Image Steganography: Current Landscape and Critical Challenges

Manas Chorge[1], Anusha P. P[2]

[1]Student, Department of Computer Science, Nagindas Khandwala College, Mumbai
[2]Professor, Department of Computer Science, Nagindas Khandwala College, Mumbai

Abstract

The practice of hiding secret information in digital images is known as steganography. In the course of time, this practice has grown immensely. Our paper looks closely at what is going on at present in image steganography. We are detailing old and new tools. We will discuss big issues related to this field, making such a practice hard to attack, tough to spot, and able to hold more data. We will also explain herein how steganography can be enhanced by machine learning. Finally, we suggest some new areas to be researched, these suggestions aims to solve the main problems and reach to a practical image steganography system.

Keywords: Image Steganography Least Significant Bit, Discrete Cosine Transform, Discrete Wavelet Transform, Machine Learning, Robustness, Detection, Information Hiding

Introduction

Image steganography involves hiding information in digital images, which offers a secure way to communicate information through digital means. This is in comparison to encryption, which uses complex algorithms to gar information. Instead, steganography embeds data in a way that does not easily draw attention from people or machines. Ever since the inception of this field, tremendous maturity has occurred due to the developments made in respect to digital image processing and information security.

Image steganographic techniques used simple methods of image pixel values manipulation at first to conceal secret data, but over time, techniques improved and today, they are complex algorithms hiding the hidden data very well and making it not only difficult to discover with a mere glance, but even difficult to discover for sure. Big steps forward have been taken with the creation of so-called Least Significant Bit methods, working with a change of the least important bits of image pixels, and such advanced approaches: Discrete Cosine Transform and the based on it, wavelet ones.

Importance and Applications

Image steganography impacts on digital watermarking important areas that are used to protect copyright, secure communication for military and intelligence work and secret data sharing in routine digital communication. It can also be used in digital forensics and maintain the data venture to safeguarding the information and detecting and protecting against hidden data as well as in finding hidden data venture.

Categorization

We categorized steganographic techniques in:

- Spatial domain techniques:

In this categorization, techniques hiding information in the pixel values directly.

- Frequency Domain Techniques: They modify the frequency components of the image.
- Machine Learning Techniques: These are highly advanced techniques that use machine learning algorithms `lll to enhance the quality of the steganographic process. State of the Art Image Steganography Techniques Spatial Domain Techniques
- Least Significant Bit (LSB) Insertion

LSB insertion is the simple and common method among all. It replaces the least significant bits of the pixels by the message bits for message embedding. This method is widely used as it is very easy to apply. But LSB insertion has weakness, which is added because the typical manipulations applied to images include compression and filtering. The PVD method uses the Pixel Value Differencing approach.

PVD does better than LSB by hiding information based on the differences in pixel values, which makes it more imperceptible with increased capacity. The technique, however, remains highly sensitive to high levels of image manipulations.

Frequency Domain Techniques

Discrete Cosine Transform (DCT)

This type of steganography works on the frequency coefficients of an image and embeds the desired information. Because of the fact that the DWT is more robust to compression and noise, its use is enormous for JPEG image formats, as it balances the rate of data holding capacity with the extent of hiding.

Discrete Wavelet Transform (DWT)

DWT outperforms others based on its robustness and capacity. It hides the information within different frequency sub-bands of the image. This scheme can protect better against some sorts of image processing attacks.

Machine Learning Techniques

Deep Learning Models: New strides in the field use deep learning models such as Convolutional Neural Networks (CNN) for finding the best features to hide and extract information in the process of steganography. Such models are expected to improve the quality of steganography.

Generative Adversarial Network (GAN) People have started using GANs in developing steganographic methods that can better resist detection and analysis. They are showing promising results in stego-images that look just like cover images.

Critical Challenges

Compression: There are compression methods, like JPEG, that decrease the quality of stego-images. This fact makes hidden data more prone to damage. The techniques should be robust until these changes happen, so that the data is safe.

Noise and Resizing: Stego-images may break because of the addition of noise or during resizing. This can distort or erase the data inside. Making sure they can handle these issues is still quite problematic.

Detection and Extraction:

Steganalysis As people come up with smarter ways to hide data, ways to find it get smarter too: Steganalysis—looking at images to find hidden info—often needs complex math and computer skills. • Trade-offs There is a strong interplay between capacity, imperceptibility, and robustness. The methods supporting larger capacity usually make more visible changes; the ones with a higher degree of attention to imperceptibility might be at the detriment of data capacity.

Computational Complexity—Most of the recent techniques are computationally intensive, in particular, when machine learning comes into play. Designing an efficient algorithm without any loss in performance is the real need for current real-world applications.

Methods to enhance robustness would need to develop to face all kind of attacks with compression and noise. Adaptive steganography or multi-level embedding could provide solutions.

Recommendations

We need to come up with a better Steganalysis if we are going to be one step ahead of up-coming Steganographic approaches. This can be achieved through the use of enhanced algorithms that can capture and recover the least absolute changes in the stego-images.

Data Capacity, Invisibility and Computing Complexity

Later research should help to balance the data capacity, invisibility, and computing complexity. Such a solution can be feasible through the use of a combination of techniques.

Machine Learning

We need to continue with the development in the search for methods of machine learning including GANs and deep models of learning. These, then, can be used in the development of steganographic methods that are shall be more effective and resilient.

Conclusion

Image steganography remains an area very hot and changing, rife with huge uses and issues. Old methods, including LSB and DCT, open windows of opportunity but set the stage, whereas new ways using machine learning present feasibility. Big issues concerning the strength found in hidden messages and how much computer power is needed are questions that may be answered. To continue learning and come up with new ideas in solving problems, we should always pursue the way toward developing still better and more useful image steganography.

References

1. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336. https://www.researchgate.net/publication/220354258_Techniques_for_Data_Hiding
2. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32-44. https://www.researchgate.net/publication/3437465_Hide_and_seek_An_introduction_to_steganography
3. Ker, A. D., & Pevnỳ, T. (2013). The square root law in stegosystems. Proceedings of the 12th ACM Workshop on Multimedia and Security (pp. 107-116). https://link.springer.com/chapter/10.1007/978-3-642-16435-4_12
4. Desai, H. V. (2014). Steganography of text and images using fractals. http://hdl.handle.net/10603/46087
5. Satyavathy, G. (2014). Secure message transmission for image steganography in peer-to-peer routing http://hdl.handle.net/10603/38614