IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Document Security within Institutions Using Image Steganography Technique

Suresh A.T.K.[1], **P Ebby Darney** [2,3]

[1]Lecturer in Computer Engineering, Government Polytechnic College, Vechoochira.
Directorate of Technical Education, Kerala State.
[2] Professor & Head, EEE, Raja Rajeswari College of Engineering Bangalore
[3] Research Supervisors, LIPS Research Foundation India

Abstract: ***The art or practise of hiding a message, image, or file within another message, image, or file is known as steganography. This essay examines how images on the institution's network can be used to hide papers within that organisation. The C programming language was used to create this free, self-contained, and user-friendly application. Before the document is delivered through the institution's network to the intended recipient, the encryption procedure is carried out on the user's computer. Images are encrypted and decrypted during this procedure, preventing hackers or casual users from reading documents that weren't created for them.***

Keywords: steganography, image, encrypting, decryption, image

1. Introduction

The majority of information is now stored and exchanged electronically as a result of advancements in information and communication technology (ICT). As a result, everyone is now concerned about and vulnerable to threats to information security. The number of people switching to this e-platform is steadily rising. Modern communications' expanding potential necessitate the use of sophisticated security measures, particularly on computer networks. With more data being transmitted over the internet, network security is becoming more crucial. Since unauthorised access and use must be prevented, confidentiality and data integrity are necessary [1]. As a result, the field of information security has grown tremendously. One of these security methods that is used to conceal information is the usage of images. This study examines how institutions might safeguard their internal data as they transition to electronic management. The steganography approach conceals information from the user while also disguising it as an image to divert the intrusive party from their intended goal.

2. Steganography Vs Cryptography

Different techniques and instruments have been used to safeguard information, particularly on the internet. Because of its simplicity and haziness, cryptography is used the most frequently. This strategy, however, is evidently ineffective because it invites intruders to target such secret information by openly declaring the so-called secured information to them. Additionally, a variety of effective methods have been developed to unlock information protected by this kind of information security instrument. Steganography is a contemporary information security tool that must be used in order to stop this unauthorised access to such sensitive data. Steganography, according to Bender [2], is a method of concealing information in digital.

3. Information Hiding

A new field of study called information concealing includes applications like steganography, digital media copyright protection, fingerprinting, and watermarking. For instance, in watermarking applications, the message includes data like owner identity and a digital time stamp, which are typically used for copyright protection [2]. Regarding fingerprints, the data set's owner inserts a serial number into the data that specifically identifies each user. This enhances copyright data to enable the user to be identified in the event of any unauthorised use of the data collection. [3].

Information can be protected using steganography in addition to cryptography. According to Moerland [4], steganography conceals the existence of the communication by embedding the plaintext or encrypted message in a digital host before transmitting it over the network. This kind of information hiding can be applied to copyright protection for digital media, including audio, video, and photos, in addition to data hiding for secrecy.

With more people participating in the cyberspace revolution, steganography becomes more crucial. According to Silman [5], "steganography is the technique of disguising information so that hidden messages cannot be detected. A variety of covert communication techniques, such as steganography, prevent the message from being seen or found.

Steganography concealed the private message within the host data set, made its presence undetectable, and was designed to be reliably transmitted to a recipient. The host data set is intentionally contaminated, but invisibly, so that it cannot be seen by information analysis.

4. Aim and Objective Of Research

Steganography aims to facilitate covert communication. The hidden message transmitted by stego-media must therefore not be understandable to humans in order to comply with a fundamental criteria of this steganography method. Steganography also aims to prevent suspicion of a secret message from being there. This kind of information concealment has recently grown in significance in a variety of application fields. These precise goals for this research effort are:

1) First, to offer steganography-based security technologies.

2) To investigate data-hiding methods using the research's encryption module.

3) To identify methods for obtaining confidential data using a decryption module.

4) To develop a programme that can be used to cheaply disguise sensitive company data.

5) Create a unique security solution that is user-friendly and improves information security.

