybersecurity guidelines, which can be achieved by covering digital information and/or translating it into an unknown framework. Thus, innovations in steganography and cryptography can be considered crucial components in the use of digital information systems.

Sangeeta Roy et al. (2019), the term "steganography" originates from the Greek language and means "hidden writing," derived from the Greek word "steganos," meaning "to cover or protect." In the last decade, following the development of new technologies, particularly in technical information and computing systems, the issue of data security has gained significant importance. One of the key aspects of data security is the concept of sharing confidential information. For this purpose, various methods are used, including encryption, steganography, encoding, etc. Steganography is one of the areas that has attracted the most interest in recent years. Once steganography is complete, the main goal is to hide information within the media so that outsiders cannot access the information contained in the media. This is a crucial difference between steganography and other methods of sharing confidential information; for example, in cryptographic methods, people become aware of the existence of information by seeing the encrypted data. They may not be able to understand the information. In steganography, no one is aware of the existence of information within the data source. This is most often done in films, videos, writings, music, and audio.

Text steganography is a more complex form of steganography because the file format does not contain media data. It is often used in image or audio files. It can be used in steganography where digital messages are written, stored, and downloaded by a computer in such a way that they do not appear different. Unlike other digital files such as images, where what is visible, stored, and kept secret are distinct, it hides details about the structure. This involves using information encoded within the text, ranging from native language to HTML file formats.

Before briefly explaining the text steganography process, it is important to consider the common terminology used in text steganography. The secret message to be encrypted is called the attachment, and the secure text/audio/video used for the attachment is called the cover. The resulting product after installation is called the stego material. The sending and receiving points are essential for aligning with a crucial marketing strategy. There are several functionalities for concealing information within the message. A list of applications is provided below. These have been implemented and reported on.

Preetam Kumari et al. (2020), with new technological advancements, it is crucial to provide a method for transmitting confidential information online without any alterations, and it is essential for people to consider their audience. One such method is steganography. It comes from two Greek words, steganos meaning to cover or hide, and graphein meaning to write. Therefore, it is common to hide private information within another file, which is called a container. Image files are often used as containers because they occupy space. The availability and the ability to obtain a stego image after embedding confidential information into a digital image through an algorithm is key. No one other than the recipient of the stego image will know that any secret information is embedded within it. This method provides the best quality when hiding private messages. This means that only the intended sender and receiver can suspect the confidential information. This is also known as an imperceptibility security scheme. Steganography and cryptography are interconnected. The term cryptography comes from the Greek word kryptos, meaning "hidden." Another way to secure information is to transform it into a readable format called ciphertext. Only the person with the secret code can decrypt it or convert it back into plain text.

Aravind Kumar et al. (2022) state that steganography is an example of data encryption and an attempt to conceal the existence of the embedded data. It is a better way to secure messages by hiding them rather than encrypting them. The existence of the message is not revealed. The first message was hidden in a battleship. To avoid making any changes to the ships, in this article we discuss how to use this technique as a message board. This document also contains information about using the tool. Steganography, along with other steganography techniques, is a useful tool that allows data storage through communication. The combination of secret photos and images creates a hidden image. The hidden image is difficult to detect without being extracted. This article explores the technology of steganography by introducing readers to its concepts. A brief history and summary of the method are provided. Some steganography methods require internet users to collect, send, or receive personal information. The most common way to do this is by converting the data into another format. Only those who can restore the received information to its original state can understand it. This method of securing information is called information hiding. The biggest drawback of this method is the availability of unencrypted data. The highlighted data, even if unreadable, still remains in the logs. If a person has enough time to search, they can delete the records. One solution to this problem is steganography. This ancient art involves hiding messages. No alterations or modifications are made. The hidden message is simple but undetectable to the reader. The purpose of steganography is to conceal the existence of the message, while encryption scrambles the message to make it unintelligible.

Nishi Madan (2023), Internet usage is increasing day by day. Due to the use of the internet, providing security has become a major issue. Coding and steganography are ways to secure your information. Encryption is used to encrypt messages to protect them from external influences. Steganography is a method used to hide information inside a frame so that no one can detect it. The cover can be an image, text, audio, or video. Steganography. It comes from the Greek words 'steganos', meaning secret, and 'graph', meaning writing, which generally means secret writing. The purpose of steganography is data encryption, while encryption is used to protect data from intruders. Image files are often used as covers due to the availability of empty space.

