QUAID-E-AWAM UNIVERSITY OF ENGINEERING, SCIENCE & TECHNOLOGY NAWABSHAH



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**Project Title:**

Enhancing Image Steganography Techniques for Secure Communication

**GROUP MEMBERS**

|  |  |  |
| --- | --- | --- |
| Names | Roll Number | Designations |
| Ubaidullah | 20IT-16 | Leader |
| Waqas | 20IT-07 | Members |
| Sawera | 20IT-64 | Members |
|  |  |  |

**Supervisor: Dr. Saima Siraj Soomro**

Signature **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Abstract**

Steganography, the practice of concealing communication, involves embedding information within other data to mask its presence. While various carrier file formats are applicable, digital images, prevalent on the Internet, are the most favored. Numerous steganographic techniques, varying in complexity and strengths, are available for concealing secret information in images. These techniques cater to different application needs, with some prioritizing absolute invisibility of the hidden information, while others emphasize accommodating larger secret messages. Additionally it aims to delineate the requisites of an effective steganographic algorithm, offering insights into the suitability of specific techniques for various applications.

**1. Introduction:**

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Stegangraphy is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information [1].

The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message [2].

In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period [3].

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [4].

**2.Literature Review**

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [5].

These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are “marked” in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [6].

With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial . A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [7].

Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether, forcing people to study other methods of secure information transfer. Businesses have also started to realise the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [8].

Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file. This reflection is based on a set of criteria that we have identified for image steganography. Gives the reader an overview of steganography in general and differentiates between different kinds of steganography.

**3. Problem Statement**

Steganography is pivotal for securing digital communication in the internet age, using covert methods to conceal information within digital images. Advancements in steganographic techniques are essential to meet the demands of diverse applications, emphasizing imperceptibility and the accommodation of larger secret messages. The field encompasses Image Domain techniques, manipulating pixel intensities, and Transform Domain techniques, offering format-independent solutions through pre-embedding transformations. Selecting an optimal steganographic algorithm involves navigating trade-offs in invisibility, payload capacity, robustness, and file format independence. The integration of steganography with cryptography, watermarking, and fingerprinting complicates evaluation, requiring a comprehensive understanding of their convergence. The challenge is to define effective steganographic algorithms, considering technique strengths and weaknesses, to enhance digital security and adapt to evolving communication landscapes.

**4. Methodology**

* 1. **) Algorithm Design:**

Develop a conceptual framework for the steganographic algorithm, incorporating insights from the literature review. Decide on the approach, whether focusing on Image Domain, Transform Domain, or a hybrid model. Integrate key elements such as bit-wise manipulation and transformation techniques.

**4.2) Implementation:**

Translate the conceptual design into a functional steganographic algorithm using a suitable programming language. Ensure compatibility with various image file formats and compression methods, optimizing the algorithm for efficiency and speed.

**4.3) Testing and Evaluation:**

Conduct rigorous testing to assess the algorithm's performance and effectiveness. Evaluate imperceptibility, payload capacity, and resistance against different attacks. Test with various image file formats, sizes, and compression levels, comparing results with benchmark algorithms.

**4.4) Integration with Other Technologies:**

Explore opportunities to integrate the steganographic algorithm with cryptography, watermarking, and fingerprinting technologies. Assess how convergence enhances overall security and mitigates vulnerabilities. Ensure seamless interoperability.

**4.5) Optimization and Fine-Tuning**:

Identify areas for optimization based on testing results and user feedback. Fine-tune algorithm parameters to balance conflicting requirements. Enhance adaptability to dynamic communication channels and evolving security needs.

**4.6) Documentation:**

Document the entire development process, including algorithm design, implementation details, testing methodologies, and results. Provide a comprehensive user guide for integrating the algorithm into various applications.

**4.7) Publication and Dissemination:**

Share findings and insights through research papers, conference presentations, or relevant channels. Contribute knowledge to academic and professional communities about the developed steganographic algorithm and its potential applications.

