ISSN: 2366-1313

CRYPTER TOOL - A PYTHON GUI TOOL FOR STEGANOGRAPHY

[1]Dr.Ch. V. Phani Krishna, [2]Balasani Dinesh, [3]Vemula Vamshi, [4]Yeldandi Venkat, [5]Veerla Sai Harshith

[1]Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad, balasanidinesh7@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad, vamshivemula444@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad, venkatyeldandi2000@gmail.com

[5]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad, Harshithveerla@gmail.com

Abstract: *Organizations have desired to keep certain sensitive communications and information secret for years. In our new age of digital media and internet communications, this need often seems even more pressing. Today's information age where technology has made information sharing and transfer increase exponentially and also makes the information vulnerable to unauthorized access, use, modification, and interception both while in storage or in transmission. It is no surprise that countless encryption methods of protecting such information like cryptography, watermarking and many more have evolved. One lesser-known but rapidly growing encryption method is Steganography. Though steganography is an ancient craft, the onset of computer technology has given it new life. Computer-based steganographic techniques introduce changes to digital covers such as Image, Audio, and Video. Our Project is a Python GUI application designed for implementing Steganography with AES Encryption. Steganography refers to hiding information inside an image file. In our project, we take the user's secret information as plain text and we convert it into Cipher text using AES Encryption. After that, we embed the Cipher text into the user's chosen cover-image file using the Steganography LSB (Least Significant Bit) Algorithm. After this process, a new image file (Stego Image) will be generated which has cipher text hidden inside image byte values.*

Keywords: *Cryptography, Steganography, Least Significant Bit Algorithm, Python GUI.*

ISSN: 2366-1313

I. INTRODUCTION

The word (Steganography\ ) comes from the Greek word "Steganos", which means covered or secret and –"graphy" which means writing or drawing. Therefore, steganography means, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected. Secret information is encoded in a way such that the very existence of the information is concealed in a human perceptible. Steganography is an ancient technology that has applications even in today's modern society. Steganography has taken many forms since its origin in ancient Greece. The first recorded use of the term can be traced back to 440 BC. During the war between Sparta and Xerxes. Dermeratus wanted to warn Sparta of Xerxes' pending invasion. To do this, he scraped the wax off one of the wooden tablets they used to send messages and carved a message on the underlying wood. Covering it with wax again, the tablet appeared to be unused and thereby slipped past the sentries' inspection. Herodotus, who documented the conflict between Persia and Greece in the fifth century B.C., felt that the art of secret writing saved Greece from Xerxes, the tyrant king of Persia. However, this would not be the last time steganography would be used in times of war. In World War II, the Germans utilized this technology. Unlike the Greeks, these messages were not physically hidden; rather they used a method termed "null ciphering." Null ciphering is a process of encoding a message in plain sight. For example, the second letter of each word in an innocent message could be extracted to reveal a hidden message. A message sent by a German spy during World War II read: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hit hard. Blockade issue affects for pretext embargo on by-products, ejecting suits and vegetable oils" . By taking the second letter of every word, the hidden message "Pershing sails for NY June 1" can be retrieved. Also during the American Revolution, invisible ink which would glow over a flame was used by both the British and Americans to communicate secretly.

By taking the second letter of every word, the hidden message **"Pershing sails for NY June 1"** can be retrieved. Also, during the American Revolution, invisible ink which would glow over a flame was used by both the British and Americans to communicate secretly.

More recent cases of steganography include using special inks to write hidden messages on bank notes and also the entertainment industry using digital

ISSN: 2366-1313

watermarking and fingerprinting of audio and video for copyright protection. Two other technologies that are closely related to steganography and cryptography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property; thus, the algorithms have different requirements than steganography and cryptography. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of hidden data. Therefore, in existing communication methods, steganography can be used to carry out hidden exchanges. The idea of steganography is to keep others from thinking that the information even exists and not to keep others from knowing the hidden information. If a steganography method causes anybody to suspect there is secret information in a carrier medium, then the method has failed.