5. Steganography Concepts

Although steganography is an old topic, the modern articulation of it is sometimes described in terms of Simmons' [6] prisoner's issue, when two prisoners want to communicate covertly to plan an escape. All of their correspondence goes through a warden, who, should she suspect any covert communication, will put them in solitary confinement [7].

The warden might either be passive or active, and he or she is free to review every form of communication that occurs between the inmates. A passive warden does nothing more than read the message to see whether it might contain sensitive information. A passive warden notes a covert communication that she suspects may include secret information, reports it to a third party, and allows the transmission to go unhindered. On the other hand, an active warden will attempt to purposefully alter the communication with the suspected hidden information in order to eliminate the information [8].

6. Applications of Steganography

The future of Internet security and privacy on open networks like the Internet depends heavily on steganographic technologies. Steganographic research is primarily motivated by the weakness of existing cryptographic techniques and the need for total confidentiality in an open-systems setting. Numerous governments have enacted laws that either restrict the power of cryptosystems or outright forbid them. Law enforcement has mostly done this out of a fear that they won't be able to gather intelligence through wiretaps and other means. This regrettably leaves the bulk of Internet users with either no encryption techniques at all or with encryption that is rather weak and frequently breakable. Advocates for civil liberties use the justification that "these restrictions are an assault on privacy" to counter this. Herein lies the role of steganography. Important information can be concealed using steganography inside of another file so that only the recipients are aware that a hidden message has been sent. It is a good idea to combine the usage of cryptography and steganography to increase security and alleviate the "crypto versus law" issues that were previously addressed. Since neither cryptography nor steganography are "turnkey solutions" to open systems privacy, as was already said, combining both technologies together can offer a very respectable level of privacy for anyone using these systems and communicating with them.

7. Kinds of Steganographic Systems

Almost all digital file types can be used for steganography, however those with a high level of redundancy are better ideal. Redundancy is the term used to describe parts of an object that offer precision that is significantly more than what is required for the object to be used and displayed [9]. According to Anderson & Petitcolas [8], the superfluous portions of an object are those that can be changed without the change being obvious. This criterion is particularly met by image and audio files, while research has also revealed additional file types that can be utilised to conceal information. Text, image, audio/video, and protocol/network are the four basic types of file formats that can be used for steganography.

7.1. Text Steganography

Text, audio, images, videos, and other sorts of material can all use steganography. However, because to the lack of redundancy in word compared to image or audio, text steganography is said to be the most challenging type of steganography. Data compression is one technique that could be applied to text steganography. Information in one representation is encoded into another representation using data compression. The size of the new data representation is lower. Huffman coding is one of the methods that can be used to achieve data compression. Huffman coding assigns shorter length codewords to source symbols that occur more frequently and longer length codewords to source symbols that occur less frequently. Wayner said that Unicode steganography employs characters that resemble those in the standard ASCII set to appear regular while really carrying additional bits of information. There should be no visible difference between the text and regular text if the text is displayed appropriately. However, on some computers, the fonts may appear differently, making the additional information visible [8]. The most significant steganographic technique historically involves disguising data in words. One simple technique involved placing a hidden message after every nth letter in each word of a text message. Its significance has only diminished since the invention of the Internet and all the many digital file types [4]. Digital files used for text steganography are not utilised very frequently since text files have relatively little redundant data.

7.2 Audio/Video Steganography

Similar methods to those used for image files are employed to conceal information in audio files. Masking is a separate method specific to audio steganography that uses the characteristics of the human ear to covertly conceal information. When there is another stronger, audible sound present, a faint but audible sound becomes inaudible [4]. This characteristic makes a route for information concealment. Although meaningful audio files have nearly as much steganographic potential as photos, their bigger size makes them less common to utilise than images [1].

7.3 Protocol/Network Steganography

According to Ahsan & Kundur [10], "protocol steganography refers to the method of inserting data into network control protocols and messages used in network transmission. There are covert channels in the OSI network model's layers where steganography can be applied [11]. A TCP/IP packet's header contains some fields that are either optional or never used, serving as an illustration of how information might be concealed. Common network steganography techniques require changing a single network protocol's characteristics. The PDU (Protocol Data Unit) or the temporal relationships between the exchanged PDUs may both be modified, or both (hybrid techniques). Additionally, it is possible to make use of the relationship between two or more distinct network protocols to.