**4.8) Continuous Improvement:**

Establish a feedback loop for continuous improvement. Gather user feedback, monitor the algorithm's performance, and incorporate updates to address identified issues. Stay informed about advancements in steganography and related fields for ongoing refinement and innovation.

**5. Steganography Concepts:**

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner’s problem proposed by Simmons [9], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [10].

**5.1) Various Types of Steganography:**

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display [11]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography.

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every letter of every word of a text message. It is only since the beginning of the

Internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data. Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography. To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used [12].

An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

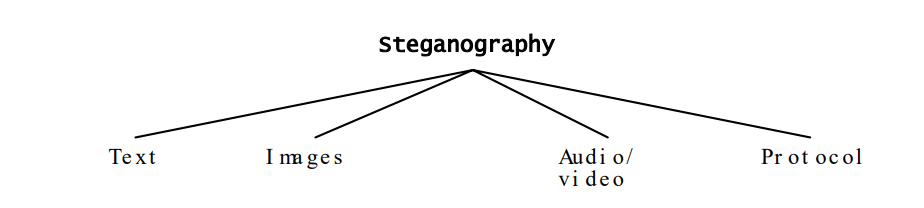


Fig: 1 shows the four main categories of file formats that can be used for steganography.

**5.2) Image Steganography:**

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist [13.]

**5.3) Image Definition:**

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its colour [14].

These pixels are displayed horizontally row by row. The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel.

The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [15].

Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours Not surprisingly the larger amount of colours that can be displayed, the larger the file size [16].

**5.4) Image Compression:**

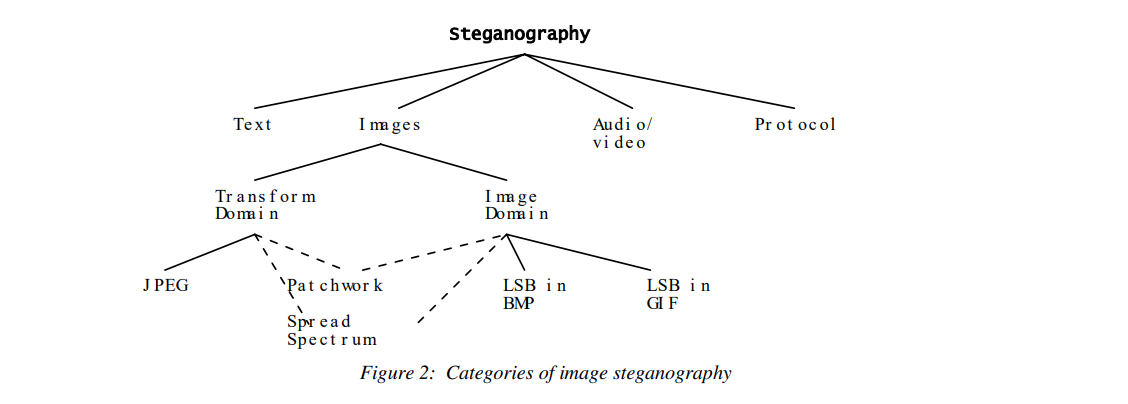
When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image’s file size. These techniques make use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. This process is called compression. In images there are two types of compression: Both methods save storage space, but the procedures that they implement differ. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group). Lossless compression, on the other hand, never removes any information from the original image, but instead represents data in mathematical formulas. The original image’s integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file). Compression plays a very important role in choosing which steganographic algorithm to use. Lossy compression techniques result in smaller image file sizes, but it increases the possibility that the embedded message may be partly lost due to the fact that excess image data will be removed. Lossless compression though, keeps the original digital image intact without the chance of lost, although is does not compress the image to such a small file size. [17].

**5.5) Image and Transform Domain:**

Steganography techniques in image concealment fall into two categories: those operating in the Image Domain and those in the Transform Domain [18]. In the Image Domain, also termed spatial domain, messages are directly embedded in pixel intensity. Conversely, the Transform Domain, also known as the frequency domain, involves transforming images before message embedding [19].

