

Two Level Hiding an Encrypted Image

by Faten Hassan Al-kadei

Submission date: 02-Jul-2019 06:45PM (UTC+0300)

Submission ID: 1148711336

File name: 00_Template_IJEECS_May_2019_v14n2.docx (3.53M)

Word count: 2911

Character count: 15227

Two Level Hiding an Encrypted Image

Faten Hassan Al-Kadei¹

¹Computer Department, Northern Technical University, Kirkuk, Iraq

Article Info

Article history:

Received
Revised
Accepted

Keywords:

A Fractal Image
B Cryptography
C Steganography
D Image Encryption
E Image Decryption
F Hiding Image

ABSTRACT (10 PT)

Encryption and hiding image are becoming a hot research area and a broad prospect for application. Different Encryption and Cryptography technologies have been rapidly developed in recent years. Numerous methods of image cryptography and hiding have been proposed to protect image data confidentiality from unauthorized persons. This article uses a secure algorithm with Low Significant Bit method to hide an encrypted high-resolution color bitmap image (secret image) in two selectively color images (i.e. two cover images). The paper introduces a two-level hiding encrypted image using MATLAB-GUI programming language. It is a powerful support for data analysis and visualization tool designed for matrix and matrix operations. In the beginning, with a key image using XOR bit operation, the original RGB image is encrypted. After that, the encrypted image is hidden into the first cover image. The cover image is then hidden into another cover to make the secret image safer without changing the perceptual quality for both covers. Then, the algorithm is tested on many bitmap images which can be an important image, fingerprint image, samples of secret medicine or bank account pattern. The correlation histograms demonstrate high correlation for all encrypted images. The PSNR is used to find steganography quality for the two cover images after hiding the secret image showing a high quality for the two levels of hiding operation.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Faten Hassan Al-Kadei,
Computer Department,
Northern Technical University, Iraq.
Email: fatenhello@yahoo.com

1. INTRODUCTION

Security became an important issue in image storage and communication, and one of the important ways the security can be ensured is encryption. In many applications, data hiding is essential; the basic methods for hobbyists are steganography and cryptography, secretive data transmission, user privacy, and so on.

A The main aim of image encryption techniques via hiding image is converting the original image to another one to be difficult to understand. In other words, its primary goal is keeping image confidentiality between users. Therefore, no one knows its content without a key for decryption. Reliable security is crucial in sending and receiving digital images in different applications such as online personal photo album, medical system images, image communications in military and videos of confidential conferences, etc.

The basic methods for hobbyists are as follows: steganography and cryptography, secretive data transmission, user privacy, etc. It has been proven that steganography is the best method of safety. Furthermore, three different methods of hiding information are generally used: steganography, cryptography and watermarking. There are different types of steganography [1][2]:

1. Steganography of Text.

2. Steganography Image.
3. Steganography Audio.
4. Steganography of Videos.

The basic principle of steganography in all of these methods is that any secret message can be embedded in another cover object that may have no meaning in such a way that encrypted. Lastly, the displayed data is only the cover data. Therefore, containing hidden information cannot be easily detected unless proper decryption is used. Each steganography has three components:

1. Secret Object.
2. Cover Object of the message.
3. Steganographic objects results.

Using specific techniques, the information that has to be hidden is encoded in cryptography; this information is generally understood as coded data that appears nonsensical. Basically, steganography is information hiding which cannot be identified as the coded information seems to be abnormal in its presence sight and undetectable. Furthermore, steganography detection is named steganalysis. Moreover, steganography is one of the powerful techniques used to hide a secret image, audio files, and videos so that no one can find a secret hidden image in another one. Besides, steganography image refers to hiding in another image or video file information (i.e., text messages, images or audio files), and by proper decoding technique, this hidden information can be retrieved. Therefore, steganography is defined as “the art of hiding data media files”, which means the way of hiding any message (e.g., text, image, audio, etc.) in any file (e.g., .mp3, wav or .png) [3][4]. In the literature, there are several methods of steganography performance; however, the Least Significant Bit (LSB) is considered as the most famous one. This is mainly because there are three components in each color image; this pixel data is saved in one byte in encoded format. It is possible to modify the low bits that contain little information for each pixel to store the hidden text. The precondition for the stored text that it must be smaller or equal to the image that is used to hide the text. There are two different image steganography methods:

In the literature, there are several methods of steganography performance; however, the Least Significant Bit (LSB) is considered as the most famous one. This is mainly because there are three components in each color image; this pixel data is saved in one byte in encoded format. It is possible to modify the low bits that contain little information for each pixel to store the hidden text. The precondition for the stored text that it must be smaller or equal to the image that is used to hide the text. There are two different image steganography methods:

1. Methods of space.
2. Transform methods, LSB method is the most common method used in spatial substitution method.
3. Retrieve the message images from recombining the lower four-bit planes.

The image pixels are assigned to be stored in the form of bits. The intensity of pixels is stored in an 8-bit (i.e., 1 byte) image on a grayscale. Similarly, each pixel requires 24 bits (8 bits for each layer) for color (red, green and blue (RGB)) images. When the LSB bit is modified, the Human Visual System (HVS) is unable to detect these changes in pixels' intensity or color. This is obscure visual redundancy which can be used to hide information in these bits with no significant difference is observed in the image. Accordingly, it is possible to modify the first bits to carry the information to store a hidden text in each pixel or a picture (see Figure 1). By replacing the LSB in a BMP type picture, it embeds data into the photo [1].



Figure 1. Hiding Information in the LSB.

Since it has the smallest effect on the amount of color, the smallest possible impact on the picture will replace this bit with a bit of the hidden data. Using this method, the image steganography embeds the

secret in each pixel of the cover image in the LSBs. It is well known that the LSB based steganography is one of the simplest techniques to hide pixel values without perceptible distortions from a secret message in the LSBs. The changes in LSB value are invisible to a human eye.

In the literature, cryptography is considered as an effective way to securely transfer information. It scrambles the image information before transmitting it to change its structure. Therefore, the attacker cannot be hacked because it is hard to get back the original image. So, it provides an image's modified shape, but it does not hide the image even if it is a good security method. The main objective is to provide the original image with better protection [5][6].

Image encryption is a process of information transformation (known as a plain image) by using an algorithm (referred to as a cipher) making it incomprehensible to any person except those with special knowledge (known as a key). This process results in an encrypted image (called a cipher image). The process of converting the cipher-image back to its original shape so that it can be perceived is called Decryption. Furthermore, image encryption is usually used to protect images (computer and storage devices images) when personal records are exposed to loss or theft of laptops or backup drives. It helps to guard against uncovering and sharing. Moreover, encryption is also applied to protect the transit data, such as data transmitted through networks (e.g., e-commerce and internet), wireless systems, mobile phones, Bluetooth devices, etc. Besides, the cryptography technique is further classified into two major types: symmetric and asymmetric key cryptography. For purposes of both encryption and decryption, symmetric key cryptography requires a single private key. On the other hand, the asymmetric key uses two keys first for encryption and the other for decryption purpose [7][8].

2. PROPOSED METHOD

Image encryption techniques attempt to convert the original image to another image that is hard to understand. Accordingly, it keeps the image to be confidential among users to ensure information security when much sensitive information is stored on computers and sent over the internet. Therefore, our method is proposed used to hide a bitmap color image (original) in another bitmap color image (cover image), to make the hidden image (secret image) more secure. As shown in Figure 2, in the first stage, the generated key image is used to encrypt the original image creating the secret image. The second stage of security works is to hide the secret image after encrypting it into two cover images. The first image is used as cover images to the secret image, while the second one is used as the cover image to hide the first cover; in consequence, providing two level hiding systems.