7.4 Image Steganography

Images are the most widely used cover objects for steganography due to the prevalence of digital images, particularly on the Internet, and the substantial amount of superfluous bits available in a digital representation of an image. There are numerous distinct picture file formats in the world of digital photos, most of them are designed for particular uses. There are multiple steganographic algorithms for these various image file types.

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [12]. Image - also known as *spatial* domain techniques embed messages in the intensity of the pixels directly, while for transform - also known as *frequency* - domain, images are first transformed and then the message is embedded in the image [13].

8. Steganography Imperceptible property

All steganographic algorithms must abide by a few fundamental guidelines. The most crucial criteria for a steganographic algorithm is that it must be undetectable. The authors suggest a set of standards to further categorise an algorithm's imperceptibility. The following criteria apply:

8.1 Invisibility

The first and most important prerequisite for a steganographic algorithm is its invisibility, as the strength of steganography depends in its capacity to go unnoticed by the human eye. The algorithm is compromised the instant one can tell that an image has been altered.

8.2 Payload capacity

Steganography aims at secret communication, in contrast to watermarking, which only needs a tiny bit of copyright information embedded. As a result, it needs a considerable quantity of embedding capacity.

8.3 Robustness against statistical attacks

Statistical steganalysis is the process of using statistical tests on picture data to find hidden information. When information is embedded, several steganographic algorithms leave a "signature" that is simple to find via statistical analysis. A steganographic algorithm must not leave a mark in the image that is statistically significant in order to avoid being seen by a warden.

8.4 Robustness against image manipulation

An active warden may make adjustments to a stego image before it is sent via trusted systems in an effort to obliterate hidden information. Before the image reaches its destination, it can be subjected to image manipulation, such as cropping or rotation. The hidden message could be destroyed by these operations, depending on how it was implanted. Steganographic methods should ideally be resistant to both malicious and unintended alterations to the image.

8.5 Independent of file format

The fact that only one type of file format is consistently transmitted between two parties may seem suspicious given the variety of picture file formats that are utilised on the Internet. Thus, the most potent steganographic algorithms can incorporate data into any kind of file. Additionally, this addresses the issue of not always being able to locate the ideal image at the ideal time and in the ideal format to use as a cover image.

8.6 Unsuspicious files

Given the variety of picture file formats that are utilised online, it may seem odd that only one kind of file format is consistently exchanged between two parties. Thus, information can be hidden in any kind of file using the most potent steganographic methods. This also addresses the issue of not always being able to locate an appropriate image at the appropriate time and in the appropriate format to use as a cover image.

Table 1: Comparison of image Steganography Algorithm

Property	*A*	*B*	*C*	*D*	*E*
Invisibility	H*	M*	H	H	H
Payload capacity	H	M	M	L	M
Robustness against statistical attacks	L	L	M	H	H
Robustness against image manipulation	L	L	M	H	M
Independent of file format	L	L	L	H	H
Unsuspicious files	L	L	H	H	H

* Depends on cover image used

H: High, M: Medium, L: Low

Table Headings

A: LSB in BMP B:
LSB in GIF

C: JPEG compression

D: Patchwork

E: Spread spectrum

It could appear odd that only one kind of file format is consistently transferred between two parties given the variety of picture file formats that are utilised on the Internet. In order to embed information in any kind of file, the most potent steganographic algorithms are able to do so. As a result, the issue of not always being able to locate a good image at the ideal time and in the ideal format to serve as a cover image is also resolved.