Image Domain techniques employ bit-wise approaches, involving bit insertion and noise manipulation, often labeled as "simple systems" [20]. These techniques are most compatible with lossless image formats, relying on the specific characteristics of each format [21].

In the Transform Domain, algorithms and image transforms are manipulated for steganography [22]. This approach embeds messages in more significant areas of the cover image, enhancing robustness . Transform Domain methods are often format-independent, allowing embedded messages to withstand conversion between lossy and lossless compression [23].



**6. Conclusion:**

Each major image file format offers distinct methods with varying strengths and weaknesses. Payload capacity and robustness often present a trade-off, such as the patchwork approach excelling in robustness but limiting information concealment. Least significant bit (LSB) insertion in both BMP and GIF compensates for this limitation but raises suspicion due to resulting suspicious files. The choice of a steganographic algorithm depends on the application's requirements, and compromises may be necessary to prioritize certain features for enhanced security.

**List of references:**

[1] Bukhari, S., Arif, M.S., Anjum, M.R. and Dilbar, S., 2016, August. Enhancing security of images by Steganography and Cryptography techniques. In 2016 Sixth International Conference on Innovative Computing Technology (INTECH) (pp. 531-534). IEEE.

[2] Silman, J., “Steganography and Steganalysis: An Overview,” SANS Institute, 2001.

[3] Jamil, T., “Steganography: The art of hiding information is plain sight,” IEEE Potentials, 18:01, 1999.

[4] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis,” Communications of the ACM, 47:10, October 2004.

[5] Anderson, R.J. &Petitcolas, F.A.P., “On the limits of steganography,” IEEE Journal of selected Areas in Communications, May 1998.

[6] Marvel, L.M., Boncelet Jr., C.G. &Retter, C., “Spread Spectrum Steganography,” IEEE Transactions on image processing, 8:08, 1999.

[7] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment,” SANS Institute, January 2002.

[8] Artz, D., “Digital Steganography: Hiding Data within Data,” IEEE Internet Computing Journal, June 2001.

[9] Simmons, G., “The prisoners problem and the subliminal channel,” CRYPTO, 1983.

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

[11] Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography,” 19th National Information Systems Security Conference, 1996.

[12] Handel, T. &Sandford, M., “Hiding data in the OSI network model,” Proceedings of the 1st International Workshop on Information Hiding, June 1996.

[13] Ahsan, K. &Kundur, D., “Practical Data hiding in TCP/IP,” Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[14] Johnson, N.F. &Jajodia, S., “Exploring Steganography: Seeing the Unseen,” Computer Journal, February 1998.

[15] “Reference guide: Graphics Technical Options and Decisions,” http://www.devx.com/projectcool/Article/19997.

[16] Owens, M., “A discussion of covert channels and steganography,” SANS Institute, 2002.

[17] Johnson, N.F. &Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software,” Proceedings of the 2nd Information Hiding Workshop, April 1998.

[18] Venkatraman, S., Abraham, A. &Paprzycki, M., “Significance of Steganography on Data Security,” Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.

[19] Krenn, R., “Steganography and Steganalysis,” http://www.krenn.nl/univ/cry/steg/article.pdf.

[20] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model,” Visual Image Signal Processing, 147:03, June 2000.

[21] Provos, N. &Honeyman, P., “Hide and Seek: An introduction to steganography,” IEEE Security and Privacy Journal, 2003.

[22] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding,” IBM Systems Journal, Vol 35, 1996.

[23] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., “Information Hiding – A survey,” Proceedings of the IEEE, 87:07, July 1999.

# Names & Signature of Student(s):

1. Ubaidullah Qureshi
2. Waqas
3. Sawera

**Name & Signature of Supervisor**

-------------------------------------------

**Signature of Chairmen**

-------------------------------------------