Republic of Iraq

Ministry of Higher Education and Scientific Research

Mustansriya University

College of Science/Department of Computer Sciences

HIDING SECRET MASSEGE IN IMAGE

A project submitted to the Department of Computer Sciences in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Sciences – Computer Sciences

BY

Wael Abbas Mahmoud

Mustafa Shehab Ahmed

SUPERVISED BY

L. Rawsam A. Hassan

Baghdad, Iraq
2023

Supervisor Certification

This is to certify that the project entitled

…… ,

prepared by …….

, and …….

,

submitted to the Department of Computer Sciences / Collage of Science at Mustansriya University in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Sciences – branch name was made under my supervision and guidance.

Signature:

Name: (Supervisor)

Title:

Date: / /

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

يوْمَ نطوي السَّمَاءَ كَطَيِ ال سِجِلِ للْكُتبِ ج كَمَا بدَأْنَا أَوَّلَ خَلْقٍ نعِيدُهُ ج

وَعْدًا عَلَيْنَا ج إِنَّا كُنَّا فاعِلين

صدق الله العلي العظيم

سورة الانبياء : الأية 104

Dedication

To all those who are enlightened by the knowledge of the mind of others, or guided by the answer The correct puzzlement of his patients, he showed with his permission humility scientists And his blessing is the mercy of those who know. Dedication I dedicate this humble work to my father, who did not spare me Days to something and to my mother who gave me affection and love I say to them: You have given me life and hope and come to me My passion for knowledge and knowledge, my brothers and my family and all of us To every one who taught me a character who has become a shining light illuminates the way Front.

الإهـداء

بعد سنين من المشوار الدراسي

ها قد وصلت الى نهاية المطاف سنين قضيتها بالتعب وسهر الليالي

وظروف الحياة الصعبة التي لم تستطيع الوقوف في طريقي

اهدي مشروع تخرجي وإلى من تتسابق الكلمات لتخرج معبرة عن

مكنون ذاتها من علمتني وعانت الصعاب لأصل إلى ما أنا فيه وعندما

تكسوني الهموم أسبح في بحر حنانها ليخفف من آلامي.. . أمي

وابي واخوتي واخواني واصدقائي

ثم إلى كل من علمني حرفاً أصبح سنا برقه يضيء الطريق أمامي

Acknowledgments

I would like to thank my fellow student at the bachelor level, and the supervisor of this research was a professor

and supervisor since the subject was title and idea until it became a message and research. He has all the thanks and appreciation and gratitude. I would like to thank all of my distinguished professors in the Department of Computer Science who have made every effort to guide me and provide me with the books I need from their libraries. I think I should be grateful to my Supervisor…

الشكر والتقدير

الحمد لله حمداً كثيراُ طيباً مُباركاً فيه ... اللهم لك الحمد حتى ترضى ولك الحمد إذا رضيت

ولك الحمد بعد الرضا

لا يســـع حـــروفـــي إلا أن تمـــتزج لتكـــون كـــلمـــات شكـــــر

وعـــــرفـــــان

ليس لأحد معين وإنما لكل من ساهم في تقديم المساعدة لي ولغيري

الى التدريسين في قسم علوم الحاسوب

والدكتور المشرف الذي لم يبخل بمساعدتي

إن قلت شكرا فشكري لن يوفيكم حقا

سعيتم فكان السعي مشكورا

جميل من الانسان أن يكون شمعة ينير درب الحائرين

ويأخذ بأيديهم ليقودهم إلى بر الأمان متجاوزا بهم أمواج الفشل والقصور فشكرا

لكم من الأعماق...

ومن الله التوفيق

Abstract:

Summary from the folds of our project that it is possible to encode the message with one of the encryption algorithms and steganography the text inside the colored image, First, we encrypted the text by the Playfair encryption algorithm, Then we analyzed the image to its three colors red, green and blue (RGB).The second stage, we embed the text message inside the blue band of the image.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RGB	Red,,Green,,Blue
LSB	least significant bit
ELSB	Enhanced least significant bit

Introduction

Chapter One

1.1- Introduction:

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.[1]

The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).[2]

The primary goal of hiding information is to avoid drawing attention to the transmission of hidden information. If suspicions arise, it is this goal that was planned to achieve the security of the secret message because if the hackers notice any change in the sent message, this observer will try to find out the information hidden inside the message.[2]

1.2 Project Objectives:

Below are the objectives for which the project was implemented:

1-Encrypting text and hide in image.

2-Analyzing the colored image into three colors

(Red,Green,Blue).

3-Hide the encrypted text in blue image to reduce the distortion of Image quality.

1.3 Steganography:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

1.4 The advantage of steganography over cryptography:

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal. In other words, steganography is more discreet than cryptography when we want to send a secret information. On the other hand, the hidden message is easier to extract. [4]

1.5 ENHANCED LEAST SIGNIFICANT BIT TECHNIQUE

LSB algorithm hide information in the least significant bit of each color i.e. RGB of the carrier image. The problem states from the fact that modifying the three colors of a pixel produces a major distortion in the resulting color. So the one method that would introduce more efficiency and less distortion is Enhanced Least Significant Bit. The proposed technque works in the spatial domain. It improves performance of LSB by hiding information in only one of the three colors that is blue color of the carrier image and it used three least significant bits in the cover to hide the message. [10]

Comparative Analysis of Least Significant Bit and Enhanced Least Significant Bit Encoding Technique

If a pixel of the cover image with the RGB (Red-Green-Blue code) color A8A8A8 # is used, binary 10101000-10101000-10101000 to hide the message 111, the result would be (10101001-10101001-10101001):

Results obtained hiding the message 111 in the pixel 10101000-10101000-10101000 with the LSB method