There are two types of files: lossless and lossy files. The original image remains intact. The compressed image is virtually identical to the original image. This applies specifically to system steganography, as the main objective of steganography is to hide text within an image using compression techniques without affecting the quality of the GIF or BMP graphics. On the other hand, lossy compression also helps in maintaining the final state. However, it does not protect the integrity of the original image. JPEG conversion using standard compression does not yield an exact copy of the original image.

Arshya Sajid Ansari et al. (2024) Steganography, on the internet and in the real world, is often attacked by computer hackers or prisoners. See how steganography works. How security is improving day by day. Steganography. There are different methods, ease of using databases to view facts and test results. Steganography search methods. This section provides information about the method.

D. Bhavana et al. (2024) Steganography is a method of hiding messages inside files, which can be audio, images, videos, and their main potential. Steganography, which is equivalent to writing to files. If steganography has malicious intent, it can be used as a weapon. The only way to obtain steganographic content is through searching and analysis. In this post, I will explain how to hide colors in audio and image files using MATLAB software.

Pasala Sanyasi Naidu (2025) This article provides a comprehensive analysis of a new and original programmed algorithm based on hiding any information, which overcomes the shortcomings of existing algorithms and ensures that the closed and stego images are similar to the graphic image. This requires a maximum performance of 69.6% and is driven by something called medium-frequency error and excessive signal power. In a wireless environment, encoders are hacked by various spyware programs that expose confidential information to anonymous users through a photo security service. In our described prototype, it helps ensure that the angel is creating an invisible image from the start.

Ramalingam (2025) states that the modern digital economy relies on interactive access techniques using information technology and reading techniques. In the modern world, digital communication has become a problem when it comes to exchanging information over the internet. Therefore, it is important to develop a data security system. This is possible through the use of technology. Steganography: The steganography method modifies these blocking mechanisms for reliable data processing and establishes its presence in network communication.

3. INFORMATION HIDING

Information hiding is a growing research area, encompassing applications such as watermarking, fingerprinting, and copyright protection. For example, in watermarking, the message contains information such as the owner's identity and a digital timestamp. In fingerprinting, the database owner assigns a unique product number to the database set that identifies the user. This is added to the copyright information so that everything can be tracked. The data returned to the user is then authorized for use. Besides cryptography, steganography can also be used to protect information.

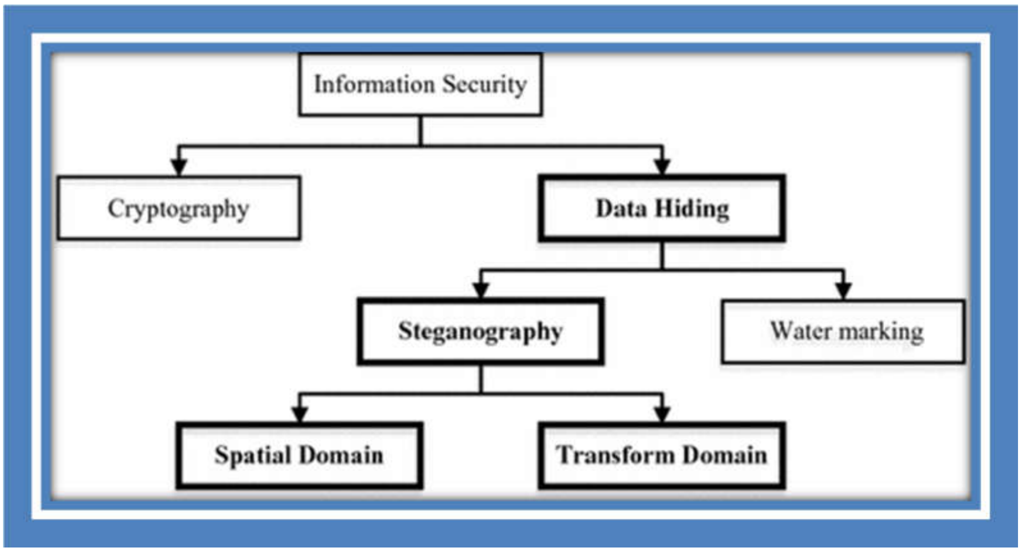

Figure 1. Information Hiding Information

In steganography, Moreland suggests embedding a hidden message in a cell phone before sending it over a network, so that the message's existence cannot be detected. In addition to tagging information for privacy, this encryption method can also be extended to copyright protection in digital media: audio, video, and images. Steganography is important because many people participate in online transactions.

