National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 916-921
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

AN ADVANCED METHOD OF TWO-LEVEL ENCRYPTION IN HIDING IMAGE STEGANOGRAPHY

Manu Raj Moudgil

Professor, Computer science and Engineering Department, BGIET Sangrur

Rajneesh Talwar

Professor & Dean DICE, Chitkara University

Amanpreet Kaur

Assistant Professor, Computer science and Engineering Department, BGIET Sangrur

Amreen Kaur

Assistant Professor, Computer science and Engineering Department, BGIET Sangrur

ABSTRACT

The picture covering is achieve lively reputatation owed to its established function as an picture is extended supervising consist of helpful data. In view of this paper, we have particuraly considered the approach of steganography by incorporating picture covering inward addition picture among unharmed architecture digital indication plan. Our advanced attempt allow the basic picture preprocessing efforts through clarify of owner picture chase by enclose of the classified picture and declaration of the picture documents inward the owner picture. Next, the stego-picture is liable as an instruction to the digital indication plan. The encouraging develpmental by-product advise the future of the plan.

Keywords- Steganography, Digital Signal Framework, RGB color model

1. INTRODUCTION

Steganography word is created from Greek words Steganos (wrapped) and Graptos (autograph) which actually aids "binding autograph". Mostly steganography is admitted as "ideal" connection. Steganography aids to bury information continuation in one more mean (phonic, broadcast, picture, connection). Today's steganography organization applied interactive media body such as picture, phonic, broadcast as binding cable. It is divergent from absolute contented of information.

Steganography aids is not to change the framework of the classified information, on the other hand it protects innermost a binding-entity (bearer entity).

After covering mechanism binding-entity and stego-entity (conduct covered data entity) are identical. So, steganography (covered data) and cryptography (secure data) are exactly divergent from peculiar one more. Due to invisibility it is crucial to compensate data beyond admitted operation in steganography. Identify operation of steganography is admitted as Steganalysis.

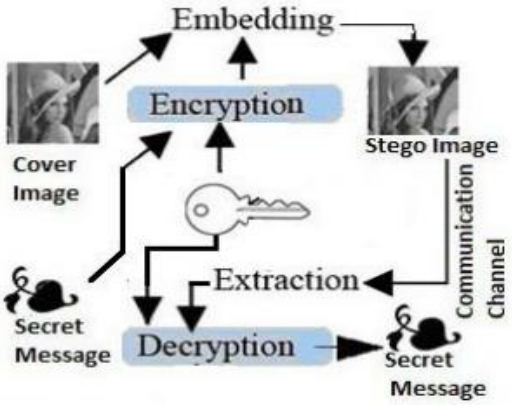


Fig.1.Generic Steganography process

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

A. Image Steganography

Just as declared previous, pictures are the largest famous binding entity applied for steganography. In the authority of digital pictures numerous divergent image folder dimensions happen, largest of them for definite operations. Since the above-mentioned divergent picture folder dimensions, divergent steganographic formula happen.

B. Image Definition

Through a computer, a picture is a cluster of characters that composed divergent luminous depth in divergent field. This fractional illustration figures a network and the particular bits are assigned as pixels. Largest pictures on the web expressed by the elliptical outline of the picture pixels defined as particles. These pixels are shown angular chain by chain. The character of particles in a hue blueprint, labeled as particle deepness. The least particle deepness in circulating hue blueprint is 8. Homogeneous and neutral proportion pictures apply 8 particles for individual pixel and are adapt to layout 256 divergent hue. Digital hue pictures are as usual saved in 24-picture folder and apply the RGB hue illustrative, additionally accepted as direct hue.

2. RELATED WORKS

In this, an enhanced LSB substitution procedure is considered by a facts masking formula. The factor of the stego-image can be deeply appreciate with ground besides formation crisis. In the examined process, the amount of footstep are very decreased. In this way, the process crisis is decreased. The ultimate activity will intention on developing the skill of the considered process[1]. Steganography is the different path used for acquiring facts by the web. In this paper, an basic achievement of image steganography in acquiring facts by a channel medium was knapsack finished by using several collection of input images as cover images and we identify that JPEG is not bind with our plan. This follows to the literatures considered that downcast the use of JPEG folder as cover images in image steganography[3].As steganography develop into larger broadly used in measuring, there are problems that are essential to be evaluated. There are a generous group of detailed way with their advantage and disfavor. This activity started a figure that can carry generous collection of hidden knowledge and implement acquire channel belted by two channel variation.The combination steganography and cryptography can be interlaced with this plan. In joining, the advised achievement is uncomplicated[4].