9. Data Flow Diagram

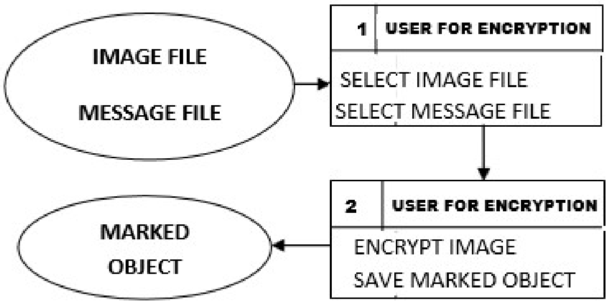


Figure 1: Data flow diagram (encryption)

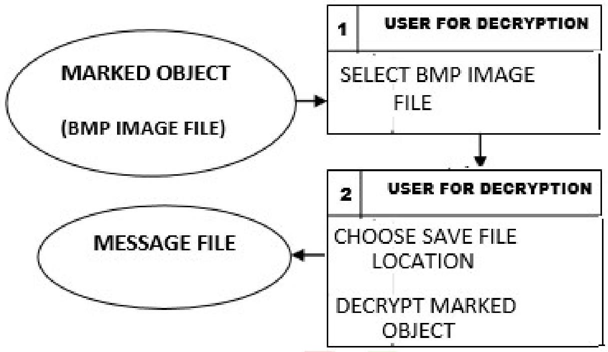


Figure 2: Data flow diagram (decryption)

The encryption and decryption components make up the steganography system, as seen in the aforementioned figures. The encryption module is chosen in order to hide the data, and the user is then prompted to select both the cover image and the embedded data. When encryption is effective, the data is buried beneath the image to create a BMP image file. The decryption module is chosen when the encrypted message is recovered. The user is then prompted to choose the marked item and the place for saving the message file that was accidentally exposed. The message file's original file name from when it was encrypted is preserved.

10. Steganography System Images

Steganography system requires any sort of picture file and the information or message that is to be disguised. It has two modules encrypt and decrypt. Microsoft.The vast array of tools and options that the Net Framework offers makes programming easier. one of them.Internet photo and image editing programmes "Auto-converting most types of pictures to BMP format" This utility is utilised in this software called "Steganography" that is created in C#.Net language. Hence, it is pretty easy to utilise this software to hide in information in any format of photographs without any necessity of converting its format to BMP. In other words, the software turns the picture on itself.

The basic inputs in the current stegosystem consist of the following:

- Image file and
- Information file

The information file can be of any type, including.doc,.docx,.pdf,.xls, etc., but the picture file must follow the bitmap format definition. The size of the picture file determines the size of information file to hide in the image. The formula relating these two parameters is presented below:

$$S \square (8.0 * (height * (width / 3) * 3) / 3 \square 1)) /1024$$

Note that: Width = width of image file,

Height = height of image file

S = maximum size of information that can be embedded by the image

11. Algorithm used

The algorithm used for Encryption and Decryption in this application is offered employing numerous layers in stead of using simply LSB layer of picture. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. Therefore, image quality degrades and image retouching occurs as we move up the layers.

The argument behind the choice of the Least Significant Bit (LSB) algorithm is because insertion is easy and requires simple approach to embedding information in a cover image. In other words, by employing LSB technique, storing 3 bits in each pixel of the image is made possible. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. A 24-bit image's grid for three pixels, for instance, might look like this:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this area of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference

12. Justification of Programming Language

Strong typing, imperative, declarative, functional, generic, object-oriented (class-based), and component-oriented programming paradigms are all supported by the multi-paradigm programming language C#. It was created by Microsoft as part of the.NET program, and Ecma (ECMA-334) and ISO (ISO/IEC 23270:2006) eventually accepted it as a standard. A programming language made specifically for the Common Language Infrastructure (CLI) is C#.

The rationale behind the choice of C# in the design of this system is conspicuously highlighted below:

- C# is a straightforward, cutting-edge, all-purpose, object-oriented programming language.

- C# makes an effort to make the syntax simpler so that the system's architecture is more rational and consistent.

- It boosts programmer efficiency and offers software robustness and endurance.

- It improves the portability of both source code and programmers.

- C# may be used to create applications for both hosted and embedded systems, from the very big, which employ sophisticated operating systems, to the very small, which have specialised functionalities.

- C# applications need less memory and processing power than other programming languages. By utilising.NET's garbage collection system, C# frees developers from worrying about memory management. The Framework can release memory as needed by performing garbage collection on items that are no longer referenced.

