Secure Secret Image carrier using Rubiks Cube and Modified LSB

Rekha.B¹, R H Goudar², Rohit.B³,
¹,²,³Dept. of Computer Network Engineering
Center for PG Studies,
¹,²,³Visvesvaraya Technological University
Belagavi, India.

August 15, 2018

Abstract

Data trade amongst sender and recipient turns out to be quick and simple. The nature of information sending, particularly the protection, should be taken note. Hiding, the information is necessary for securing information. It should be possible utilizing methods like cryptography and steganography. This paper defines the image steganography utilizing secret grayscale image and to hide the secret image, the RGB image is used as a cover. Since a secret picture is inserted within a cover, the encrypting procedure is done to give a more dependable security. The encryption technique utilized depends on the principle of Rubiks cube, by moving the pixel position in a digital picture. The modified LSB replacement technique uses in this Steganography works space. The goal of this plane is to get a great character hidden secret picture to put information secret.

Key Words: steganography, embedding, extraction, Rubik cube, LSB.
1 Introduction

These days, data and communication innovation develops quickly. Data trade amongst sender and collector turns out to be quick and simple. The nature of information sending, particularly the protection, must be taken note. There is a probability that unauthorized humans tap and modification message transmitted over microwave or other media. Securing a message should be possible utilizing cryptography or hiding data by scrambling the adjustment of information. In cryptography, information that has been encoded are yet accessible. While in steganography, information is embedded in to cover object. Information is covered up, trusting that unapproved parties are not suspicious about what is inside cover object. Before information can be perused, secret information must be removed first. In this paper, we explain a symmetric encryption strategy based with respect to the standards of a Rubik’s cube. In symmetric-key plans, the encryption and decoding keys are the same. In this way, conveying parties must have a similar key before they can accomplish secret communication. Scientifically, the Rubik’s Cube is a permutation group. The Rubiks Cube has six faces and in each face is secured by nine stickers, six face has unique strong colors generally white, red, blue, orange, green, and yellow. In 3 3 3, Rubik’s cube has six appearances (face) with changed color in each face, at the point when the nine distinct bits of all the six appearances (face) have the same color at that point the cube is solved. Each face rotated clockwise or anti-clockwise direction. The 3*3*3 Rubiks cube has eight vertexes and twelve edges. Cube is solved by utilizing 18 different rotation for traditional Rubiks cube. 18 different rotation are upper (1), horizontal (2), down (3), upper-opposite (4), horizontal reverse (5), down inverse (6), front (7), center (8), back (9), front-opposite (10), center opposite (11), back-reverse (12), left (13), vertical (14), right (15), left-opposite (16), vertical-reverse (17) and right inverse (18). In this paper, secret imaged encryption is done by using the Rubik’s cube standard. In past analysis, Rubik’s cube rule is suggested for encryption. The first initial image is mixed. At that point, by using the secret keys XOR administrator is connected into lines and sections of the scrambled picture. This encryption system has idealized hiding capacity and it is asserted as a great encryption system. When
an image is encoded, that image is embedded within a cover picture to hide it. The rest of the paper is organized as follows. Related work is represented in Section 2. Existing methods are explained in Section 3. Section 4 shows the proposed method. Section 5 presents experimental results. Finally, concludes the paper in Section 6.

2 RELATED WORK

Sevierda Raniprma, Bambang Hidayat, Nur Andin [1] This paper introduces information hiding systems by connecting encoding and steganography to accomplish top-grade covered-up secret pictures. Vyom Chhabra, Tejeswini Sundaram [2] in this strategy is a symmetric encryption method. Subsequently, the decoding procedure is the switch of the encryption procedure and it utilizes a similar secret key to decrypt. At first, the Plain Text is acquired from the client. The text is then changed over to binary digits, i.e. 0 or 1. The Binary Values are then populated on the information structure depicting the Rubik’s Cube model. When this stage is finished, the value is passed into two parts which are responsible for the encryption procedure and the generation of the ciphertext. The two segments: (1) Shuffling and (2) Vignere Cipher task. Rajavel D1*, Shantharajah SP2 [3] This present researchSecure Secret Image carrier using Rubiks Cube and Modified LSB

Rekha.B Rohit.B Department of Computer Network Engineering Department of computer Center for PG studies, VTU, Belagavi. Networking Engineering Center for PG Studies, VTU, Belagavi India. R.H. Goudar Department of computer networking Engineering Center for PG Studies, VTU, Belagavi India 2 actualizes the content scrambling encryption method in view of creating a random number arrangement for rotating Rubik’s cube. A Cubical portrayal of the message gives the curiosity of the examination and afford the new way to deal with the encryption system. Cubical type of text is more dependable for scrambling calculation, because single revolution of a cube scrambles the text in five out of six faces of a cube. Irregular number plays an important role in this to deal to define the rotation type, where the programmer(hacker) can’t effectively decode the cipher message without the key. Loukhaoukha 1, Chouinard, and Berdai [5] created a picture encoding algorithm.
utilizing a Rubiks cube rule to permute picture pixels. After a picture is mixed, to each line and section the XOR administrator is applied so as to befuddle the connection amongst original and encoded image this process explained in Fig.1.