RECOVERING INFORMATION FILE FROM A STEGO-OBJECT

Recovering a message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. In general, the information-hiding process extracts redundant bits from the cover-object. The process consists of two steps: i. Identification of redundant (least significant) bits in a cover object. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover object. ii. Embedding process. It selects the subset of the redundant bits to be replaced with data from the information file. The stego-object is created by replacing the selected redundant bits with information file bits. Basically, the model for steganography is shown in Figure 1. The cover- the object is a carrier or medium to embed the information file.

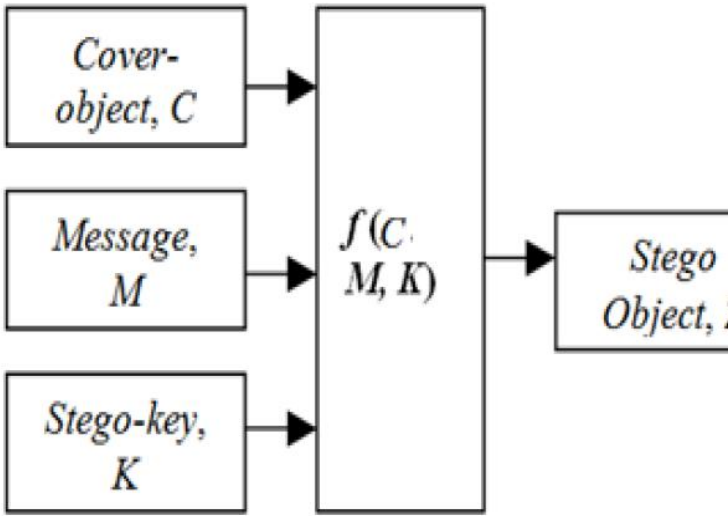

Fig.1 Basic Model of Steganography

ENCRYPTION WITH STEGANOGRAPHY

Most of the steganography tools online don't have encryption with it. Whoever has a stego image and steganography tool can access the hidden information, even

ISSN: 2366-1313

though the steganography algorithm is very specific, it is possible that the attacker might be able to get data from stego images using any steganography tools. In this research, we came up with Encryption with Steganography. We have used AES encryption for steganography. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is much stronger than DES and triple DES despite being harder to implement. In our project, we take user secret information as plain text and convert it into cipher text using AES Encryption and this will generate a "Key" that can be used for decryption. Then, we embed this cipher text into the cover image using the Steganography LSB (Least Significant Bit) Algorithm. After this entire process, a new image file will be generated called "stego image" and the Decryption Key is given to the user.

II. LITERATURE SURVEY

The growing possibilities of modern communications require the use of secure means of protecting information. The most common method of protecting information is cryptography whereby the information is scrambled into an unintelligible stream that cannot be decrypted by the casual viewer. Steganography is an approach to information hiding whereby the information is hidden inconspicuously inside a host data set such that its presence is imperceptible. Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography must not be confused with cryptography. Cryptography hides the contents of the secret information from malicious people, whereas steganography conceals the very existence of the information. Therefore, the methods used in breaking the system are different. In cryptography, the system is broken when the attacker can decrypt the unreadable data to form back the secret information. But to extract hidden information that is embedded using steganography, the attacker, first of all, needs to realize the very existence of the secret information. Without this knowledge, the secret data can pass through even right under his or her nose. Also in cryptography, the structure of information is scrambled to make it meaningless and unintelligible unless the decryption key or algorithm is available. It makes no attempt to disguise or hide the encoded information. Basically, cryptography offers the ability of storing and transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the

ISSN: 2366-1313

identity of someone or something. In contrast, steganography does not alter the structure of the secret information, but instead hides it inside a cover-image so that it cannot be seen or known. A message in a cipher text (encrypted message), for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other words, steganography prevents an unintended recipient from suspecting that a secret message exists. In addition, the security of the classical steganography system relies on the secrecy of the data encoding system.