13. The Steganography System Block Diagram and Flow Chart

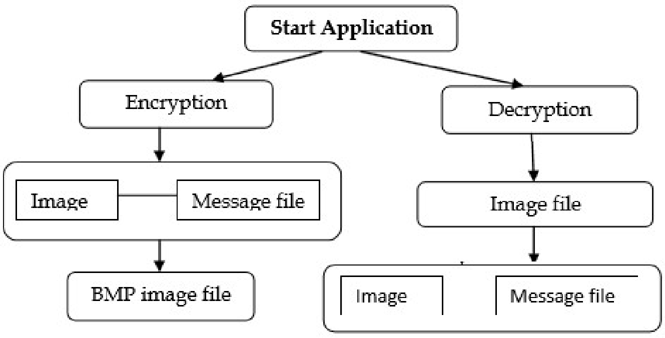


Figure 3: System block diagram

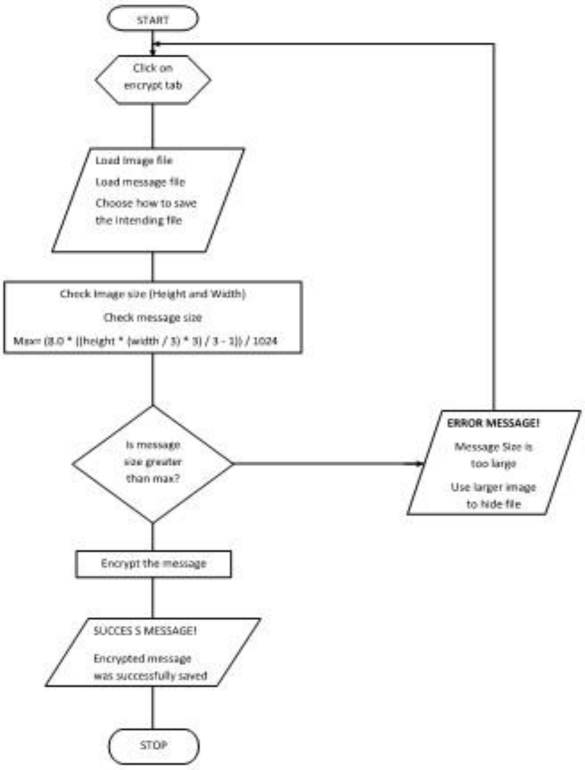

START
Click on encrypt tab
Load image file
Load message file
Choose how to save the intending file
Check image size (Height and Width)
Check message size
Max= (8.0 * ((height * (width / 3) * 3) / 3 - 1)) / 1024
Is message size greater than max?
ERROR MESSAGE!
Message Size is too large
Use larger image to hide file
Encrypt the message
SUCCES S MESSAGE!
Encrypted message was successfully saved
STOP

Figure 4: System flow chart.