"Steganography is the art of labeling information in a way that prevents the discovery of hidden messages. Steganography encompasses a range of secret communication methods that conceal a message from being seen or known." Steganography hides a secret message within host data and anonymity, and must deliver it reliably to the recipient. The host's records are intentionally manipulated, but in a confidential manner that should not be noticeable in data analysis.

4. CONCEPTS OF STEGANOGRAPHY

Although steganography is an old concept, its modern formulation is often given in the context of the Simmons' prisoner problem, in which two prisoners want to communicate secretly to coordinate an escape plan. All their communications are given to a prison guard, who will arrest them if he suspects any secret exchange of information. The prison administrator, who is free to monitor all communications between the prisoners, may be passive or active. The prison guard only checks the operation to see if there is any confidential information. If he suspects that there is confidential information on the network, the prison guard actively monitors the discovered confidential communication, reports it externally, and allows the message to be sent without interruption. On the other hand, a powerful administrator intentionally attempts to delete information and modify the communication and sensitive data.

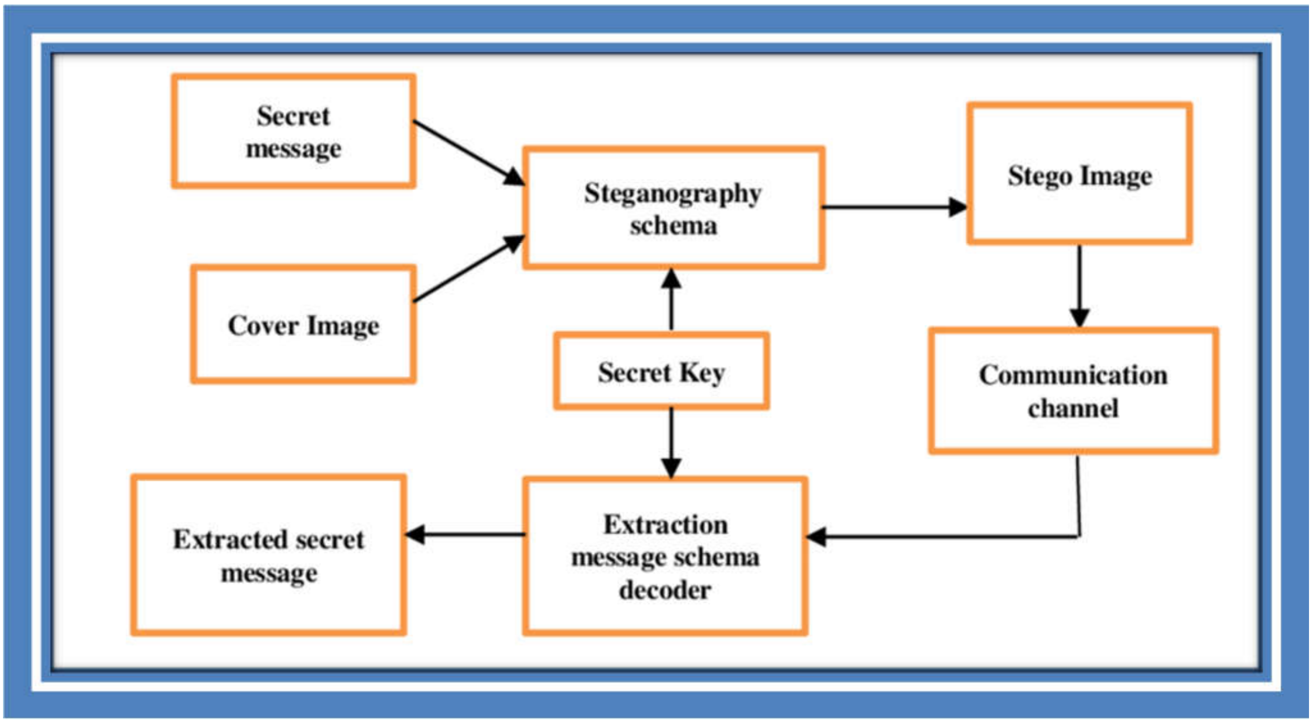

Figure 2. Steganography Concepts

5. BITMAP STEGANOGRAPHY TECHNIQUE

One of the most basic types of images is the bitmap. Because download size is technology-independent, bitmaps generated from pixels are in this tri-color file format. (Green, Red, and Blue, known as GRB) are the opposite generation. One byte of information represents the color of a single pixel and indicates the color's endpoint. The colors we see in these images are created by combinations of these three colors. 1 byte is equal to eight bits, with the first being called the Most Significant Bit (MSB) and the last being called the Least Significant Bit (LSB), representing the last bit of data. Data names and data file names must be spelled correctly, and this can be done by defining the source memory.