Fig.1.Rubiks cube Encryption system

3 EXISTING METHODOLOGY

In existing system first will inserted the original information to cover image by using LSB method and will get the watermarked information, this process is called embedding as shown in figure 2, then embedding image transfer to receiver, in the receiver side, receiver extract the original information from the cover image this process is called extraction as shown in figure 3.
4 PROPOSED METHODOLOGY

In this paper presents the information hiding into the cover image through modified LSB. Before hiding in to cover image information is encrypted using the principle of Rubiks cube. After applying principle of Rubiks cube will get encrypt information then inserted in to cover image by using the modified LSB method. After hiding the secret information in to cover image will get the watermarked image this process called embedding as shown in Fig.4.

In receiver side, to get the original information the receiver Extract
the original information from the cover image by using modified LSB method in reverse will get the encrypted information. To decrypt the information receiver use the Rubik’s cube rule finally will get the original information, this process called extraction process is shown in Fig. 5. The Rubik’s cube has six different faces with different colors in every face, 9 different pieces over all six faces have similar color then cube is solved. A message is similarly isolated into 6 distinct blocks and number of a cube (N) is framed by taking information from 6 blocks, a number of pieces in each cube is made of B Size. B Size = (3 × 3) pieces 6faces = 54 For 3 × 3 × 3 cubes, a message is separated into N number cubes each solid shape (cube) contains 54 pieces and each 54 pieces is framed into six unique faces (different) (3 × 3 of 6 grids) containing nine pieces each. Every framework is set in cubical space by six varies faces front, back, upper, right, left and down as appeared in Figure 6.

Fig. 6. message arrangement in cubical structure

This project introduces information about hiding procedures by connecting encoding and steganography to accomplish brilliant covered up a secret picture. Steganography framework clarified in Fig. 7, with an encoding build on Rubik’s cube rule. Most importantly, a secret picture which is the grayscale picture is encoded (encrypted) utilizing system in view of Rubik’s cube rule, getting to be encoded picture. After that, it is inserted within a cover picture. Here procedure provides Stego picture. Now Stego picture is prepared to send.
5 LEAST SIGNIFICANT BIT

The least significant bit is the easiest algorithm, in which every 8-bit pixels minimum significant is over composed with a bit from the watermark. The modified LSB is different from LSB in specifying the position of embedding. To do this modified LSB method key is used to identify the initial position of embedding.

6 RESULTS

The process is done by utilizing the MATLAB tool. A Grayscale image is used as a secret image and RGB image use as a cover image. The secret image is encoded by using Rubik's cube rule and
encrypted secret information inserted in to cover image by utilizing
the modified LSB method. from fig.8, (A)encrypted secret image
histogram is uniform and it is different compared to the original
one. this image encryption is responsible to make confusion to
unauthorized people.

Fig.8. (a)secret image, (b)secret image histogram, (c)Rubik cube
encrypted secret image, (d)Rubik cube encrypted secret image
histogram
Fig. 9 shows the performance analysis of secret image size Vs PSNR. Size of secret image is increases the peak signal noise ratio is decrease. In this analysis different size of a secret image is used i.e. 64x64, 128x128, 256x256 to check the performance factor.

Fig. 10 shows the performance analysis of secret image size Vs MSE. Performance analysis of secret image size Vs MSE it shows in above fig. 10 to check the performance factor of the secret image. by seeing this figure, it shows the size of a secret image is increase, mean squared error is also increasing.
7 CONCLUSION

The steganography framework is joined with encryption of the secure secret image is done by using Rubik’s cube rule to keeping the data secure. A secret picture can be completely covered up within a cover picture by using the modified LSB method. In the event that some way or another secret picture is separated, it is difficult to unscramble (decrypt) secret picture because of properties of encryption system perplexity and dissemination, furthermore its substantial key space. This gives a high level of security as any hacker would need to check for all conceivable cube sizes and key sizes. and This process is depending on the Rubik’s cube rule to change the pixels of the picture. To confuse the relationship amongst unique and encoded pictures, to each row and segments of a picture the XOR operator is applied utilizing a key.
References