The encryption is then achieved by first generating of the encryption key image using different computation methods and the XOR operation. Then, encrypted image pixels are hidden in another image (i.e., cover1) in the LSB to create the level-1 image. This image is then hidden in another image (i.e., cover 2) to generate the level-2 image to add an extra layer of security (see Figure 3). Since each pixel needs 8 bytes to be hidden in the cover image, the secret image should be less than the cover image (Cover1) at least by 1/8. Additionally, Cover1 must be less than the Cover2 by 1/8; in consequence, these covers are stretched to be of the proper size. As illustrated in Figure 2, the main encryption and hiding algorithm are summarized in the following steps:

- step-1: Load the color bitmap image (Original image).
- step-2: Generate a key image.
- step-3: Encrypt the original image with the generated key to get the Secret one.
- step-4: Load the cover image (Cover1).
- step-5: Hide the encrypted Secret image in Cover1 generating level-1 stego image.
- step-6: Load the second cover image (Cover2).
- step-7: Hide the level-1 stego image in Cover2 generating level-2 stego image.
- step-8: Output Stego image.
- step-9: End.

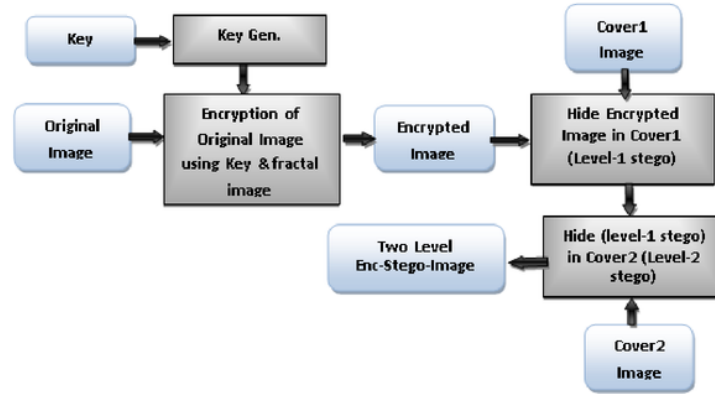


Figure 2: Encryption and Hiding Steps Diagram.

The key generation Algorithm mentioned in step-2 in the above algorithm is applied using the following steps (see Figure 3):

- step-1: Load the color bitmap image (Original image).
- step-2: Apply the function (Reshape) on the Secret image; this function changes the size and the position of the image pixels to obtain the Final Secret image.
- step-3: Find the mean factor by using Mean function.
- step-4: Input two External Keys to be used in key image generation.
- step-5: Apply calculations using the above-selected keys and mean factor on the Original image to create a key image by taking the mod of each pixel.
- step-6: Rotated the key image (180) degree using rotation function (imrotate).
- step-7: Combine the images from step-1 and step-5 using bitwise XOR function to obtain the Secret image.
- step-8: Output Secret image.
- step-9: End.

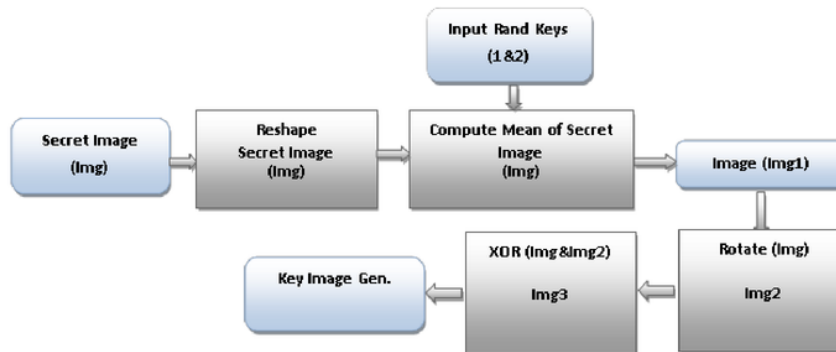


Figure 3. Key Image Generation Diagram.

To get back the original image, the Decryption and Un-hiding steps are applied in reverse sequence as shown in the following algorithm (see Figure 4):

- step-1: Input level-1 Stego image (Cover1).
- step-2: Get level-1stego image from the Level-2 stego image (hidden in Cover2).
- step-3: Get the secret encrypted image from the level-1stego image.
- step-4: Input secret keys
- step-5: Generate the Key image using the above generation algorithm.