Table 1: Results with LSB method

	Hexadecimal	Decimal	Red	Green	Blue
Original pixel	A8A8A8	11053224	168	168	168
Modified pixel	A9A9A9	11119017	169	169	169

The three least significant bits of the pixel have changed, introducing a small distortion, but the difference between the old and new color represents a leap of 65793 colors in the scale of colors. Enhanced LSB method that would introduce more efficiency and less distortion would store the 3 bits of information to hide in the same color. Using the same example, the 3 bits of information will be introduced in the 3 LSB bits of blue color (10101000-10101111-10101111):

Results obtained hiding the message 111 in the pixel 10101000-10101000-10101000 with the ELSB method:

Table 2: Results with ELSB method

	Hexadecimal	Decimal	Red	Green	Blue
Original pixel	A8A8A8	11053224	168	168	168
Modified pixel	A9A9A9	11053231	168	168	175

In this case the leap in the scale of colors is 7.[4]

1.6 Types of Steganography Techniques

There are several types and forms of steganography, and in the sections below, we'll explore a few interesting and commonly used ones. Broadly steganography techniques could be classified into

Physical: One that does not involve the use of digital mediums or files. Examples of such techniques include

1. Passing messages written with invisible ink, which can then be read by the intended recipient by applying certain chemical techniques
2. By using ciphering techniques to hide information within textual information. Here is an example of a null cypher technique used by a prisoner to convey a secret message to his outfit, which was intercepted and decoded by the FBI. See graphic below, which looks like an ordinary letter, however, when one looks at every fifth word (highlighted in red) it reveals a plot to murder someone i.e, refer to the last few red words "IF GUILTY OF WRITEUP, HE SHOULD BE HIT."

Microdots involve shrinking messages to such tiny dimensions, they are made almost invisible. These also involve positioning ‘hard-to-see’ dots within a message to convey a specific message.

- Digital: Involves the usage of digital mediums such as hiding information within . [4]

1. Text files
2. Image or picture files
3. Audio files
4. Video files

1.7 **Cryptosystem**:

A cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext to encode or decode messages securely. The term “cryptosystem” is shorthand for “cryptographic system” and refers to a computer system that employs cryptography, a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. [5]

To help keep data secure, cryptosystems incorporate the algorithms for key generation, encryption and decryption techniques. At the heart of cryptographic operations is a cryptographic key, a string of bits used by a cryptographic algorithm to transform plain text into cipher text or the reverse. The key is part of the variable data provided as input to a cryptographic algorithm to execute this sort of operation. The cryptographic scheme’s security depends on the security of the keys used. [5]

.

Cryptosystems are used for sending messages in a secure manner over the internet, such as credit card information and other private data. In another application of cryptography, a system for secure electronic mail might include methods for digital signatures, cryptographic hash functions and key management techniques. [5]

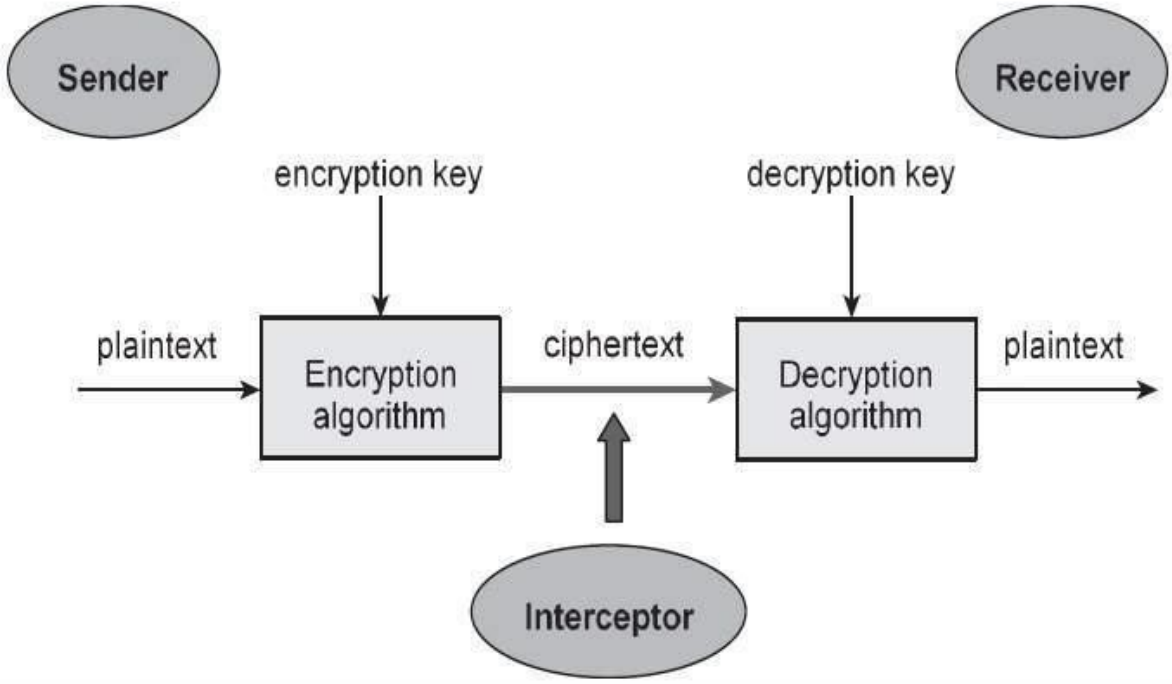


FIGURE (1.1) Encryption and decryption

The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data. The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext. [6]

Components of cryptosystems

A basic cryptosystem includes the following components:

- Plaintext- This is the data that needs to be protected.