14. The System Model and Output Screens and Implementation

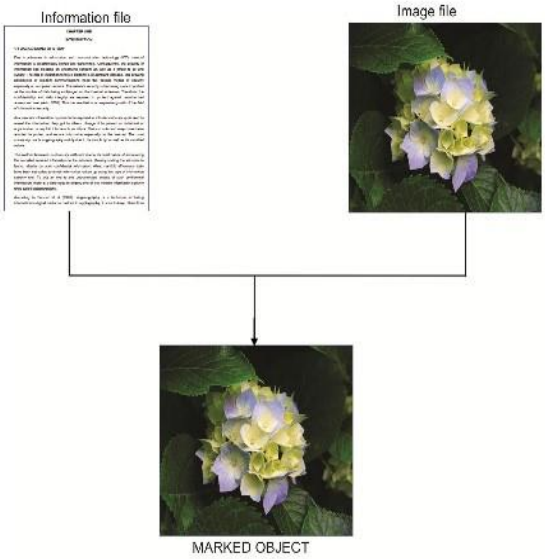


Figure 5: Encryption process model

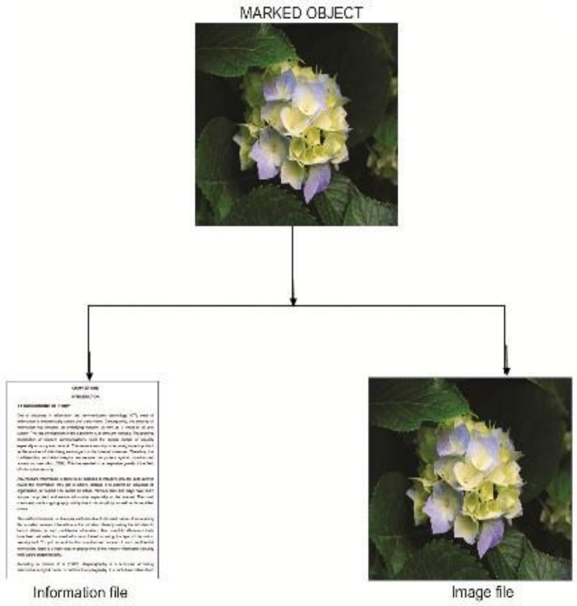


Figure 6: Decryption process model

In figure 6, a document is hidden i.e. encrypted inside an image to form a “marked object”, while the marked object in figure 7 is decrypted to generate the original document encrypted. This process describes the steganography process described in the paper.

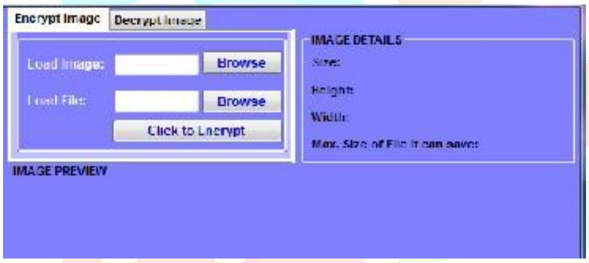
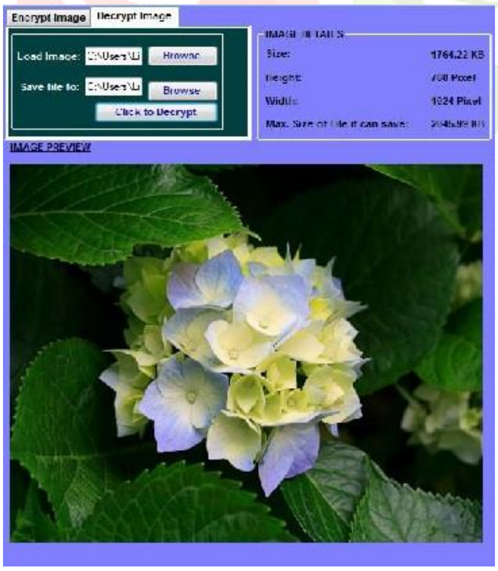


Figure 7: The steganography system image select screen



Load Image: C:\Users\Li

Save file to: C:\Users\Li

Size: 1764.22 KB

Height: 768 Pixel

Width: 1024 Pixel

Max. Size of File it can save: 2045.99 KB

Figure 8: The steganography system after selecting the image and file

Encryption and decryption modules make up the system. Information is concealed in an image using the encrypt module; neither the information nor the file is visible to anyone. This module accepts any kind of image and message and outputs a single image file. To unlock the information that is buried within an image file, utilise the decrypt module. It uses the image file as an input and outputs two files—one of which is the identical image file and the other is a message file that is concealed within it—into the destination folder.

Before encrypting the file inside the image, we must save the file's name and size in a certain location on the image. In the LSB layer, we might save the file name before the file information and the file size and file name size in the image's most right-down pixels. To retrieve a file from an encrypted image in the decrypted state, this information must be written. Microsoft C#.Net 2008-based software is compiled, packed, created, and released to become an executable stand-alone programme. Now, other computer systems can run the software after installation.