- step-6: Decrypt the secret image using the key image in reverse steps of the Encryption to get the Original image.
 step-7: Output the Original image.
 step-8: End

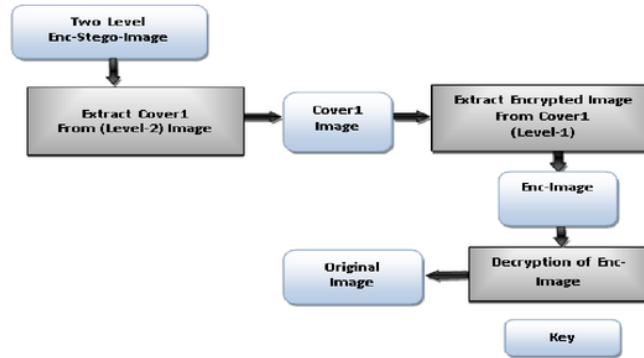


Figure 4. Decryption and Un-Hiding Steps Diagram.

3. THE GUI SYSTEM FOR PROPOSED METHOD

All operations of the system are performed through a designed system using Matlab Graphic User Interface (GUI) tools to make all systems operations easier. A number of examples are illustrated in Figures A1 to A6 in Appendix A. The system operations that the designed GUI system can perform are listed below:

1. Selecting, loading and displaying the original image.
2. Encrypting the original image with input keys and display the encrypted image.
3. Displaying the histograms of both the original and encrypted images.
4. Selecting and load Cover1.
5. Hiding the encrypted image in cover-1(level-1 stego image) and display it.
6. Selecting and loading Cover2.
7. Hiding the encrypted Cover1 (level-1 stego image) in Cover-2 (level- stego image).
8. Displaying the final stego image.
9. Unhiding the Cover1 from level-2 stego image.
10. Unhiding the secret image from (level-1 stego image).
11. Decrypting the secret image using the generated key image.
12. Lastly, calculate the PSNR for cover images.

4. ⁵ RESULTS AND ANALYSIS

The proposed method has been tested with different secure images (Fprint, Medim, GISim, Codeim and Eyeim) and different cover images (Nature, Bird, fruit, Baboon, Car, etc.). The resulted images are tested using histograms in Matlab application and human vision as follows:

1. The first security stage is Encryption operation. Using two random secret keys to create secret image encryption gave the system a random key image. The system has tested several times with different keys and each time it provided different key image (see Figure 5).
2. As shown in Figure 6, the encrypted secret images is not intelligible in vision because of using different methods on the secure image before encrypting it with the generated key image.
3. Comparing histograms of the original images and the encrypted image showed high correlation for the encrypted image pixels (see Figure 6).
4. The second security stage is hiding operation has done on two levels. The first level is hiding the secret image in the first cover; while the second level is hiding this cover again in another cover. The PSNR has then calculated to find the quality of each cover images (cover image level-1 & level -2). All tested results showed a high quality for all covers in both levels of hiding operation, and it was more than 50 Db (see Figure 7).