Once the encoding system is known, the steganography system is defeated. It is possible to combine the techniques by encrypting messages using cryptography and then hiding the encrypted message using steganography. The resulting stego-image (encrypted image) can be transmitted or stored without revealing that secret information is being exchanged or preserved. Furthermore, even if an attacker were to defeat the steganographic technique and suspect the message from the stego-object (encrypted image), he would still require the steganographic decoding algorithm (steganographic system) to decipher the encrypted message [9]. Common techniques used in steganography are least significant bit insertion (LSB), masking and filtering, and transformation techniques.

III. SYSTEM DESIGN TRADEOFF PARAMETERS

Designing any steganographic system must take into consideration the following parameters: i. Capacity: The amount of data that can be hidden without significant change to the cover ii. Robustness: the resistance to possible modification or destruction of unseen data. iii. Invisibility: The hiding process should be performed in a way that does not raise any suspicion. Increasing the capacity of any cover to store more data than a practical possible threshold, then its transparency or robustness will be affected and vice versa. Similarly, invisibility and robustness are related; if any of these two parameters are influenced; it can affect the performance of the other one.

SYSTEM ARCHITECTURE

The data-hiding PROCESS using the steganographic technique in this project can be explained using this simple block diagram (Architecture). The graphical block representation of this system is shown in **figure.2**

ISSN: 2366-1313

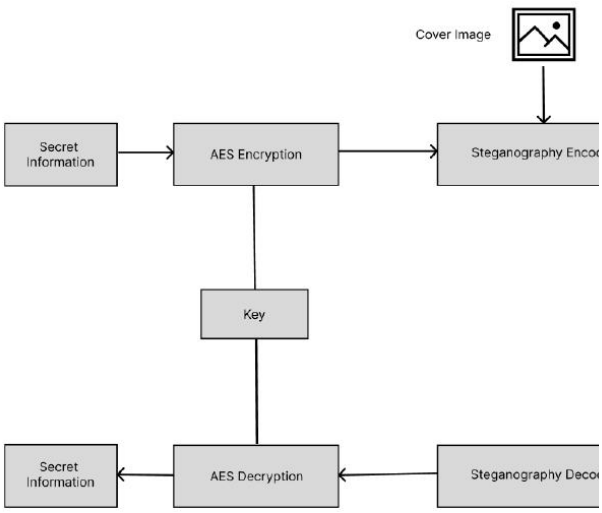

Fig.2 Proposed architecture

Architecture Components:

1. AES Encryption/ Decryption: The user's secret information is taken as plain text and is converted into cipher text using AES Encryption during decoding. We require AES Decryption for converting back cipher text into plain text.

2. Steganography Encoder/ Decoder: Steganography Encoder is used for hiding information inside the cover image and a Steganography decoder is used for retrieving information from the stego image.

3. Cover Image: Cover Image is the image in which the data has to be hidden.

4. Stego Image: Stego Image is an output image generated from the encoding section.

SYSTEM DESIGN MODULE PHASES

The systems module designs at different phases are

- Steg Hide module phase
- Steg UnHide module phase

Steg Hide Module

The Steg Hide phase of the system is the primary stage. In this phase, the user selects the image file, which acts as a carrier or cover image as well as an information file that will be hidden in the carrier image. In this module, the project will be having AES Encryption and Steganography Encoder. The information is converted into cipher text using Encryption. The cipher text is embedded into the cover image using LSB (Least Significant Bit) Algorithm. In the encryption module, the information file will be embedded into the cover or carrier image file. The embedding will be done based on the principle of the "Least Significant Bit" (LSB) algorithm.

The LSB algorithm uses the least significant bits of each pixel and replaces them with the significant bits of the information, such that the information will be encrypted into the carrier image. This process makes the picture not lose its resolution

Steg UnHide Module

In the Steg UnHide module of the system, the user selects the stego-image from a location. The user then sends the stego-

ISSN: 2366-1313

image to the decryption phase. In the decryption phase, the same "Least Significant Algorithm" is implemented but in the reverse way. Here the least significant bits from the stego-image are extracted and combined in an order to structure the original information bits. After successful arrangement, the information is decrypted from the carrier file and accessed as an original information file. The information file extraction from the carrier image.

