https://dx.doi.org/10.22161/ijaers.74.57 ISSN: 2349-6495(P) | 2456-1908(O)

Gray Code Based Data Hiding in an Image using LSB Embedding Technique

S. Vivekanandan, C. Manju, P. Deepa and R. Lavanya

Department of CSE, Velalar College of Engineering and Technology, Tamilnadu, India

Abstract**—** *Data concealment is one among the techniques for concealment knowledge the information from data hackers. It's the foremost helpful technique. Gray code technique is additionally used as a result of the security level is high. During this technique a standard image is reborn into black and white color image. To use LSB embedding technique it suggests that an information is encrypted and it's reborn into binary kind. A picture contains the components every pixel to insert the LSB and encrypts the information, and also the image. A sender is to insert the information within the image and sends to the receiver aspect. The receiver decrypts the image, and it's simply read a picture and information. An information is definitely hack by the hacker, so, we to tend to use Separate reversible technique it suggests that an information, and it contains random bits enclosed the information. Therefore, the hacker does not perceive which means of the knowledge. It's terribly high level security.*

Keywords**— *Decrypt, Encrypt, Gray code, LSB, Separable Reversible Data Hiding.***

I. INTRODUCTION

A gray code is a binary form of two successive values. Different in one bit, For example 00, 01, 10, 11, etc., Now currently gray code is widely used for error correction in digital communications. Gray code is designed to detect the output from electric mechanical switches. This code is non-weighted code compare to other codes. It is also known as minimum change code.

Methodology: Convert the binary to gray code

a) In this code, we can change only one bit in that code.

b) It is called as Reflected binary code or Frank code.

c) For example, A decimal 3 to 4, the gray code changes from 0010 to 0110.

d) The binary changes from 0011 to 0100 to change 3bits.

In the real time environment use data encryption and decryption processes. This process is the latest technique in network sides. Encryption is the most important security tool. Why means data passes through the shared devices and network segments where many people can access the information. Encryption that involves transformation of data into scrambled, it is called a Cipher text. This process uses the authentication key it's a large number associated with password. The encrypted text is decipherable only by the receiver. The deciphering process is called decryption. Revised process of encryption is known as decryption. Encrypted data or that related file is received at the receiver then the data been to be decrypted. So the information can be easily viewed by the at the end receiver.

Steganography technique is the concealment of data within the other datum. It is difficult to prevent the presence of hidden data or information. LSB Steganography is one of the easiest to implement method in image steganography. But rarely used in primitive form. It is can be cracked using steno analysis basic techniques. This method we can embed the one bit of the data is hiding in each pixel of that image then the results in insignificant distortion. LSB method is not suitable for use image manipulation technique likes image compression. This algorithm uses combination of LSB technique or a method it is similar to private key cryptography. The key is associated with every stegano data and must be available with both sender and the receiver.

Key is used as a seed in our random bit generator function. To generate the random bits are used to circular rotation each of the bytes the stegano data.

II. OVERVIEW

Now currently a signal processing is encrypted domain has attracted with the research internet. Effective and popular meaning as privacy protection, and encryption converts original signal into the data. The traditional processing is usually takes places before encryption and after decryption. Novel scheme for separable reversible data hiding in the encrypted images. To encrypts the original uncompressed image using as an encryption key. Data hider replace the

https://dx.doi.org/10.22161/ijaers.74.57 ISSN: 2349-6495(P) | 2456-1908(O)

LSB of the encrypted image using a key to create the sparse space to accommodate some additional data. Reversible data hiding approach is mainly used in this project. The following are the main modules of that project:

a) Image file selection: Image file selection carried out the open a file dialog control and path is displayed in the text box, and the image is also displayed in the picture control box. And select the image in the file.
b) Pseudo random bit input: In this random bit keys is used for during image encryption.
c) Image encryption: Image bits and pseudo random bits are performed as X-OR operation and the result bit sequence replaced for an image bits. That the image can be encrypted.
d) Text data input: To hide the data is keyed and the text is being embedded into the encrypted image.
e) Data embedding after gray code conversion: The record in which the data is being hide is selected. The data is converted into gray code.
f) Data extraction: The encrypted image sent by the received, and the reverse operation is carried out to fetch the data.
g) Image encryption: The encryption image is applied with reverse operations to get the original image.

