UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Faculty of Computer Science and Information Technology

Wavelet _based Image Steganography

By

Reham Abdullah Mohamed Ibrahim

A Thesis

Submitted to the College of Graduate Studies and Academic Advancements
in Partial Fulfillment of the Requirement for the Degree of Master of Science in
Computer Science

Supervisor

Dr.Talaat Wahby Hussien

September , 2016

Abstract

Information protecting one of the biggest challenges in computer science and Steganography one of the most common ways to maintain the confidentiality of data.Science of steganography one of the concealing information technologies in the medium without drawing attention to it.

This research is based on the concealment of confidential information in two layers, the first layer is a new way of algorithm developer least Significant bit(LSB) , It works to hide a message in a picture depending on the jumping technique to hide text in specific places.

Conducted in the first layer where the experiments used three different sizes of the texts were hidden in same sizes (350) photos account was fifth best results in terms of peak signal-to-noise ratio **(PSNR)** to be used in the layer and second where he was hiding in a new image with the same size and then was chosen the best result.

In the second layer the system hides the output of the first layer in the new image using an algorithm discrete wavelet transform (DWT).

Model has shown good result in terms of information security and image quality.

المستخلص

حماية المعلومات واحده من اكبر التحديات في علم الحاسوب الاخفاء واحده منناكثر الطرق شيوعا للمحافظه على سرية البيانات.علم الاخفاء واحده من تقنيات اخفاءالمعلومات في وسيط بدون لفت الانتباه لذلك.

يقوم هذا البحث على اخفاء المعلومات السريه في طبقتين الطبقه الاولى عباره عن طريقه جديده مطوره من خوارزمية البت الاقل اهميه (LSB) تعمل على اخفاء الرساله في صورة اعتمادا تقنية القفز لاخفاء النص في اماكن محدده.

اجريت في الطبقه الاولى عده تجارب حيث استخدمت ثلالث نصوص ذات ذات احجام مختلفه تم اخفاءها في خمس صور ذات احجام متساويه (350) وتم حساب افضل خمس نتائج من حيث
(PSNR peak signal-to-noise ratio) ليتم استخدامها في الطبقه الثانيه حيث تم إخفاءهم في صورة جديده ذات نفس الحجم ومن ثم تم اختيارافضل نتيجه .

وفي الطبقه الثانيه يقوم النظام باخفاء ناتج الطبقه الاولى في صورة جديده باستخدام خوارزمية
وقد اظهر النموذج نتائج جيده من حيث امن المعلومات ومن حيث جوده الصورة.(DWT) .

1.1 Introduction

In this chapter begin overview of steganography and background of the problem describe first , objective ,scope and methodology .

1.2 Overview

Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret.

Information hiding is one of the important areas of information security, which includes various methods like cryptography, steganography and watermarking.

Cryptography means sender convert plaintext to cipher text by using Encryption key and other side receiver decrypt cipher text to plain text by using The area of research emphasize on which technique is best suited as individual or together for data hiding.Digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible).

The proposed method of information security in the research is steganography .

Steganograph*y* comes from the Greek Steganos, which mean covered or secret and graphy means writing or drawing.Steganography can be classified into image ,text,audio and video steganography based on the cover media used to embed secret data .

The goal of steganography is to embed secret data into a cover in such a way that no one apart from the sender and intended recipients even realizes there is a secret data.

Steganography ,watermarking and encryption techniques are used to ensure data confidentiality however the main difference between them is :

Table (1.1): explain Comering between Steganography, Cryptography and Water Marking

	Steganography	Cryptography	Water Marking
Techniques	LSB, Spatial Domain, Jsteg, Outguess	Transposition, Substitution, RSA	compensated prediction, DCT
Naked eye Identification	No, as message is Hide within other carrier (cover image)	Yes, as message is convert in Other way, which sough something is hidden	Yes, as actual message is hiding by some watermark.
Capacity	Differs as different Technology usually low hiding capacity	Capacity is so high, but as message is long it chances to be decrypt	Capacity depends on the size of hidden data.

Detection	Not easy to detect because to find steganographic image is hard.	Not easy to detect ,depend on technology used to generate	Not easy to detect
Strength	Hide message without altering the message, it conceals information	Hide message by altering the message by assigning key	Extend information and become an attribute of the cover image
Imperceptibility	High	High	High
Applicability	Universally	Universally	Universally
Robust	Yes	Yes	Yes

Least Significant Bit (LSB) image stenography is one of the earliest techniques It was simplest and effective in the implantation of steganographic concepts.used to embed the secret data in to the least significant bits of the pixel values in a cover image is Least Significant Bit modification coding technique. LSB is basically follow insertion process in which last bit is simply replaced by the bit of secret message.

A discrete wavelet transform (DWT) is a sampled wavelet function. The Discrete Wavelet Transform (DWT), which is based on sub-band coding is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. Rather than calculate the wavelet coefficients at every point, the DWT uses only a subset of positions and scales. This method results in an perfect and more efficient manner of a wavelet transform.

Multi-Level Steganography is a new concept of information hiding in telecommunication networksthat uses features of an existing steganographic method (the upper-level method) to create a new one (the lower-level method).

