International Journal of Research in Engineering, Science and Management
Volume-2, Issue-6, June-2019
www.ijresm.com | ISSN (Online): 2581-5792

Image Steganography

Juhi Aggarwal[1], Shrey Upadhyay[2], Vikas Swain[3]
[1]*Professor, Dept. of Computer Science and Engg., Babu Banarsi Das Institute of Technology, Ghaziabad, India*
[2,3]*B.Tech. Student, Dept. of Computer Science and Engg., Babu Banarsi Das Inst. of Tech., Ghaziabad, India*

***Abstract*: Steganography is the practice of concealing messages in such a way that no one can know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties i.e., sender and receiver. This project will express how Steganography is used in a modern framework while providing a practical considerate of what Steganography is and how to achieve it.**

***Keywords*: Image Steganography**

1. Introduction

Steganography is the process of concealing messages within a larger one in such a way that no one can know the presence or contents of the secreted message. While related, Steganography is not to be muddled with Encryption, which is the process of making a message inarticulate. Steganography attempts to hide the presence of communiqué. The basic structure of Steganography is made up of three components: the "carrier", the message, and the key. The transporter can be a landscape, a digital image, an mp3, even a TCP/IP package among other things. It is the entity that will 'carry' the secreted message. A key is used to decrypt /decipher /determine the hidden message. This can be whatever from a password, a pattern, a black-light, or even lemon fluid. Under this venture we will emphasis on the practice of Steganography inside alphanumeric images (BMP and PNG) using LSB Substitution, although the chattels of Image Steganography may be substituted with audio mp3's, zip archives, and any other digital article format relatively effortlessly.

2. Applications

Image Steganography has many applications, specifically in today's modern, high-tech biosphere. Confidentiality and concealment are a concern for maximum individuals on the internet. Image Steganography permits for two parties to communicate surreptitiously and covertly. It harmonies for some morally-conscious individuals to carefully whistle blow on internal actions; it allows for copyright protection on digital documents using the message as a cardinal watermark. One of the other main uses for Image Steganography is for the transference of high-level or top-secret documents between international governments. While Image Steganography has many genuine uses, it can also be quite nefarious. It can be used by hackers to refer viruses and trojans to negotiation machines, and also by terrorists and other organizations that rely on covert operations to communicate surreptitiously and safely.

3. Implementation

There are presently three effective methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification.

- LSB (Least Significant Bit) Substitution is the procedure of altering the least important bit of the pixels of the carrier image. Blocking the whole thing by breaking up an image into "blocks" and using Discrete Cosine Transforms (DCT). Each block is wrecked into 64 DCT factors that estimated luminance and color—the values of which are modified for walloping messages. Palette Modification replaces the idle colors inside an image's color palette with colors that represent the hidden message.

4. Recognition attacks

While the determination of Steganography is to fleece messages, it may not be very operative at doing so. There are several attacks that one may implement to test for Steganographic images they are: Visual Attacks, Enhanced LSB Attacks, Chi-Square Analysis, and other statistical scrutinizes. In execution a visual occurrence you must have the original "virgin" image to compare it the Steganographic image and visually relate the two for artifacts. In the Enhanced LSB Attack, you process the image for the least noteworthy bits and if the LSB is equal to one, multiply it by 255 so that it becomes its extreme value. Procedures and bit masking, somewhat that we have never understood earlier. This project was enjoyable from the start and only got more interesting as we went on emerging it. We became more attentive in the subject the more we explored on it. We have learnt that while executing Image Steganography, it is vital thinking of how to detect and attack it and the methods to do so are far more complex than actually doing the Steganography itself. There is a lot of research that is commencement to discover new ways to detect Steganography, most of which involves some disparity of statistical breakdown.

References

[1] https://en.wikipedia.org/wiki/Steganography
[2] https://www.slideshare.net/sharafshaik/ppt-steganography
[3] https://dictionary.cambridge.org/dictionary/english/steganography