To use the software the user needs to run the application. The user has two tab options -encrypt and decrypt which appear as adjacent tabs at the top left-hand corner of the program. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file. For encryption operation, the user first clicks on the encrypt tab to select the module. He then clicks on the image browse button to surf for the location of the image and select the image. At the top right hand corner of the system, the image information (size and height) as well as the maximum size of the message it can hide in Megabytes is well displayed. After this, the user then proceeds to the "information file" browse button to choose the information file to be hidden. Finally, the user clicks on the encrypt button and the system prompts him to save the message by choosing the location and the file name. This is sequentially followed by waiting information by the system to show the processing status of the system. On the other hand, to decrypt an already encrypted message using the system, the user first selects the decrypt tab followed by the image browse button to select the message to be decrypted. At the tail end of the process, the user selects the "decrypt button" and where to save the decrypted message.

15. System Documentation

15.1 Hardware Requirement

This has to do with the basic hardware the system needs to possess for optimum performance and includes system unit with the following configuration:

Table 2:

Parameter	*Minimum Requirement*
Processor	1GHz
Hard disk	1 GB
RAM	512MB
Operating System	Windows xp or latter

System requirement

15.2 Software Requirement

For effective functioning of this software, there is a software platform required to run on the system. This software tool acts as a platform for the new system to work. Here, I am referring to .NET Framework of at least version 3.5

15.3 Manpower or Operational Requirement

This deals with the skill and personal energy which is a necessary and/or otherwise the prerequisite for the functioning and manipulation of the system. The system however is easy to operate and manipulate even as little or no training is required for its operations.

15.4 Environmental Requirement

This has to do with the overall requirement of the environment in which the system operates. For this system to work well, it needs a dust free environment Air conditional

15.4 System Maintenance

System maintenance ensures that errors which appear during operation of the system are eliminated. It also implements system changes and expansions.

Therefore, this section is dedicated to outline the ways necessary for maintaining the new system, which are: Proper handling of the system: This entails starting up (booting) and rebooting the system rightly to prevent file corruption or system "halting".

- Scanning regularly the hard disks and floppy disks used in the system to avoid the invasion of viruses, horses and worms.
- To avoid sudden breakdown of the system, the computer hardware should be serviced regularly.

16. Summary and Recommendation

16.1 Summary

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

In addition, it has been proved beyond reasonable doubt that, stegosystem has quite a multitudinous applications both in individual transactions and business dealings. It complements the existing system to leave up legal band and to reinforce the present level of security.

16.2 Recommendations

Steganography is seen as a high-level type of encryption; hence, I recommend it to be used in information security within institutions as its use will results in a mechanism to implement two of the five key pillars of information security, namely confidentiality and integrity. Here, the confidentiality of the hidden message is protected due to it being unrecognisable in its hidden and encrypted form both in the place of storage and during transmission while the encrypting of the concealed message protects the integrity of the data.

Besides this, I also recommend more research to be done in the area of stego-key provision to ensure absolute lock of the information being transmitted in this stego-system. Again, applications of steganography are wide ranging, and are indeed valuable if used in the correct manner. Therefore, I would like to recommend the use of this new technology in business and individual transactions to reduce cost and enhance the net revenue of such business or individual as the case may be. Since neither Cryptography nor Steganography are considered "turnkey solutions" to open systems privacy, I recommend the use of both technologies together to provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems. Finally, since this security technology may be misused and abused, resulting in disastrous consequences, I recommend the use of official instrument to control the transmission of embedded information through Steganography to check the use of such tool in concocting criminal and inhumane plots in the society.

References

[1] Artz, D. (2001). Digital Steganography: Hiding Data within Data. *IEEE Internet Computing Journal*, (June).

[2] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., (1996). Techniques for data hiding. *IBM Systems Journal*, 35(2).

[3] Dunbar, B. (2002). Steganographic techniques and their use in an Open-Systems environment. SANS Institute, January.

[4] Moerland, T.(2001). Steganography and Steganalysis. *Leiden Institute of Advanced Computing Science.* Accessed September 12, 2012. Available from www.liacs.nl/home/ tmoerl/privtech.pdf

[5] Silman, J.,(2001). Steganography and Steganalysis: An Overview. *SANS Institute.*

[6] Simmons, G., (1983). The prisoners problem and the subliminal channel. *CRYPTO.*

[7] Chandramouli, R., Kharrazi, M. & Memon, N.(2003). Image steganography and steganalysis: Concepts and Practice. *Proceedings of the 2nd International Workshop on Digital Watermarking*, October.