IV. IMPLEMENTATION

The system design translates to programming codes using Microsoft Visual studio code and Python 3 programming language. Microsoft visual studio code comes with an inbuilt code analyser, this automated testing of programming code for the purpose of debugging an application before it is distributed or sold. Code analysis consists of statements created with a text editor or visual programming tool and then saved in a file. The code is the most permanent form of a program, even though the program may later be modified, improved or upgraded. The code analysis can be either static or dynamic. i. In static analysis, debugging is done by examining the code without actually executing the program. This can reveal errors at an early stage in program development, often eliminating the need for multiple revisions later. ii. Dynamic analysis is performed in an effort to uncover more subtle defects or vulnerabilities. Dynamic analysis consists of real-time program testing. A major advantage of these methods of code analysis is the fact that it does not require developers to make educated guesses at situations likely to produce errors. Other advantages include eliminating unnecessary program components and ensuring that the program under test is compatible with other programs likely to be run concurrently.

The Implementation steps for our proposed system are as follows:

Step 1: Importing all the required Python libraries.

Step 2: Make two functions for AES Encryption and Decryption.

Step 3: Define another two functions for Steg Hide and Steg UnHide

Step 4: Define Least Significant Bit (LSB) Algorithm used for Steganography Encoder.

Step 5: An image will be taken as input from user, inside which we want to hide the secret data. We will call this image as "cover image".

Step 6: Plain text data will be taken as input from user.

ISSN: 2366-1313

Step 7: The plain text will be converted into an encrypted text using a key.

Step 8: The encrypted text will be converted into raw binary data using ASCII table.

Step 9: Each bit of this binary data will be embedded in the Least Significant Bit(LSB) of RGB values of each pixel in the cover image.

Step 10: The changes in color value are so small that a normal human eye won't be able to detect these changes.

Step 11: This modified image will contain the secret data, which can only be read if someone has the right Key