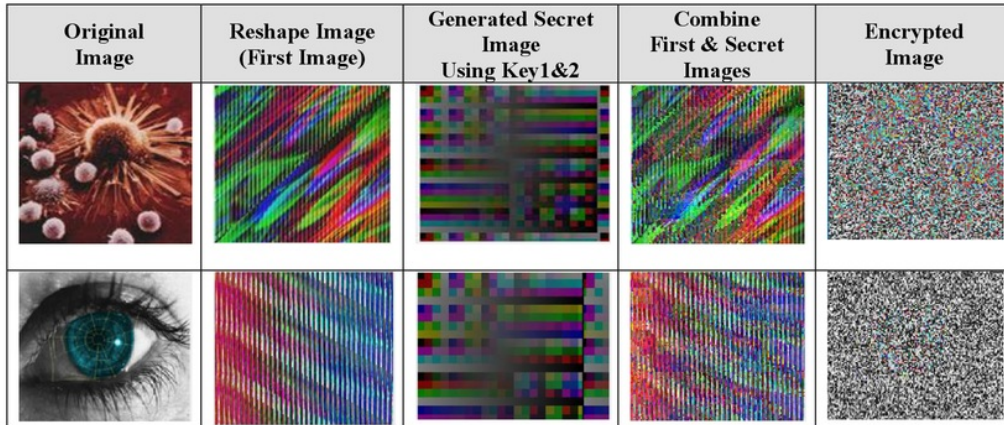


Figure 5. Secret image encryption steps

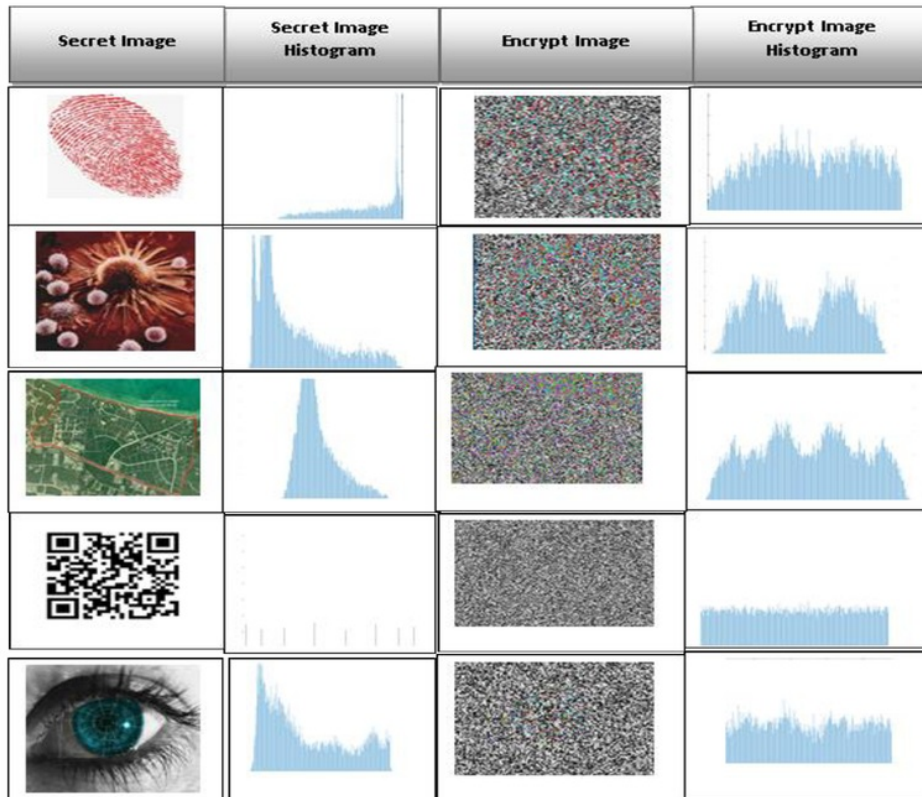


Figure 6. Histograms of original secret images and encrypted images.

Secure Image	Cover Image Level-1	PSNR of Cover1	Cover Image Level-2	PSNR of Cover2
















		52.9833		51.6642
		52.1794		51.6655
		51.1399		53.0003
		51.1353		51.6529
		52.3869		51.6538

Figure 7. The PSNR of the cover images (Cover1 & Cover2) after hiding operation.

5. CONCLUSION

In this article, we used new symmetric cryptography algorithms to encrypt and hide a secure color image in another color image. The findings showed that the proposed encryption technique had provided the system with a high secured image. This approved by the high correlation shown in the resulted histograms that prevent attacks on the secret image.

Using two-level hiding to hide a color image provided efficient security for the secret image. Both used cover images were at high quality PSNR after hiding the secret image information, because of using the LSB technique. The broad range of cipher key ensures the secret image's integrity and authenticity.

REFERENCES

- [1] S. Bhallamudi, "Image Steganography," in *EE7150 – Digital Image Processing*, 2015, pp. 1–17.
- [2] Z. Alqadi, B. Zahran, Q. Jaber, B. Ayyoub, J. Al-Azzeh, and A. Sharadqh, "Proposed Implementation Method to Improve LSB Efficiency," *Int. J. Comput. Sci. Mob. Comput.*, vol. 8, no. 3, pp. 306–319, 2019.
- [3] M. G. Anchal Chander Lekha, "Hiding an Image Data into Video Stenography Using Different Algorithm and MATLAB: A Review," *Int. J. Comput. Sci. Trends Technol.*, vol. 6, no. 2, pp. 12–16, 2018.
- [4] A. B. M.S. Bouridah, T. Bouden, "Fractional Chaos Synchronization for Color Image Encryption," in *Third International Conference on Technological Advances in Electrical Engineering (ICTAEE'18.)*,

Title of manuscript is short and clear, implies research results (First Author)

2018, pp. 1–8.