[8] Anderson, R.J. & Petitcolas, F.A.(1998). On the limits of steganography. *IEEE Journal of selected Areas in Communications*, (May): 22.

[9] Currie, D.L. & Irvine, C.E., (1996). Surmounting the effects of lossy compression on Steganography. *19th National Information Systems Security Conference*.

[10] Ahsan, K. & Kundur, D.(2002). Practical Data Hiding in TCP/IP. *Proceedings of the Workshop on Multimedia Security at ACM Multimedia.*

[11] Handel, T. & Sandford, M.(1996). Hiding data in the OSI network model. *Proceedings of the 1st International Workshop on Information Hiding*, June.

[12] Silman, J.,(2001). Steganography and Steganalysis: An Overview. *SANS Institute.*

[13] Lee, Y.K. & Chen, L.H. (2000). High capacity image steganographic model. *Visual Image Signal Processing,* 147(03), June.

[14] John B, A., Jeyan, J. V. M. L., NT, J., Kumar, A., Assessment of the Properties of Modified Pearl Millet Starch. *Starch.* 2022, 2200160.

[15] Suman Rana,Bhavin Soni,Dr. P. Ebby Darney,Jyothi NT, "EFFECTS OF T4 HORMONES ON HUMANBODY AND THEIR ANALYSIS", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.10, Issue 10, pp.d332-d339, October 2022,

[16] Ashika Parveen1, JV Muruga Lal Jeyan[2], Jyothi NT[3] International Study on Application of Value Stream Mapping to Identify the Necessity of Lean System Implementation , International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930

[17] JV Muruga lal Jeyan, Jyothi NT Rashi Kaushik Systematic Review and Survey on Dominant Influence of Vedas and Ignorance Transpired in Space Science and Aviation", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 7, page no.b490-b493, July-2022,

[18] JV Muruga lal Jeyan, Jyothi NT , Boopesh Raja, Rajarajan G "THEORY STRATEGY OF SUBSONIC WIND TUNNEL FOR LOW VELOCITY ", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.j572-j580, June-2022,

[19] JV Muruga lal Jeyan, Jyothi NT, Reshmitha Shree, Bhawadharanee S, Rajarajan, THEORETICAL STUDY OF HYPERSONIC WIND TUNNEL TEST FACILITY IN INDIA ", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.j512-j518, June-2022,

[20] JV Muruga lal Jeyan, Jyothi NT , V S Devika Thampuratty, B Nithin, Rajarajan, CONCEPT DESIGN AND DEVELOPMENT OF SUPERSONIC WIND TUNNEL ", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.9, Issue 6, page no. ppj209-j217, June-2022,

[21] Muthu Venkatesh, Rajarajan G Jyothi NT JV Muruga Lal Jeyan "Systematic Survey of Wind Tunnel Test facility in India", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.9, Issue 6, page no.h830-h840, June-2022,

[22] Ashika Parveen, JV Muruga Lal Jeyan, Jyothi NT "Investigation Of Lean Developments And The Study Of Lean Techniques Through Event Studies" Internation Journal for Science and Advance Research In Technology, 8(4)

[23] P Gopala Krishnan, JV Muruga Lal Jeyan, Jyothi NT "Novel Evaluation Of Aircraft Data Structure Optimization Techniques And Opportunities" International Journal for Science and Advance Research In Technology, 8(4)

[24] Suryansh Upadhyay, JV Muruga lal Jeyan, Jyothi NT Preliminary Study on Brain Computer Interface © August 2021| IJIRT | Volume 8 Issue 3 | ISSN: 2349-6002 IJIRT 152537 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY 720

[25] Sruthi.s.kumar, Jyothi Nt , Jv Muruga lal jeyan . Computational Turbine Blade Analysis with Thermal Barrier Coating International Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 12, Issue 4, (Series-I) April 2022, pp. 01-08, DOI: 10.9790/9622-1204010108