



Investigation and Development of a Steganography Application

Author: Dominic Luke Bamsey

School of Applied Computing, Faculty of Architecture, Computing and Engineering, University of Wales Trinity St David, Mount Pleasant, Swansea, SA1 6ED, Email:

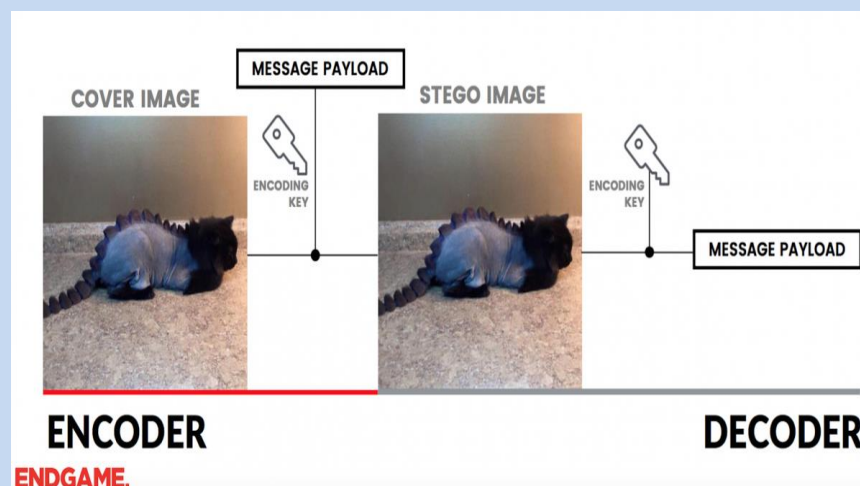
dbamsey.142820@student.uwtsd.ac.uk

Overview

Steganography means “cover writing” in Greek and it is a method of communicating through hidden messages stored in objects. The data is hidden in an image by a technique called encoding and the encoded image is known as a “stego” image.

The message is encoded into an image and is then sent over an unsecured network to a particular person, who then decodes the “stego” image and retrieves the data from the image. [1]

This is very useful for people looking to conceal data, so that only people with the access codes can decode and view the data. The application of steganography can include covert communication and image tamper proofing for example water marking.[4]



Objectives and Aims

- Investigate the current steganography techniques and software that use steganography.
- Design and develop a steganography program, to conceal data from people without access codes, so that only certain people can view the data.
- Evaluating the steganography program by how much information can be added before corrupting the image file.



Development Methods

- The development methodology that is going to be used for this project is the spiral model. The spiral model has four different phases and they are planning, risk analysis, engineering and evaluation phase.
- During the planning phase the requirements for the project are acquired.
 - In the risk analysis phase, the risk are identified and the alternative solution for the project.
 - the engineering phase is where the software is developed and tested.
 - the evaluation phase checks the output of the project before continuing to the next spiral.[5]

Bibliography

[1] “What is Spiral model- advantages, disadvantages and when to use it?” [Online]. Available: <http://istqbexamcertification.com/what-is-spiral-model-advantages-disadvantages-and-when-to-use-it/>. [Accessed: 04-Oct-2017]. [2] “hidden_data-01.png (5000×3750).” [Online]. Available: https://media.wired.com/photos/594db1736b76bb7625b89e48/master/pass/hidden_data-01.png. [Accessed: 03-Oct-2017]. [3] “Screen Shot 2016-08-26 at 9.53.34 AM.png (1200×499).” [Online]. Available: <https://www.endgame.com/sites/default/files/Screen Shot 2016-08-26 at 9.53.34 AM.png>. [Accessed: 03-Oct-2017]. [4] L. M. Marvel, C. G. Boncelet, and C. T. Retter, “Spread spectrum image steganography,” *IEEE Trans. Image Process.*, vol. 8, no. 8, pp. 1075–1083, 1999. [5] R. E. Vinodhini, P. Malathi, and T. G. Kumar, “A survey on DNA and image steganography,” in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017, pp. 1–7.