III. EXISTING SYSTEM

Uses the gray code primarily based technique is employed to hide a text within the digital image and rewrite it. The prevailing theme is formed of image encoding, information embedding and information encrypting phases. The information hider compress the LSB of the encrypted image employing a data-hiding key to make a distributed area to accommodate the extra data. At the receiver aspect, the information embedded within the created area are often simply retrieved from the encrypted image containing extra data consistent with the data- hiding key. Since the information embedded solely affects the LSB, a secret writing with the encoding key may result in a picture like the initial version. Once exploitation each of the encoding and data-hiding keys, the embedded extra information are often with success extracted, and therefore, the original image is often dead recovered by exploiting the special correlation in natural image.

DRAWBACKS OF EXISTING SYSTEM

a) Only text is encoded with its gray to code value. Not extra content is added to perturbate.
b) Separate encoding mechanisms are used for image encryption, and data hiding.
c) Operates on gray scale image data only.
d) Carrier image must be large since one bit per pixel is used.

IV. PROPOSED SYSTEM

The projected system implements all the prevailing system methodologies. Additionally, the RGB color image is taken for image coding. Throughout image coding pseudo-random bits are X-or with image pixel bits as in existing system. Throughout reverse method, either the initial image or text alone will be retrieved by the receiver. Additionally, text computer file are discomposed such random characters are infix within the initial text. Moreover, the text information is encrypted mistreatment Triple DES coding, so hide in to the encrypted image.

ADVANTAGES OF PROPOSED SYSTEM

a) Same encryption mechanisms are used for image coding, and information concealing.
b) Operates on RGB image information conjointly. 2 least vital bits of a given pixels can even be used for information concealing.
c) Tiny carrier image conjointly supports a lot of information concealing than the prevailing system.
d) Text perturbation and Triple DES coding makes the appliance safer. It provides analyses of the quantity of speed measurements required to form reproduction detection selections, that shows are quite low, and also the quantity of overhead incurred by running the protocol.

https://dx.doi.org/10.22161/ijaers.74.57 ISSN: 2349-6495(P) | 2456-1908(O)