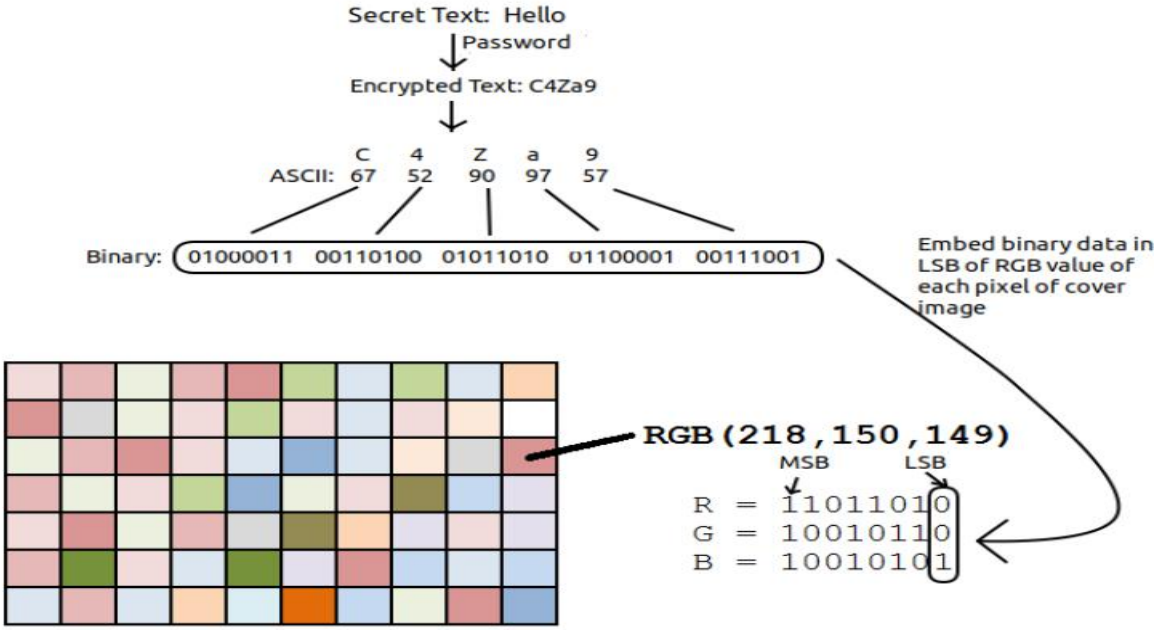

Fig.3 **LSB Working**

V. RESULTS

ISSN: 2366-1313

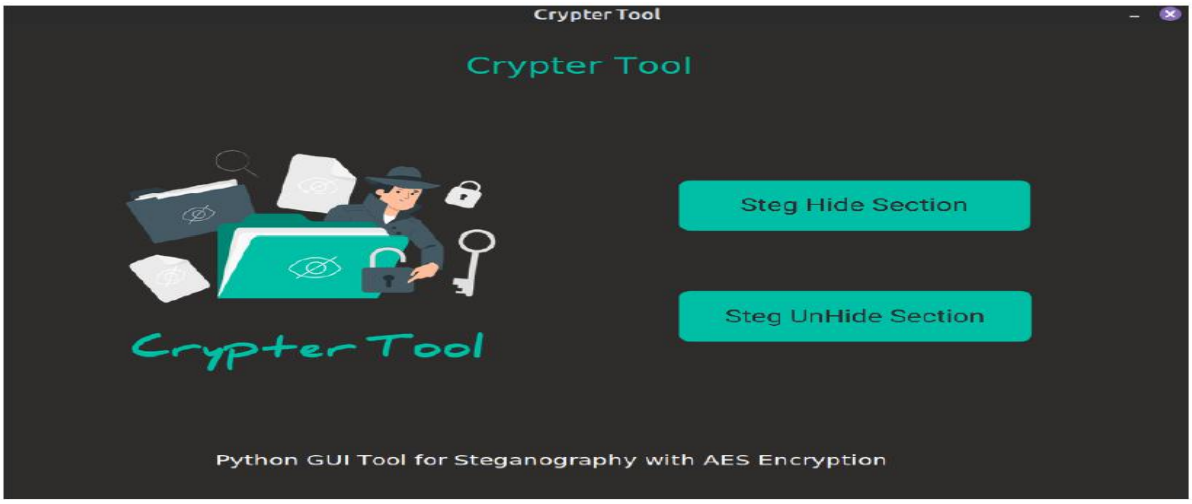

Fig.4 Home Screen page

This is the first screen which shows up when the system is launched, the screen has two option tab;

a. Steg Hide Section

b. Steg UnHide Section

STEG HIDE SCREEN

i. Before selecting cover image This section has options for selecting the cover image and entering secret information. Click on the button “choose an image” that is next to the select Image textbox. A dialog box will display as Shown, Specify where and which image file to be used as a carrier image and click on Open button to upload it into the system