Encryption algorithm- This is the mathematical algorithm that takes plaintext as the input and returns ciphertext. It also produces the unique encryption key for that text.

- Ciphertext- This is the encrypted, or unreadable, version of the plaintext.
- Decryption algorithm- This is the mathematical algorithm that takes ciphertext as the input and decodes it into plaintext. It also uses the unique decryption key for that text.
- Encryption key- This is the value known to the sender that is used to compute the ciphertext for the given plaintext.
- Decryption key- This is the value known to the receiver that is used to decode the given ciphertext into plaintext. [7]

Types of cryptosystems

Cryptosystems are categorized by the method they use to encrypt data, either symmetrically or asymmetrically.

1. symmetric key encryption is when the cryptosystem uses the same key for both encryption and decryption. In this method, keys are shared with both parties prior to transmission and are changed regularly to prevent any system attacks.
2. Asymmetric key encryption is when the cryptosystem uses different keys for encryption and decryption. However, the keys are mathematically related. In this method, each party has their own pair of keys that is exchanged during transmission. [7]

•

Cryptosystem attack examples

Modern cryptography has become highly complex, and because encryption is used to keep data secure, cryptographic systems are an attractive target for attackers. What is considered strong encryption today will likely not be sufficient a few years from now due to advances in CPU technologies and new attack techniques. [8]

Common types of cryptographic attacks include the following:

- Brute force attacks attempt every possible combination for a key or password. Increasing key length boosts the time to perform a brute force attack because the number of potential keys rises.
- In a replay attack, the malicious individual intercepts an encrypted message between two parties (such as a request for authentication) and later

"replays" the captured message to open a new session. Incorporating a time stamp and expiration period into each message can help eliminate this type of attack.

- In a man-in-the-middle (MitM) attack, a malicious individual sits between two communicating parties and intercepts communications (including the setup of the cryptographic session). The attacker responds to the originator's initialization requests, sets up a secure session with the originator and then establishes a second secure session with the intended recipient using a different key and posing as the originator. The attacker has access to all traffic passing between the two parties.

- An implementation attack takes advantage of vulnerabilities in the implementation of a cryptosystem to exploit the software code, not just errors and flaws but the logic implementation to work the encryption system.

A statistical attack exploits statistical weaknesses in a cryptosystem, such as floating-point errors. Another weakness that might lead to a statistical attack is the inability to produce truly random numbers. (Because software-based random number generators have a limited capacity, attackers could potentially predict encryption keys). Statistical attacks are aimed at finding vulnerabilities in the hardware or operating system hosting the cryptography application.

- A cipher text-only attack is one of the most difficult types of cyberattack to perpetrate because the attacker has very little information to begin with. For example, the attacker might start with some unintelligible data that he or she suspects may be an important encrypted message but then gather several pieces of ciphertext that can help him or her find trends or statistical data that would aid in an attack.
- In a known plaintext attack, an attacker who has a copy of both the encrypted message and the plaintext message used to generate the ciphertext may be able to break weaker codes. This type of attack is aimed at finding the link – the cryptographic key that was used to encrypt the message. Once the key is found, the attacker can then decrypt all messages that encrypted using that key. [8]

1.7.1 The Playfair algorithm :

The **Playfair** He created the blade at the beginning of the 20th century, and was killed in the Boer War. Branding which means encoding pairs vs.[9]

•

encoding singly. The characters contained within the 25-character limit; So we have the 25 factorial! number of keys equal to

Before performing the encryption process, Code Playfair replay the message a bit. To implement this

1- Replace each letter I with the letter J.
2- Write the message in pairs of letters.
3- Do not allow identical pairs of letters, and if they exist, insert the letter Z between them.
4- Add a Z at the end, if the number of characters is odd.
5- To show how the Playfair code works, we will choose a specific key that does not distinguish our choice[9]

encryption base

To return the message appropriately, we display the base in the code playfair system. original source. The sixth row matches the first row, and the sixth column matches the first column; Can expand in key design

A rule in the Playfair codebase is as follows:

Title, key, the letter to the right of it in the key.

If a letter falls in the same column in the key box, each letter replaces the letter that lies below it in the extended key box.

If the letter does not fall into the first column, which falls into the first letter, it falls into the first letter. The second letter is replaced by the letter in the fourth corner of the rectangle, which was formed from the three letters erased so far.

We now encode the following message: Good BROOMS SWEEP CLEAN.[9]

You only need to type the message in the pairs of characters that appear in the lower case letters that you want to type as needed. Accordingly, we obtain the following:

NZ EA CL EP EZ SW SZ OM OZ BR OD GO

And so, for the number we modeled; GO becomes FP, OD becomes UT, and OM becomes PO. The full ciphertext becomes:

DY CS BG CM CM BV TV DV PO UW EC UT FP

An example is the case with replacement blades, which refer to the owner to wholesale restoration. The method used to decipher the playfair cipher was to include this in the previous phrase, get rid of the repeated characters, and then put the characters not in alphabetical order. UNIVERSTYOFLD When discarding characters, sometimes the order of the characters in the key box.[9]

1.7.2 Encryption:

In cryptography, **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.https://en.wikipedia.org/wiki/Encryption - cite_note-:0-1 Only

authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing. Modern encryption schemes utilize the concepts of public-key and symmetric-key. Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption. [9]

1.7.3 Programming Section:

Transferring highly confidential information to a secure location without unauthorized access to that information presents many dangers. Over the centuries, people have made repeated attempts to develop particularly hardto-decipher **secret languages**. From ancient Rome to the Second World War to the present day, orders were sent in encrypted form by statesmen and important commanders to deceive the enemy or keep the information out of the hands of unauthorized persons.