6. BIG DATA STORAGE AND MANAGEMENT

One of the first things an organization needs to control when dealing with big data is where and how this data will be stored once it is received. Common methods for systematic data retention and retrieval include affiliated sites, data marketplaces, and data repositories. Data is extracted from external sources, modified to meet operational needs, and finally uploaded to a storage data store using Extract, Transform, Load (ETL) or Extract, Load, Transform (ELT) tools. Data is then uploaded to a website or database. Therefore, data is cleaned, transformed, and cataloged before data mining and analytics services are available online.

However, unlike enterprise data warehouse (EDW) environments, the Big Data area requires Magnetic, Agile, and Deep (MAD) analytical capabilities. First, traditional EDW methods do not encourage the inclusion of new information sources until they are cleaned and integrated. Due to the availability of data today, the Big Data field must be magnetic, attracting all data sources regardless of data quality. Furthermore, given the increasing number of data sources, as well as the complexity of data analysis, Big Data storage analysts must be able to create and use data quickly and easily. This requires a robust database with logical and portable content that can adapt to synchronization and rapid data growth.

7. BIG DATA

Large data sets cannot be stored, processed, or analyzed using traditional tools. Today, there are millions of data sources generating data rapidly. These data sources are available worldwide. Some major data sources include social media and networks. Data also comes in various formats, such as structured data, small format data, and unstructured data. For example, in a standard Excel spreadsheet, data is categorized as structured data with a simple format. In contrast, emails come in a fixed format, and photos and videos come in unstructured data. All this mixed data constitutes Big Data.

8. METHODOLOGY

Typically, in LSB input mode, a random number generator is used to distribute and hide private messages within small pixel art images. To do this, one of the commonly available pixel skin images is randomly selected and used to hide some of the text. This means that the random function uses the main character unit only once per pixel in the image. And because a standard color image has many pixels, this actually represents a large number of pixels. Therefore, the random number generator takes a long time to complete. Also, generating large vectors of many unique random numbers is a difficult task for the function viewer. The entire area of the group of photos is logically divided.