ISSN: 2366-1313

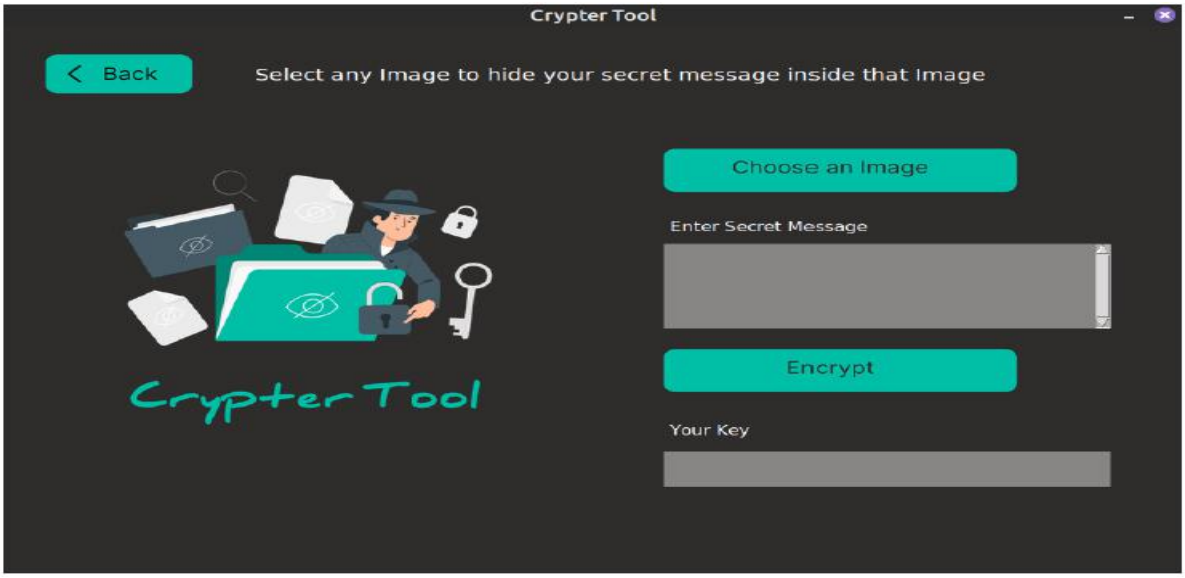

Fig.5 Steg Hide before selecting image screenshot

ii. after clicking encrypt button Click on the button "Encrypt" that is next to the select Image textbox. After clicking, a message box will appear saying that the stego image saved in program location and you will be given with a decryption key.

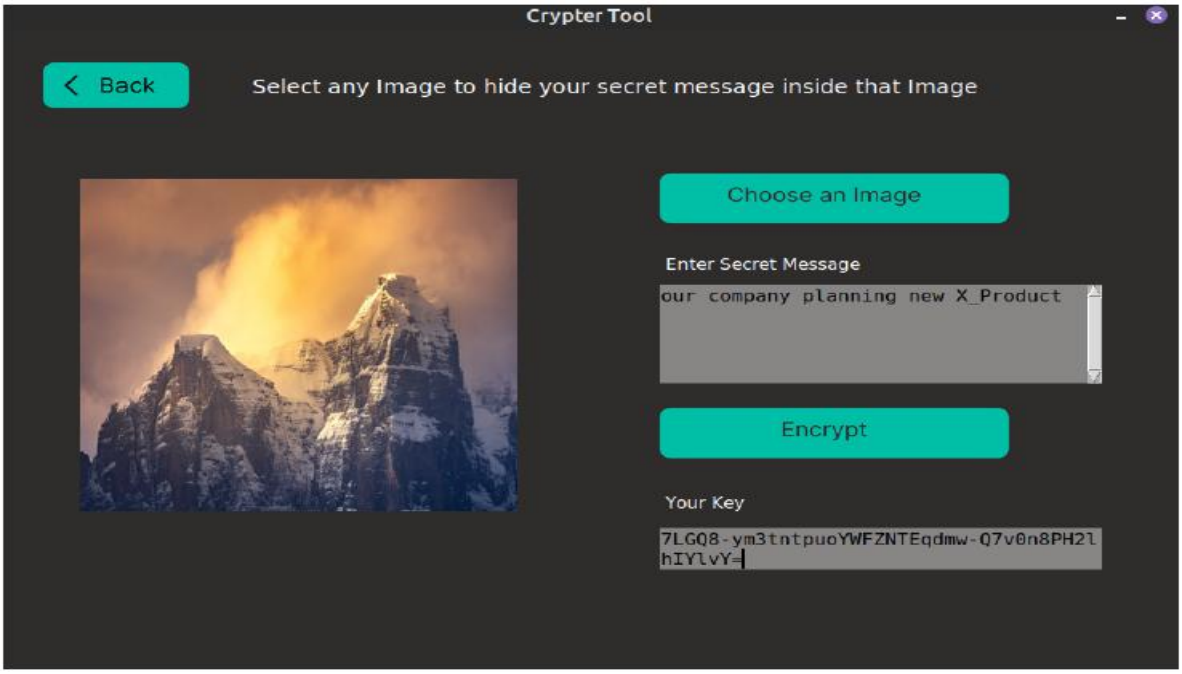

Fig.6 Steg Hide after clicking button encrypt screenshot

2. STEG UNHIDE SCREEN

ISSN: 2366-1313

i. Before selecting stego image: This section has options for selecting the cover image and Decryption Key. Click on the button "choose an image" that is next to the select Image textbox. A dialog box will display as Shown, Specify where and which image file to be decoded and click on Decrypt button.