- [5] K. D. Patel and S. Belani, "Image encryption using different techniques: A review," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 1, pp. 30–34, 2011.
- [6] R. Kaur and E. K. Singh, "Image encryption techniques: a selected review," *J. Comput. Eng.*, vol. 9, no. 6, pp. 80–83, 2013.
- [7] A. Nag *et al.*, "Image encryption using affine transform and XOR operation," in *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*, 2011, pp. 309–312.
- [8] R. M. Rad, A. Attar, and R. E. Atani, "A new fast and simple image encryption algorithm using scan patterns and XOR," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 6, no. 5, pp. 275–290, 2013.

Appendix (A)

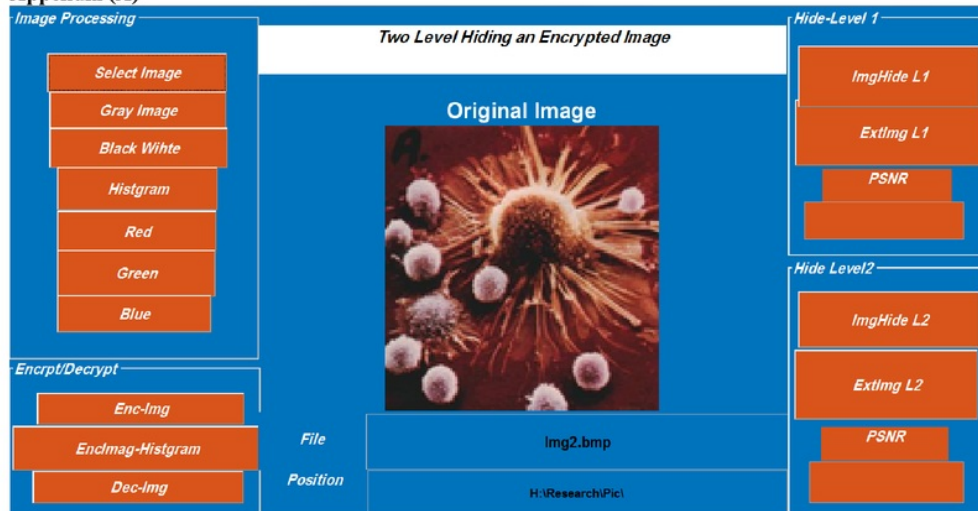


Figure A1. GUI of the system showing the original loaded image.

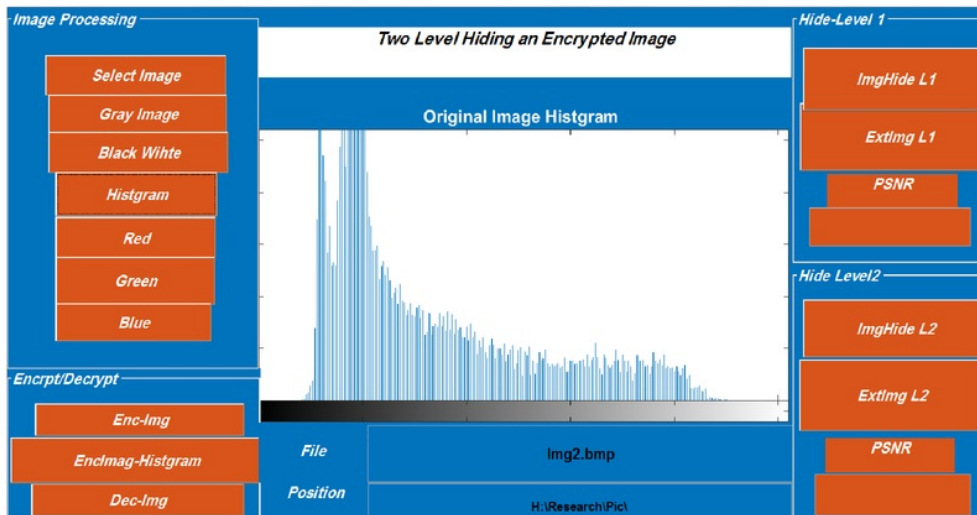


Figure A2. GUI of the system showing the Histogram of the original secret image.