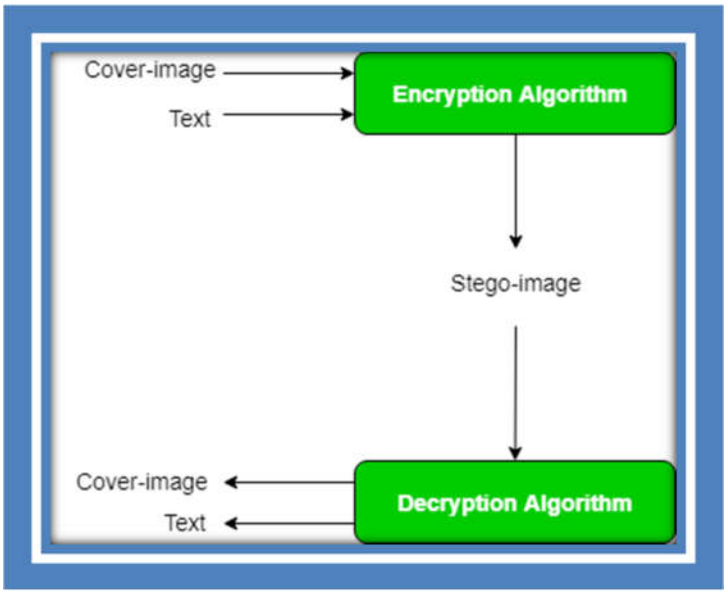

Figure 3. Algorithm Process

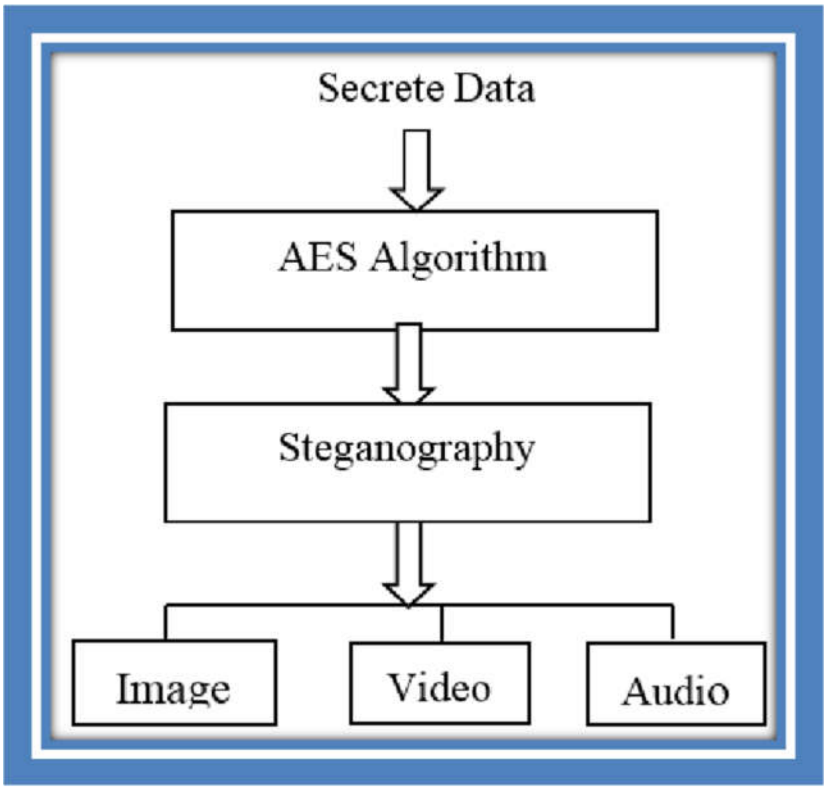

Figure 4. Data Process

Steganography is a method of hiding secret data within any type of digital media. The main purpose behind steganography is to conceal the existence of data within a medium such as audio, video, or images. When we talk about image steganography, the idea behind it is quite simple. Images are composed of pixels, which typically represent the color of that particular pixel. In a grayscale (black and white) image, these pixel values range from 0 to 255, where 0 is black and 255 is white.

9. ALGORITHM

The algorithm used for encryption and extraction in this application is designed to utilize multiple pages, rather than just using the LSB of the image. The written data starts at the last section (Table 8 or LSB); this is because this bit is the least significant, and all bits are doubled from the bottom. Therefore, all stages of the image level go downwards, and the resulting image is returned. The reason for using the Least Significant Bit (LSB) algorithm is its ease of implementation and the need for a simple way to embed data in the image display. In other words, by using the LSB algorithm, it is possible to save 3 bits in the pixels of an image. An 800 × 600 pixel image can store a total of 1,440,000 bits or 180,000 bits of compressed data.