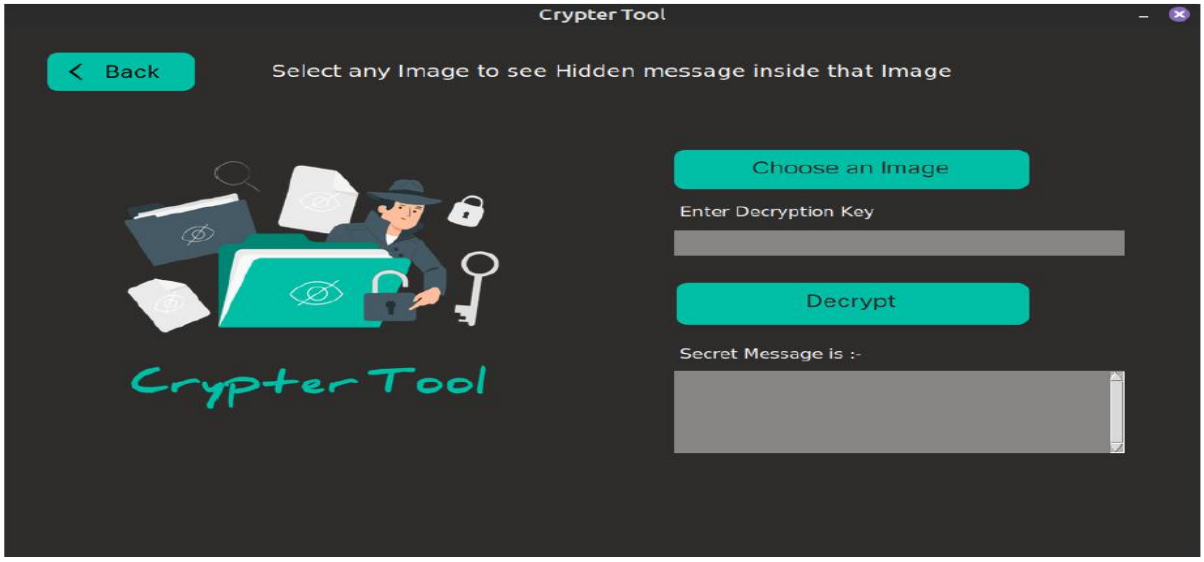

Fig.7 Steg UnHide before selecting image screenshot

ii. after clicking decrypt button Click on the button "Decrypt". After clicking, if decryption is correct for decrypting the cipher text then it will display secret information