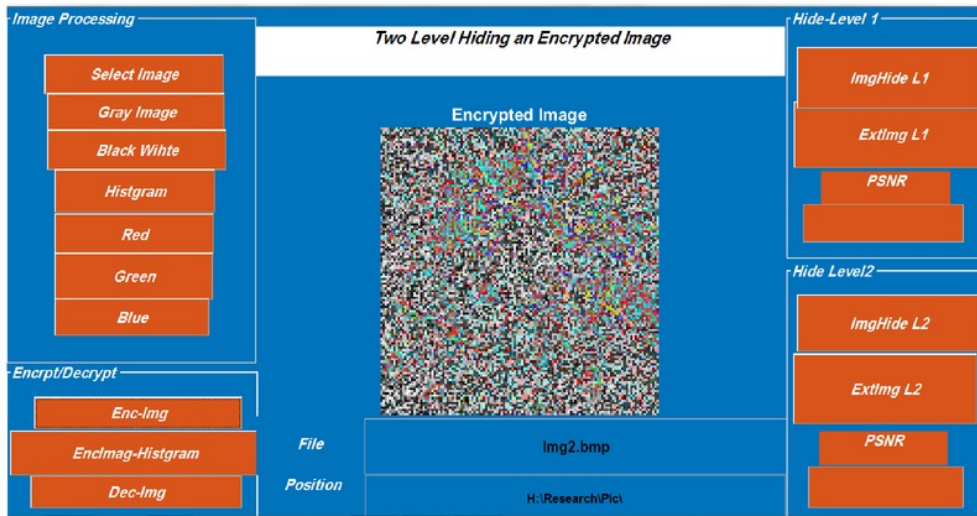


Figure A3. GUI of the system showing the encrypted secret image.

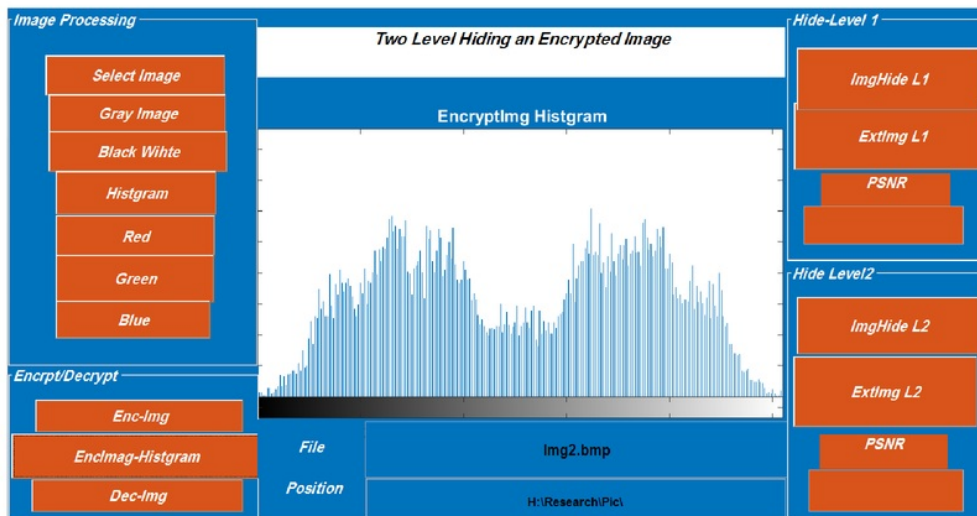


Figure A4. GUI of the system showing the Histogram of the encrypted secret image.