10. THE STEGANOGRAPHY SYSTEM BLOCK DIAGRAM AND FLOW DIAGRAM

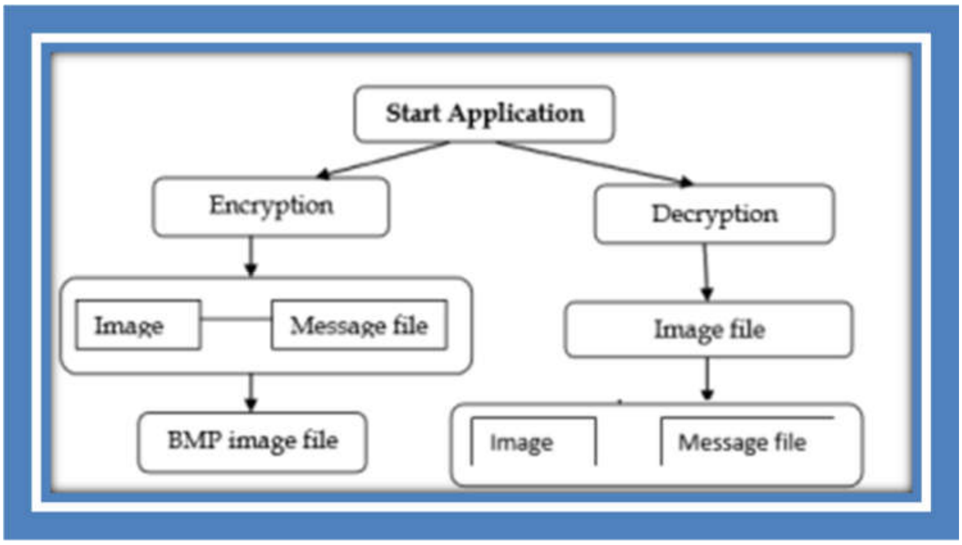

Figure 5. Steganography system block diagram and flow diagram

11. DIFFERENT TYPES OF BIG DATA ANALYTICS

11.1 Descriptive Analytics

This summarizes past data in a format that people can easily read. It helps in generating reports such as company revenue, profit, sales, and much more. It also helps in generating social media statistics.

11.2 Diagnostic Analytics

This is primarily for understanding what caused a particular problem. Strategies like data mining and data recovery are examples of this. Organizations use diagnostic analytics because it provides a deeper understanding of a specific problem.

11.3 Predictive Analytics

This type of analytics examines past and current data to make predictions about the future. Predictive analytics uses data mining, AI, and machine learning to analyze existing data and make predictions about the future. It is useful for predicting customer trends, market trends, and more.

12. SYSTEM ANALYSIS

In our tests, the core algorithm of the steganography system was tested on cover images of different sizes and color depths. Furthermore, the tests were conducted only on English and English/Arabic text. The length of the text used varied (from 1 font to any text up to 1/8th of the cover size). In this article, the masking method uses a single image. Additionally, the main masking algorithm can be easily modified to accommodate three-color channels to handle longer messages.