V. FIGURES

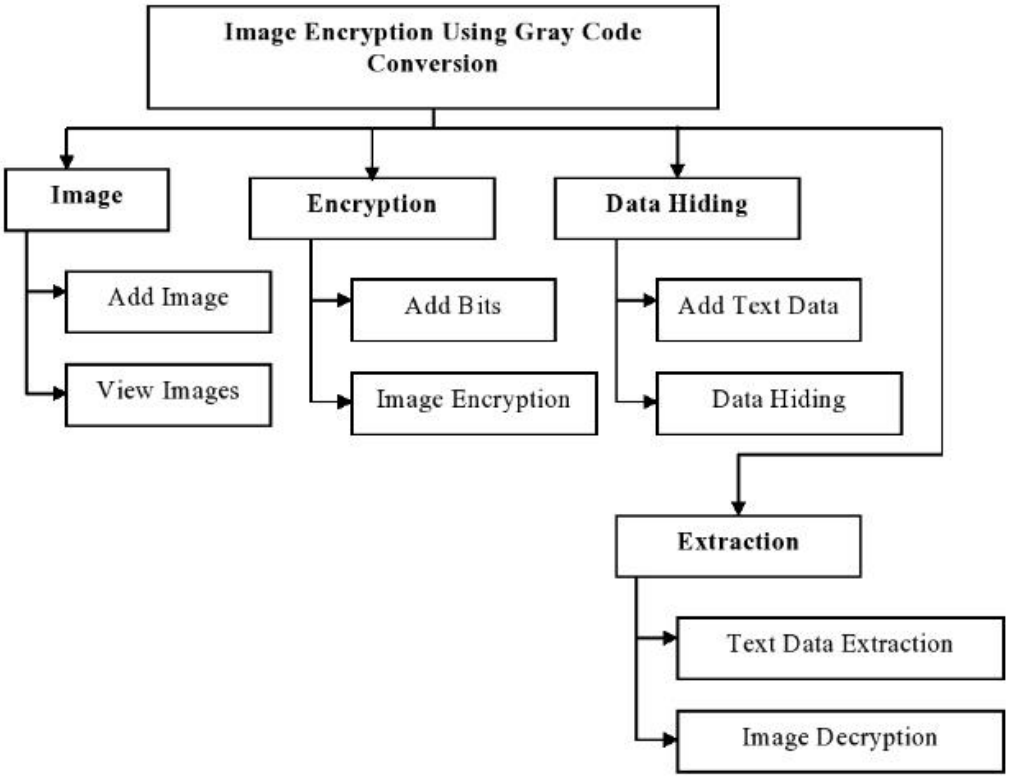

Fig.1: System flow Diagram

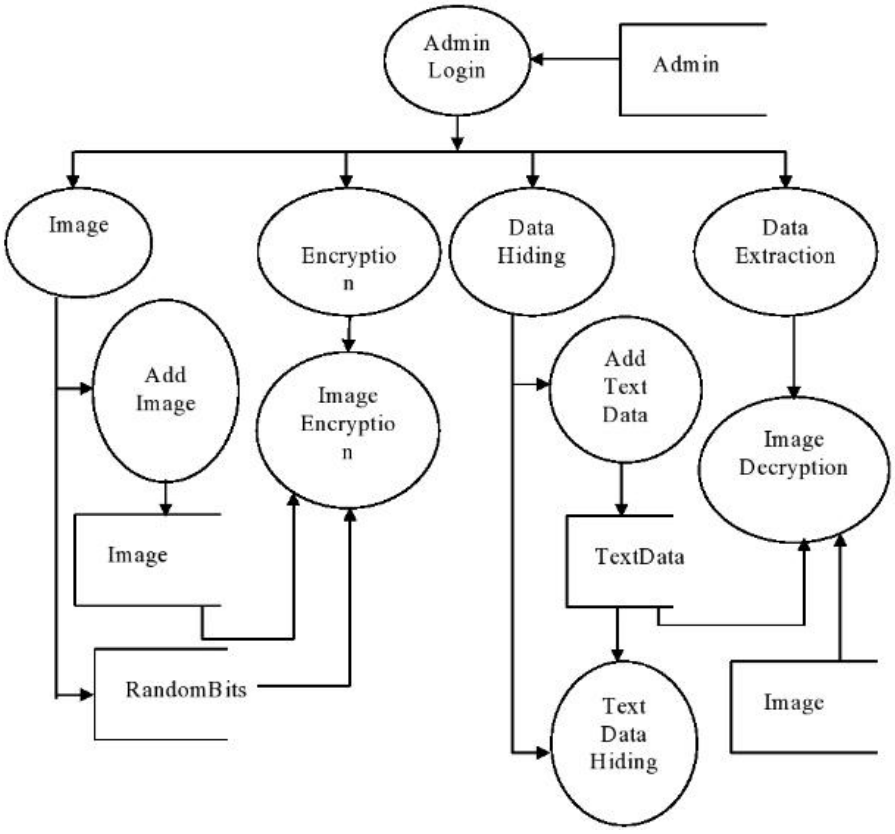

Fig.2: Data flow Diagram

https://dx.doi.org/10.22161/ijaers.74.57 *ISSN: 2349-6495(P) | 2456-1908(O)*

2. TABLES

Table.1: Admin

S.NO	FIELD NAME	DATA TYPE	SIZE
1	UserName	Varchar	15
2	Password	Varchar	15

Table.2: Images

S.NO	FIELD NAME	DATA TYPE	SIZE
1	ImageId	Int	4
2	ImagePath	Varchar	255
3	ImageWidth	Int	4
4	ImageHeight	Int	4
5	OriginalImageData	Image	16
6	XORBits	Varchar	1024

Table.3: Raw messages

S.NO	FIELD NAME	DATA TYPE	SIZE
1	Sno	Int	4
2	MessageData	Varchar	300
3	EntryTime	DateTime	8
4	PertubatedMessage	Varchar	1000
5	EncryptedMessage	Varchar	8000

VI. CONCLUSION AND FUTURE WORK

In separable reversible data hiding at the receiver side when the receiver has data hiding key only know the receiver. It is easy to extract and add additional data also. Novel GRB and LSB method for embedding the data, the size of the net payload can be increased sufficiently. We can hide the data into encrypted image also. Text can be inserted into video and can be decrypted at the end of the receiver. Data can also be encrypted as audio form and decrypt by the receiver.

REFERENCES

[1] Ahmed A. Abd EL-Latif, Bassem Abd- EI-Atty, Salvador E. Venegas-Andraca "A novel image steganography technique based on quantum substitution boxes", Optics & Laser Technology, Volume 116, August 2019, Pages 92-102

[2] Liu, Yunxia, Liu Shuyang, Wang, Yonghao, Zhao, Hongguo, Liu, Si "Video steganography: A review", Neurocomputing, Volume 335, 28 March 2019, Pages 238-250

[3] Charan GS, NithinKumar SSV, Vaithiyanathan V, Divya Lakshmi, Karthikeyan B "A novel LSB based image steganography with multi-level encryption", ICIIECS 2014-2015, IEEE International Conference on Innovations in Information, Embedded and Communica-tion Systems, 12 August 2015, Article number 7192867.