Unfortunately, these forms of encryption were usually very easy to crack. For instance, one could easily decipher secret languages, which have arisen from the displacement of letters (e.g., today is a beautiful day = heute ist ein schöner Tag = heu teis teinsch önert ag). The weak point of all sophisticated secret languages is that once the key has been found, any text can be "translated". At least with the use of computers, it has become **impossible** to keep secret a key attributed to the shifting of letters. [9]

Today, other encryption methods have to be used to avoid sharing confidential information with everyone. In this case, too, again a key is used, which only the sending and the receiving side know. For encryption and decryption, so-called encryption algorithms are used. An encryption algorithm is a mathematical method, according to which the conversion of the data takes place.

Password Depot uses the encryption algorithm **playfair** to encrypt your confidential data. [9]

CHAPTER TWO
Technologies

2.1 Introduction:

Digital image processing includes taking the digital image and utilizing computer imaging software to process them . Digital image processing mentions to the technology of implementing a number of computer algorithms to process digital images. The outcomes of this process either image or properties or representation characteristics of the original image. The basic purpose of digital image processing is to permit human beings to acquire an image of high quality or descriptive characteristics of the original image There are different applications of digital image processing that can be found in medical imaging, remote sensing, forensics, communications and etc [10].

Image de-noising is a vital image processing task i.e. as a process itself as well as a component in other processes. There are many ways to de-noise an image or a set of data and methods exists. The important property of a good image de-noising model is that it should completely remove noise as far as possible as well as preserve edges. Traditionally, there are two types of models i.e. linear model and non-liner model. Generally, linear models are

used. The benefits of linear noise removing models is the speed and the limitations of the linear models is, the models are not able to preserve edges of the images in efficient manner I.e. the edges, which are recognized as discontinuities in the image, are smeared out. [10].

2.2 Images Types

There are different types of image data depending on many things such as the bit resolution, image content, and the actual image data type that is required for storage. The different existing image data types listed below:

2.2.1 Grayscale Image

Each pixel is a shade of grey, normally from 0 (black(to 255 (white(Each pixel can be represented by eight bits, or exactly one byte. This is a very natural range for image file handling. Other grey scale ranges are used, but generally they are a power of 2 [10]

Figure bellow describe this type of image:

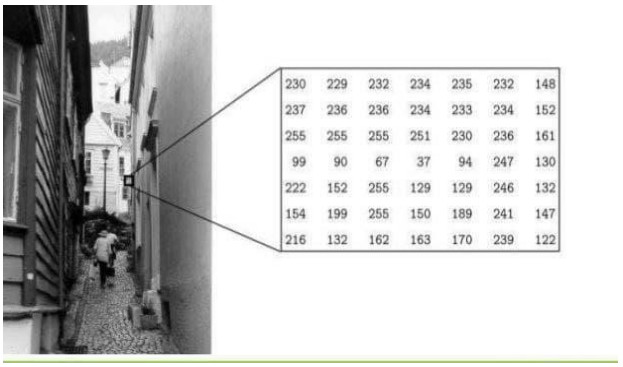


Figure (2.1)grayscale image

2.2.2 TrueColor RGB Image

Each pixel has a particula colour described by the amount of red, green and blue in it. If each of these components has a range 0-255, this gives a total of different possible colors in the image this is enough colors for any image.since the total number of bits required for each pixel is 24,such images are also called 24-bit color images.[10]

Figure bellow describe this type of image:

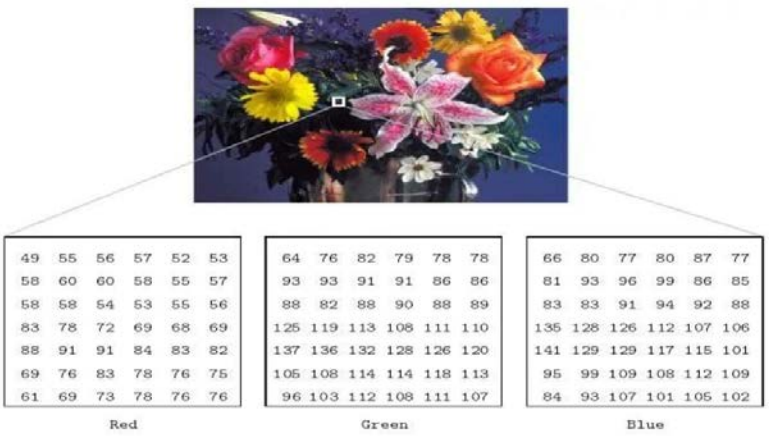


Figure (2.2) true color RGB image

2.2.3 Binary Image

Each pixel is just black or white. Since there are only two possible values for each pixel, we only need one bit per pixel. Such images can therefore be very efficient in terms of storage [11].

Figure bellow describe this type of image:

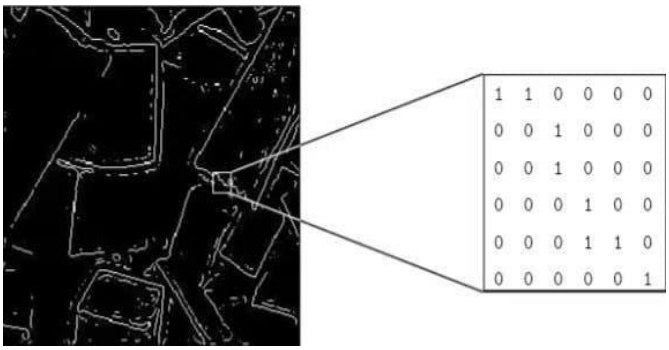


Figure (2.3) binary image

2.2.4 Indexed image

The image has an associated colour map, or color palette, which is a list of all the colours used in that image. Each pixel has a value in this index. It is convenient if an image has 256 colors or less.[11]