Multi-Level Steganography (MLS) was originally proposed by Al-Najjar for image steganography. MLS is based on combining two or more steganography methods in such a way that one method (the upper-level) is a carrier for the other method (the lower-level) .

1.3 Problem Statement

Systems that use only one level of Steganography are usually more vulnerable, due to the fact that they lack the complexity to keep the data secure. This is why two levels of Steganography will be used in this system.

Furthermore the most commonly used Steganography algorithm which is the normal (LSB) algorithm is proved to be weak and the secret data is easy to retrieve. For this reason the proposed system uses a modified more secure version of LSB called the (RE_LSB).

We propose to build multi-level steganography system deal and fix most of the problem above.

The second Steganography level also employs another strong algorithm Discrete Wavelet Transform.

1.4 Objective of the Research

The main objective is developing a system that applies multilevel image Steganography to concealing secret data into image by applying two-levels of image steganography.

Additionally the proposed method has some sub-objectives:

1- Add more complexity to the Steganography process through applying it in two levels.

2- Enhancing the confidentiality of the secret information by using two level image steganography in one system.

3- to balance the capacity of embedded data (secret text) and the changed pixels value especially in level one.

4- Measure the performance of the proposed algorithm.

1.5 Research Questions

1- How to use two levels of image steganography with different techniques to hide the secret information?

2- How to extract the image (intermediate cover object) from image (cover object) and extract secret information (text) from image (intermediate cover object)?

3- How the proposed method helps in hiding the secret information (text) to protect it from unauthorized disclosure?

4- How to measure the performance of the proposed system?

1.6 Research Methodology and Tools

By applying deep study in one-level LSB image steganography techniques , We discovered the existence of vulnerabilities in LSB image steganography ,multi-level steganography can meet the vulnerabilities founded in LSB by adding another level of image steganography using Discrete Wavelet Transform based image steganography.

1.7 Research Scope

The scope of this research will be steganography technique especially multilevel steganography (MLS) focusing on Image steganography. The hiding of secret information (text) will be achieved by two levels of image steganography,level one uses modified least significant bit (RE_LSB) image steganography to hide the secret information into image. While level two employs DWT based image steganography to hide the image output from level one in another image.

The secret text massage used here is English language text, under MS Windows. The images used are RGB images (colored images). In “.PNG ,JPG and .JEPG” extensions. Figure 1 explains the scope of proposed method in details.

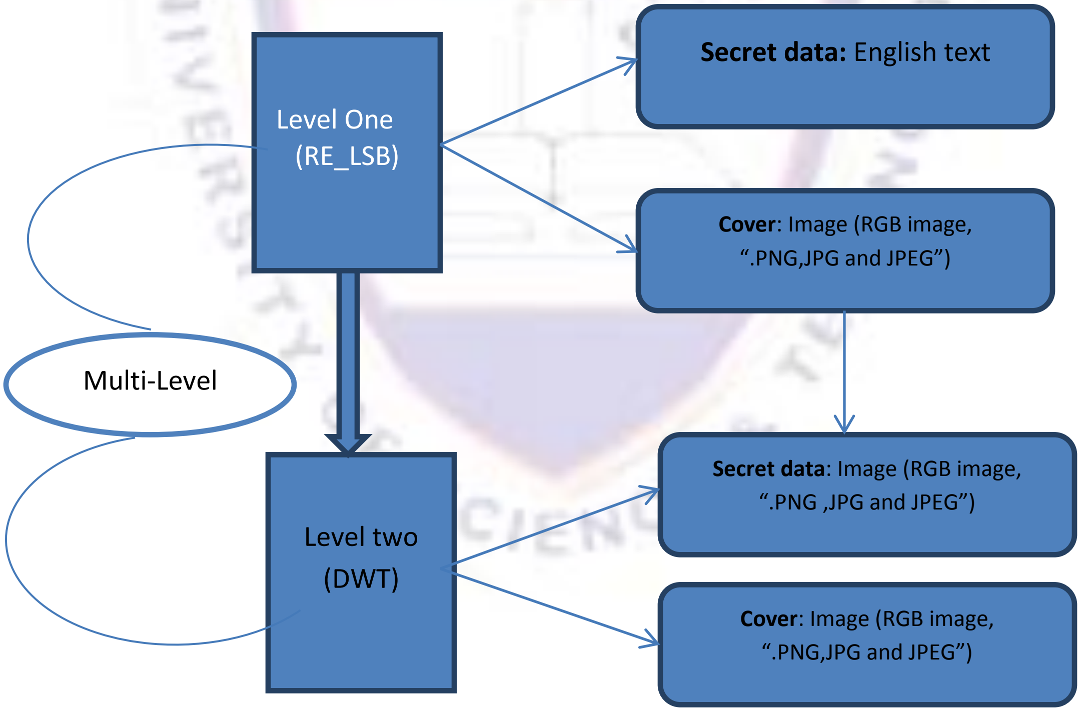

Figure (1.1) : explains the scope of proposed method

1.8 Research Organization

Chapter one gives introduction about the steganography, and multilevel steganography ,defining the types of steganography. Recently literatures review and related works will be explained in chapter two. Chapter three explains the proposed algorithm, tools and techniques used in the project. The analysis of the proposed algorithm and discussion of the results appears in chapter four and finally Chapter five presents the conclusion, recommendations and future work.