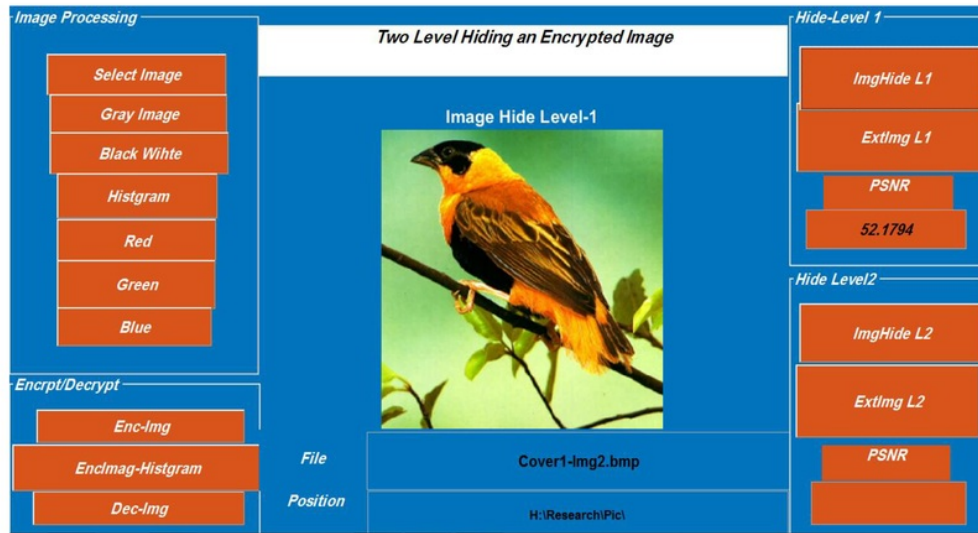


Figure A5. GUI of the system showing the Cover1 that contains the encrypted secret image

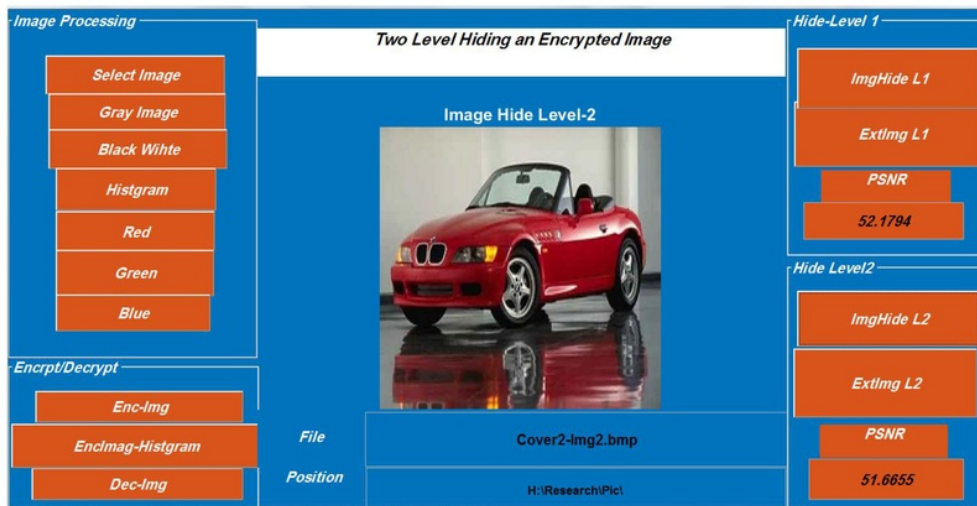


Figure A6. GUI of the system showing the Cover2 that contain the Cover1 image.

Two Level Hiding an Encrypted Image

ORIGINALITY REPORT

6%

SIMILARITY INDEX

1%

INTERNET SOURCES

1%

PUBLICATIONS

5%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Visvesvaraya Technological University Student Paper	2%
2	Submitted to University of Wales central institutions Student Paper	1%
3	Submitted to Amman Arab University for Graduate Studies Student Paper	1%
4	Submitted to University of Mustansiriyah Student Paper	1%
5	"Advanced Computational and Communication Paradigms", Springer Nature, 2018 Publication	1%
6	Submitted to iGroup Student Paper	1%

Exclude bibliography On