Figure bellow describe this type of image:

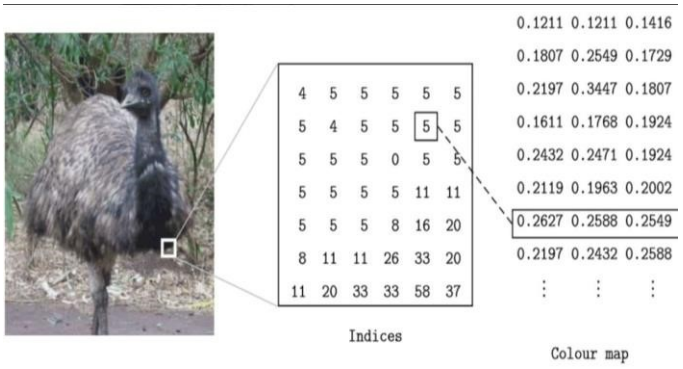


Figure (2.4) index image.

2.3 Image file formats :

it are standardized means of organizing and storing digital images. Image files are composed of digital data in one of these formats that can be rasterized for use on a computer display or printer. An image file format may store data in uncompressed, compressed, or vector formats. Once rasterized, an image becomes a grid of pixels, each of which has a number

of bits to designate its color equal to the color depth of the device displaying it .

2.3.1 JPEG 2000

JPEG 2000 is a compression standard enabling both lossless and lossy storage. The compression methods used are different from the ones in standard JFIF/JPEG; they improve quality and compression ratios, but also require more computational power to process. JPEG 2000 also adds features that are missing in JPEG. It is not nearly as common as JPEG, but it is used currently in professional movie editing and distribution (some digital cinemas, for example, use JPEG 2000 for individual movie frames). [12].

2.3.2 Exif (Exchangeable image file format(:

The Exif format is a file standard similar to the JFIF format with TIFF extensions; it is incorporated in the JPEG-writing software used in most cameras. Its purpose is to record and to standardize the exchange of images with image metadata between digital cameras and editing and viewing software. The metadata are recorded for individual images and include such things as camera settings, time and date, shutter speed, exposure, image size, compression, name of camera, color information. When images are viewed or edited by image editing software, all of this image information can be displayed . The actual Exif metadata as such may be carried within different host formats, e.g. TIFF, JFIF (JPEG) or PNG. IFF-META is another example. [12].

2.3.3 TIFF (Tagged Image File Format (:

The TIFF format is a flexible format that normally saves eight bits or sixteen bits per color (red, green, blue) for 24-bit and 48-bit totals, respectively, usually using either the TIFF or TIF filename extension. The tagged structure was designed to be easily extendible, and many vendors have introduced proprietary special-purpose tags – with the result that no one reader handles every flavor of TIFF file. [12].

2.3.4 GIF (Graphics Interchange Format(:

GIF is in normal use limited to an 8-bit palette, or 256 colors (while 24-bit color depth is technically possible).[1][2] GIF is most suitable for storing graphics with few colors, such as simple diagrams, shapes, logos, and cartoon style images, as it uses LZW lossless compression, which is more effective when large areas have a single color, and less effective for photographic or dithered images. Due to GIF's simplicity and age, it achieved almost universal software support.

2.3.5 BMP file format :

The BMP file format (Windows bitmap) handles graphic files within the Microsoft Windows OS. Typically, BMP files are uncompressed, and therefore large and lossless; their advantage is their simple structure and wide acceptance in Windows programs. [12].

2.4 Language Programming Used:

2.4.1 Visual C#

Visual C# is a programming language developed by Microsoft that is used to create desktop, web, and mobile applications for the Windows operating system. It

is part of the .NET framework and is an object-oriented language that uses syntax similar to Java.[13]

Visual C# is a popular language for creating Windows applications because it provides a wide range of features such as a rich set of libraries, built-in memory management, and support for multi-threading. It is also easy to learn for developers who are familiar with other C-style languages. Visual Studio is the primary integrated development environment (IDE) used to develop and debug C# applications. Visual C# supports the development of a variety of applications including Windows Forms, WPF, ASP.NET, and Xamarin.[13]

Visual C# is designed to be a modern language that can take advantage of the latest advancements in computer hardware and software. It supports a variety of programming paradigms including imperative, declarative, functional, and object-oriented programming. In addition to its core language features, Visual C# also provides a number of advanced features such as LINQ (Language Integrated Query), async/await, and dynamic typing. These features make it easier to write code that is more concise, expressive, and efficient.[13]

One of the main advantages of Visual C# is its integration with the .NET framework. This allows developers to access a wide range of libraries and tools that can help them build robust and scalable applications. The .NET framework also provides a common runtime environment that allows C# applications to run on multiple platforms, including Windows, macOS, and Linux.[13]

Overall, Visual C# is a powerful and versatile language that is well-suited for a wide range of applications, from simple desktop utilities to complex enterprise software systems. Its rich set of features and tight integration with the .NET framework make it a popular choice among developers who are looking for a modern, efficient, and scalable programming language.[13]

CHAPTER THREE

Requirements Analysis and project Design

3.1 – project Design:

Form -1- The first interface before execution, which contains text encryption and decryption, as well as image analysis:

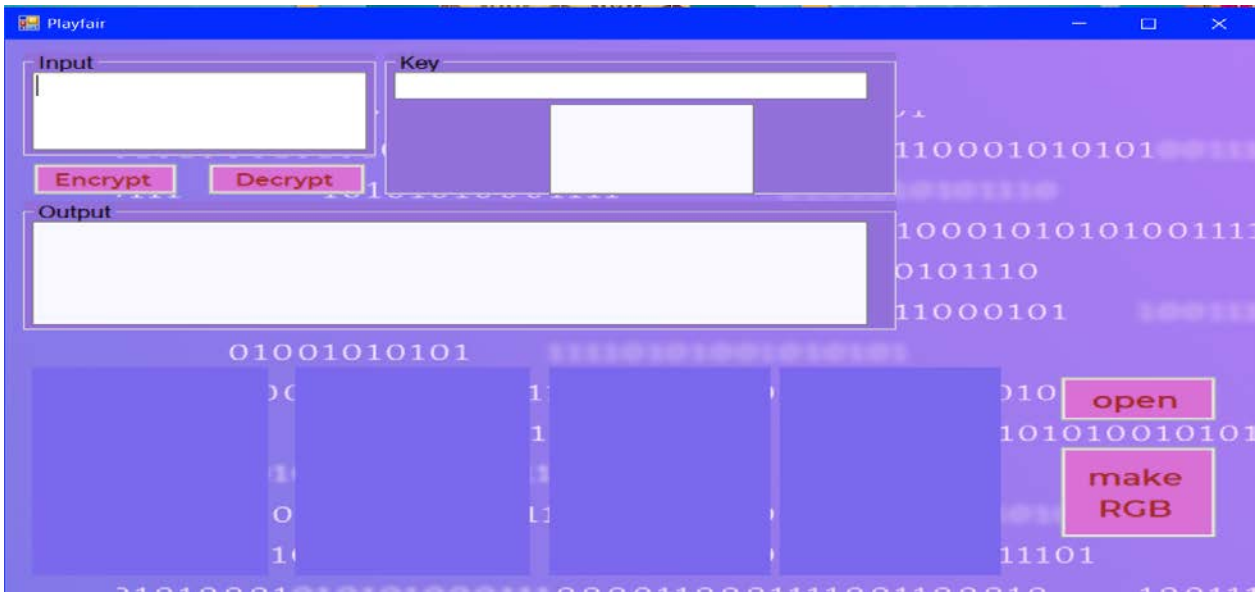


Figure (3.1) The first interface

Form2 : Here we entered the image for analysis:

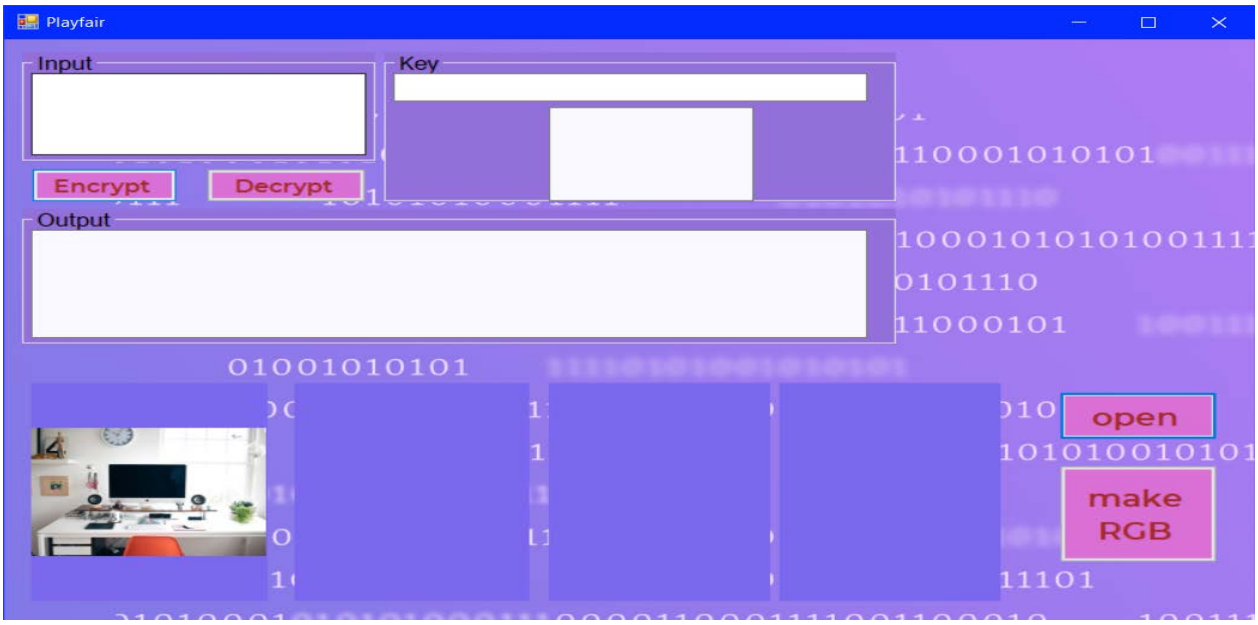


Figure (3.2) Insert the image

1- Form -3- The image was analyzed into three colors(RGB):