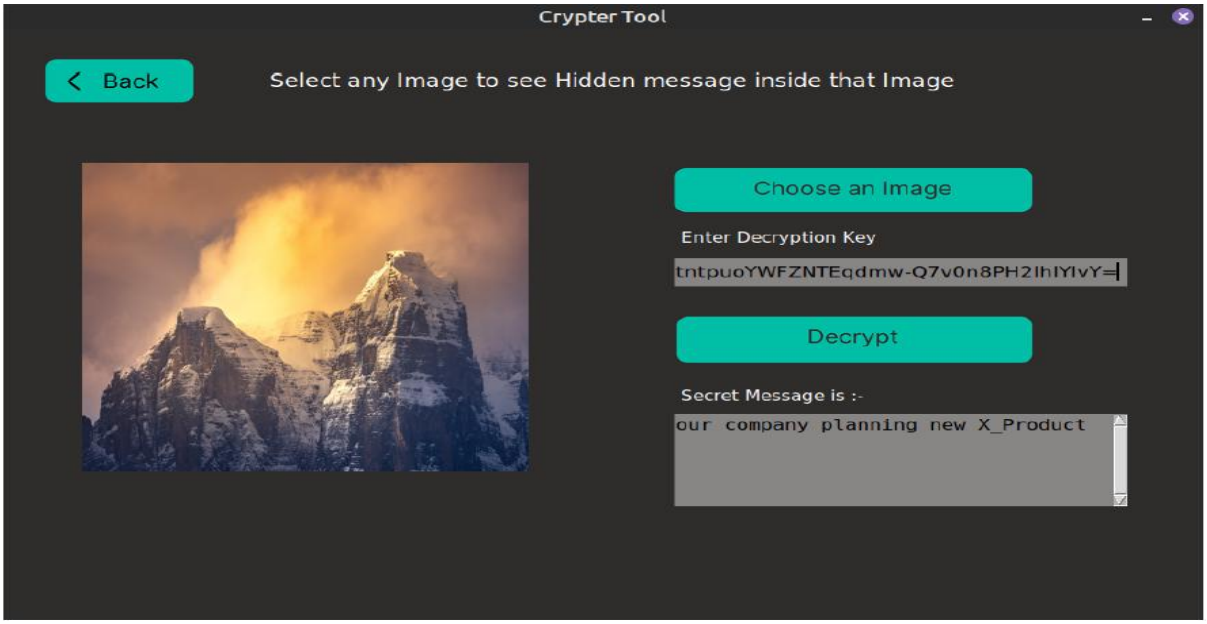

Fig.8 Steg Unhide after clicking decrypt button screenshot

ISSN: 2366-1313

VI. CONCLUSION

On the basis of our project study, this research came up with the following conclusions: An encryption system which can hide information and data in an image file was the best way to keep such data and information from unauthorized usage and modification. Since even a leaked stego-image will still require a known algorithm or the steganographic system to decrypt it. Moreover, it could be concluded that the implementation of the image steganographic system in the said company hides the very existence of the form of encryption deployed. This has helped to prevent suspecting the very existence of the hidden data or information file. This means that the company has reduced the risk of information and data modification and access by unauthorized persons as well as making information in the company more manageable, that is information is available, authentic, and confidential and its integrity is protected. We used the least significant bit algorithm in this project for developing the system because it is faster, reliable and compression ratio is moderate compared to other algorithms. And lastly, the study concludes that the personnel of the company are the fundamental barometers of the level of efficiency provided by the image steganographic system. In order to develop an ultimate Encryption system, a prior consultation among the employees would be advisable in order to cater the needs of who and which department will use the system and the types of images to use since every image has a copyright or an owner.

REFERENCES

[1] Shirey R. Internet Security Glossary, Version 2. RFC 4949. 2007.

[2]. Mohammad Fahmi, Alalem Abdallah , Muhanah Manasrah,(2008) "A Steganographic Data Security Algorithm with Reduced Steganalysis Threat," Birzeit University, Birzeit.

[3] Wang, H & Wang, S," Cyber warfare: Steganography vs. Steganalysis ", Communications of the ACM, 47:10, October 2004

[4] Johnson NF, Jajodia S. Exploring steganography: seeing the unseen. IEEE Computer 1998;31(2):26–34.

[5] R A Isbell, "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, 10 May 2002.

[6] M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, pp. 21-25, January 14-15,2003.

ISSN: 2366-1313

[7] J.Zollner, H. Federrath, H. Klimant, et al., “Modeling the Security of Steganographic Systems”, in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.

[8] N. Provos, P. Honeyman, “Detecting Steganography Content on the Internet”. CITI Technical Report 01-11, 2001.

[9] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99, Ed., Apr. 1999, pp. 274--278.

[10] C. Cachin, “An Information-Theoretic Model for Steganography”, in Proceedings 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.

[11] Evans, J.A.S. (2006).The beginnings of history: Herodotus and the Persian wars. Campbellville, Ont.: Edgar Kent. ISBN 0-88866-652-7