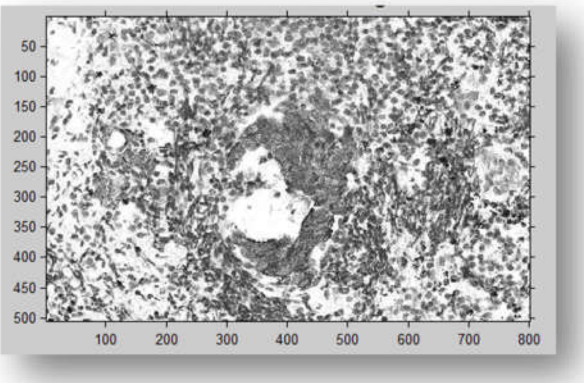

Figure 6. Original cover image

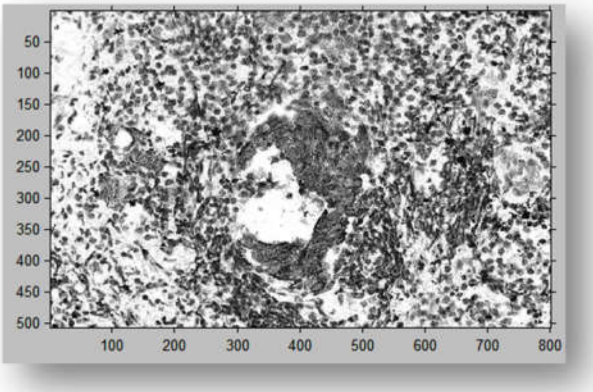

Figure 7. Hidden cover image

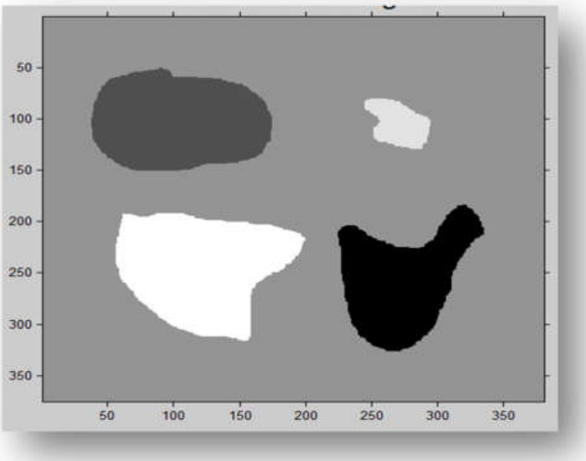

Figure 8. Original cover image

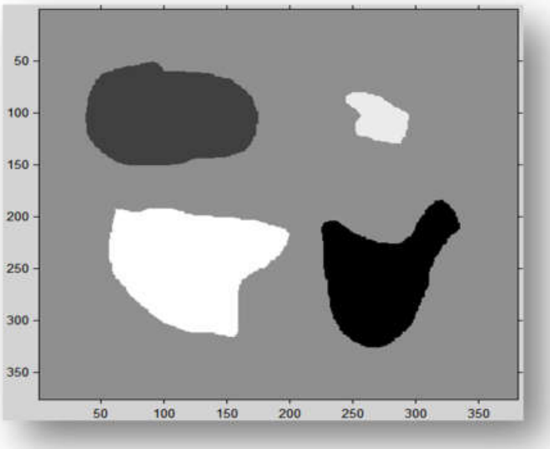

Figure 9. Hidden cover image

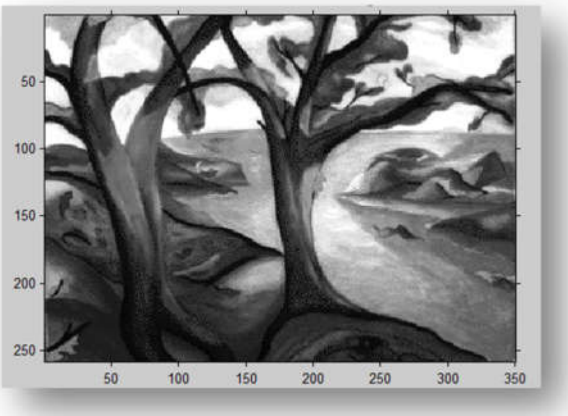

Figure 10. Original cover image

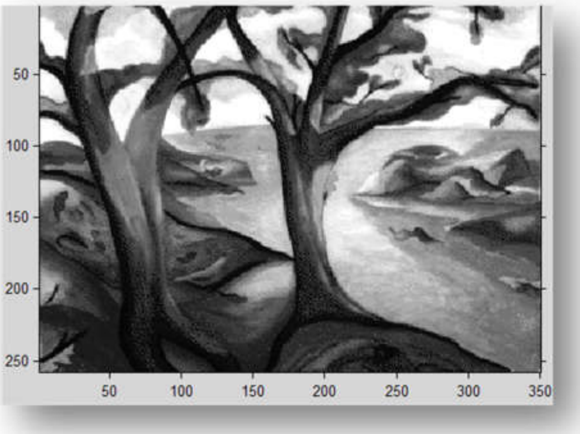

Figure 11. Hidden cover image

This system captures all types of images to conceal this information and also encodes and decodes the patterns. In this application, instead of simply using the LSB of the image, an algorithm is used to encode and embed multiple scales. The record source starts at the beginning (column 8 or LSB) of the last layer associated with this database. This is crucial compared to other components. To hide files and data, a recorder is used on the image so that no one can view the information or files. One file format is acceptable for the output, and this module can take any type of image as input.