Figure (3.3) Image analysis

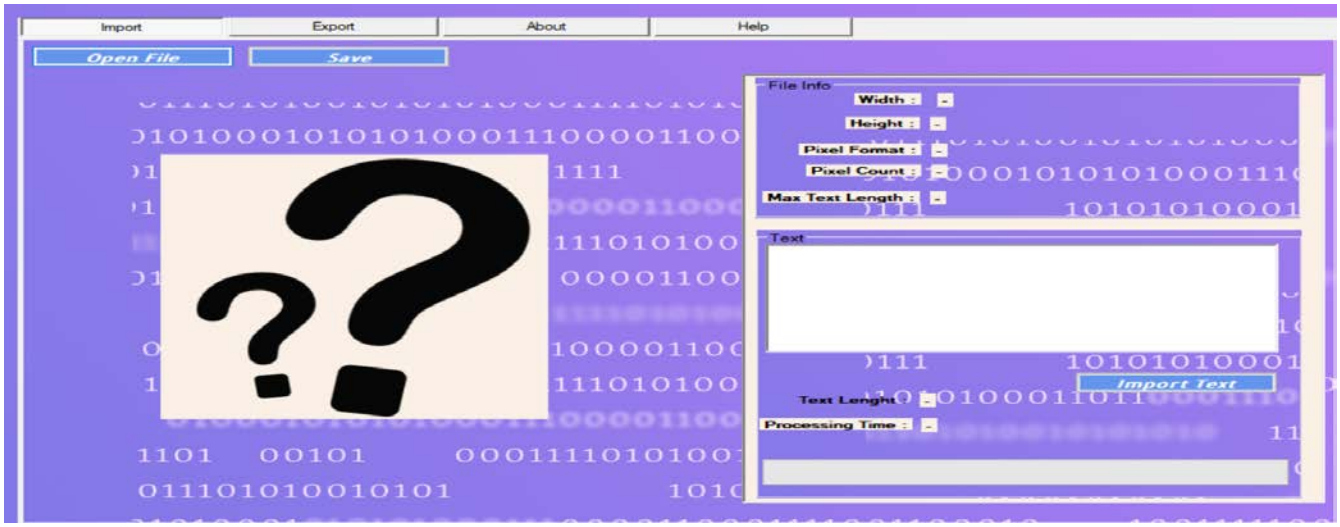
2- Form4: Enter the word to be encrypted and enter the key:

Figure (3.4) Enter text and key

4-Form5: The text was encrypted and the letters appeared untidy:

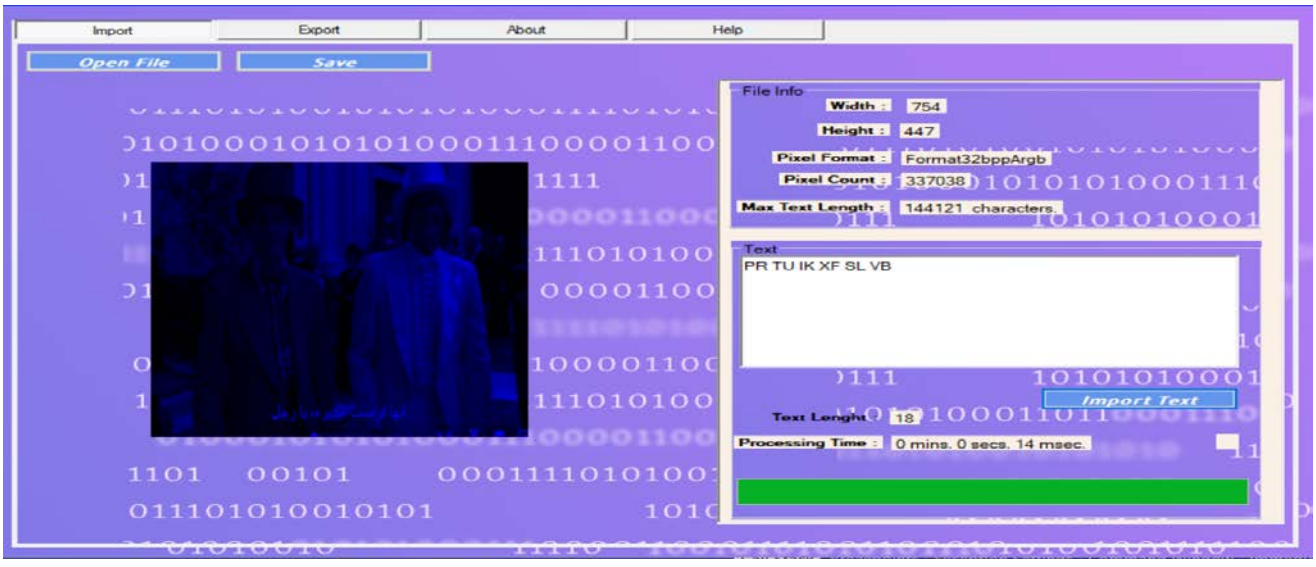
Figure(3.5) ciphertext

5-Form6: The second interface, which contains a way to hide the image:

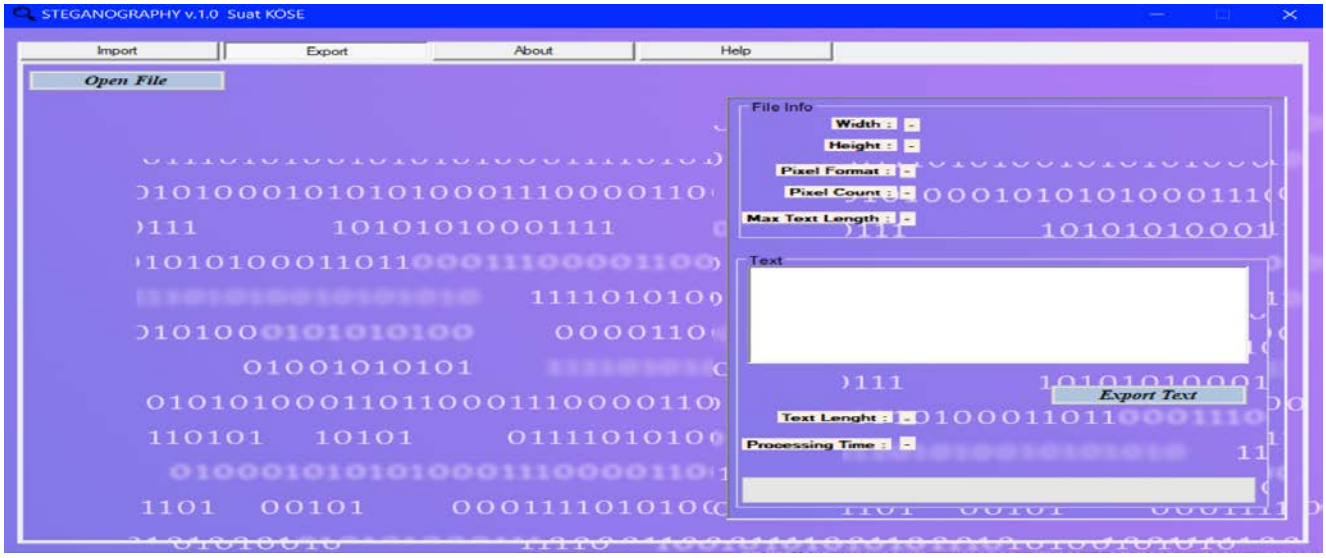


Figure(3.6) Steganography

6-Form7: We inserted the image into the hide button and brought the ciphertext to hide it inside the blue image:



Figure(3.7) Hide the text inside the image



7-Form8: The text has been hidden:

Figure(3.8) Steganography

8-Form9: And here we came with the image in which the text was hidden inside, and we opened the concealment by way of the Unhide button:

Figure(3.9)Export Text

Chapter

Four

4.2 Conclusions :

- We conclude that it is possible to hide important data within other files such as image, video, sounds and other files that are complex in their component arrays and thus obtain high results from concealment of data.

4.2 Future Work :

- We recommend that the system be developed further to include all types of text and files, as well as the use of the artificial intelligence algorithm to be highly secure.

Reference:

1- Zhang, Y., L. Wu, and S. Wang, “Magnetic resonance image classification by an improved LSB algorithm,” Progress In Electromagnetics Research, Vol. 116, 65–79, 2015.

2- Mohsin, S. A., N. M. Sheikh, and U. Saeed, “Steography : Effect of the air-tissue interface,” Progress In Electromagnetics Research, Vol. 83, 81–91, 2008.

3- Golestanirad, L., A. P. Izquierdo, S. J. Graham, J. R. Mosig, and C. Pollo, “Effect of realistic modeling of deep Image stimulation on the prediction of volume of activated tissue,” Progress In Electromagnetics Research, Vol. 126, 1–16, 2012.

4- Barker, Elaine; Barker, William; Burr, William; Polk, William; Smid, Miles (July 2012). "Recommendation for Key Management" (PDF). NIST Special Publication 800-57. NIST. Retrieved 19 August 2013. 5- Von Neumann, John (1951). "Various techniques used in connection with random digits" (PDF). National Bureau of Standards Applied Mathematics Series. **12**: 36–38. Press et al. (2007), chap.7

6- "Option Explicit and Option Strict in C Sharp .NET and in Visual ". Support. Microsoft. 19 March 2010. Retrieved 22 August 2013.

7- "Main Procedure in Visual Basic". MSDN – Developer Center.

Retrieved 20 January 2010.

8- "Visual Basic Version of Hello, World". MSDN – Developer Center. Retrieved 20 January 2010.

9- "Microsoft Visual Basic 6.0 Migration Resource Center". MSDN. Microsoft. Retrieved 9 November 2014.

10- https://msdn.microsoft.com/en-us/library/aa903378(v=vs.71).aspx

11- Krill, Paul (2009-02-27). "Microsoft converging programming languages | Developer World". InfoWorld. Retrieved 2013-08-18.

12- Mackenzie, Duncan (2016). "Navigate The .NET Framework And Your Projects With The My Namespace". MSDN Magazine Visual Studio 2005 Guided Tour 2006. Microsoft.

13- Whitney, Tyler (November 2005). "My.Internals: Examining the Visual Basic My Feature". MSDN. Microsoft.

14- Sherriff, Lucy (22 February 2005). "Real Software slams MS IsNot patent application". The Register. Retrieved 6 April 2009.

الملخص:

ملخص من ثنايا مشروعنا أنه من الممكن تشفير الرسالة بإحدى خوارزميات التشفير وإخفاء النص داخل الصورة الملونه ، قمنا بتشفير النص بواسطة خوارزمية تشفير Playfair، ثم قمنا بتحويل الصورة إلى ثلاثة ألوان الأحمر والأخضر والأزرق (RGB)وإخفائها النص داخل الصورة الزرقاء في البتات الثلاثه الاخيرة.

إقرار المشر ف

اوكد بأن هذا المشروع الموسوم:

الذي تم اعداده من قبل الطالبين:

والمقدم الى قسم علوم الحاسوب - كلية العلوم – الجامعة المستنصرية كجزء من متطلبات نيل شهادة البكالوريوس في علوم الحاسوب – تخصص قد تم تحت أشرافي وتوجيهاتي .

التوقيع:

الاسم: (المشرف)

المرتبة العلمية:

التاريخ:

جمهورية العرا ق

وزارة التعليم العالي والبحث العلمي

الجامعة المستنصرية

كلية العلوم – قسم علوم الحاسوب

HIDING SECRET MASSEGE IN IMAGE

مشروع تخرج مقدم الى كلية العلوم / قسم علوم الحاسوب كجزء من متطلبات نيل شهادة البكالوريوس في علوم الحاسوب – علوم الحاسوب

من قبل

وائل عباس محمود

مصطفى شهاب احمد

بأشرا ف

م.روسم عبد العظيم حسن

بغداد، العراق

2022م