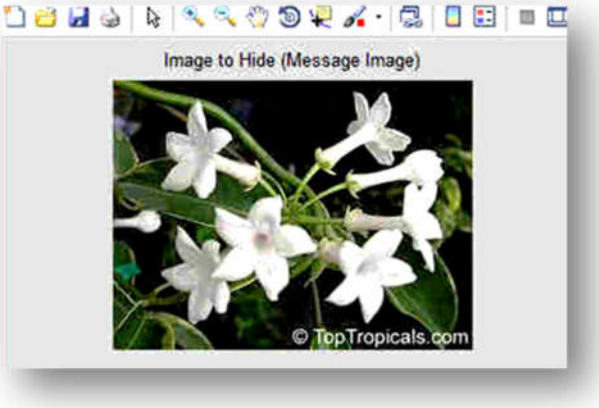

Figure 12. Image to hide

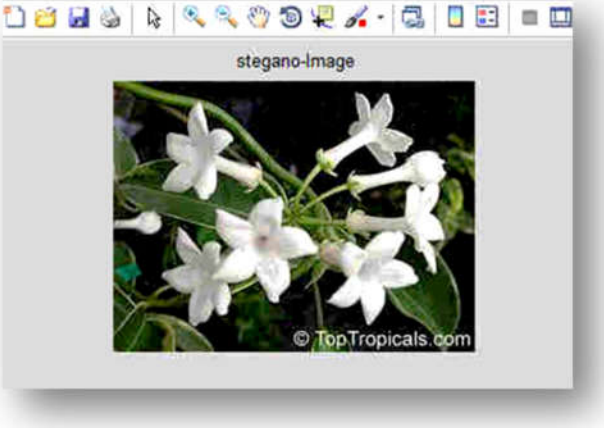

Figure 13. Stegano Image

13. CONCLUSIONS

During system testing, the LSB input system can be identified and configured using the MATLAB programming language. Encryption in English and English/Arabic languages of varying lengths is used with different colored cover images, image content, and sizes, along with stego image system effects for systematic measurement. It introduced concepts such as scraping capability, sub-clustering, double rewriting, and replication to strengthen large amounts of data. As far as we know, the algorithm is defined as an algorithm. Steganography was the first to be able to use PNG to create additional information and to prevent images from being blocked to prevent expressions. In this study, we explored the conceptual aspect of Big Data, which has recently gained considerable interest due to its unprecedented opportunities and benefits. In the information age we live in, various types of high-speed data are generated every day, and they contain patterns of descriptive information and hidden information that need to be extracted and utilized. Therefore, Big Data analytics can be used to drive business transformation and improve decision-making by utilizing advanced Big Data analytics techniques and extracting confidential and critical information.

REFERENCES

1. Bakshi, K.: Considerations for Big Data: Architecture and Approaches. In: Proceedings of the IEEE Aerospace Conference, pp. 1–7 (2012)
2. Cebr: Data equity, Unlocking the value of big data. in: SAS Reports, pp. 1–44 (2012)
3. Cooke, F.L. Plant maintenance strategy: Evidence from four British manufacturing firms. J. Qual. Maint. Eng. 2003, 9, 239–249.
4. Cuzzocrea, A., Song, I., Davis, K.C.: Analytics over Large-Scale Multidimensional Data: The Big Data Revolution! In: Proceedings of the ACM International Workshop on Data Warehousing and OLAP, pp. 101–104 (2011)
5. Dunlap, M., Hellerstein, J.M., Welton, C.: MAD Skills: New Analysis Practices for Big Data. Proceedings of the ACM VLDB Endowment 2(2), 1481–1492 (2009)
6. Economist Intelligence Unit: The Deciding Factor: Big Data & Decision Making. In: Capgemini Reports, pp. 1–24 (2012)
7. Elgendy, N.: Big Data Analytics in Support of the Decision Making Process. MSc Thesis, German University in Cairo, p. 164 (2013)
8. EMC: Data Science and Big Data Analytics. In: EMC Education Services, pp. 1–508 (2012)
9. Hvolby, H.-H.; Tseng, B. Maintenance management models: A study of the published literature to identify empirical evidence. A greater practical focus is needed. Int. J. Qual. Reliab. Manag. 2015, 32, 635–664.
10. J. Fridrich, "Deep residual network for steganalysis of digital images," IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1181–1193, 2018.
11. J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010.
12. J. Huang, and X. Li, "A new cost function for spatial image steganography," in Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), pp. 4206–4210, Paris, France, 2014.
13. J. K. Mandal, Paramartha Dutta, ―Hash Based Least Significant Bit Technique for Video Steganography (HLSB)‖, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
14. J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285–287, 2006.
15. Md. Saifur Rahman, Md. Ismail Hossain ―A New Approach for LSB Based Image Steganography using Secret Key‖, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
16. Memon, N., 2001 "Analysis of LSB based image steganography techniques ", Image Processing, Proceedings. 2001 International Conference on,pub. IEEE, Vol. 3.

17. P. Honeyman, “Hide and seek: an introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.
18. R. Ndoundam, "PDF steganography based on Chinese Remainder Theorem", Journal of information security and applications (2016), Elsevier, Vol. 29, 2016, pp. 1-15.
19. R. Roy, and S. Changder, “Secure key based image realization steganography,” in Proceedings of the 2013 IEEE 2nd International Conference on Image Information Processing (ICIIP), pp. 377–382, Shimla, India, 2013.
20. Zhang, X., Xu, Z.: RCFile, A Fast and Spaceefficient Data Placement Structure in MapReduce-based Warehouse Systems. In: IEEE International Conference on Data Engineering (ICDE), pp. 1199–1208 (2011)