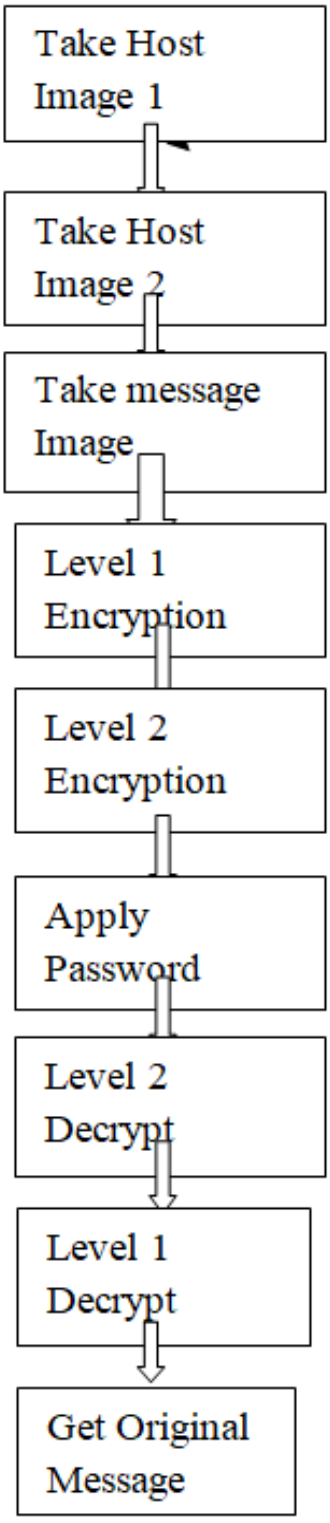
3. OBJECTIVES

The picture covering is achieve lively reputatation owed to its established function as an picture is extended supervising consist of helpgul data. In view of this paper, we have particuraly considered the approach of steganography by incorporating picture covering inward addition picture among unharmed architecture digital indication plan. Our advanced attempt allow the basic picture preprocessing efforts through clarify of owner picture chase by enclose of the classified picture and declaration of the picture documents inward the owner picture. Next, the stego-picture is liable as an instruction to the digital indication plan. The encouraging develpmental by-product advise the future of the plan. The sending of digital hue picture generally endure from document repetition which depend upon enormous cache capacity. In this concern, hue quantization can be borne away which estimates the authentic pixels of the classified picture with their adjoining definitive hue. In view of these approaches densely build upon the hue document posture that they confrontation and achieve the quantization. The aim of digital indication is very expressive as it cerify the correctness of the dealer additonally the sending of the appropriate document. The strength of the digital indication plan is generally approved for sending of classified data over troubled chain.

4. PLANNING OF WORK

Persuing are the modifications build upon manner for improved gurantee. The first level is SI-Stego-picture. The second level is CI 1-Cover picture 1.The third level is cover stego picture into cover picture 1 applying LSB approach which is altered by the creator.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in



Flowchart of Encrypted Image and decrypted image

The fourth level is assign the indication on the Cover picture 1 after deposit Stego picture into it. The fifth level is CI 2-Cover image 2.The sixth level is cover picture 1 will exploit as stego picture for cover picture 2. This is level 3 of gurantee. So alike if notable coduct to skilled the high proportionate of gurantee, the assailant clammed up to go addition 2 levels. The seventh level is at the moment the ultimate cover picture to transfer. The eighth level is at the teller boundary , we will acquire cover picture 2. The ninth level is assign the inverse

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

LSB on cover picture 2 to attain cover picture 1. The tenth level is assign the indication on cover picture 1 to attain cover picture with stego picture. The eleventh level is again assign inverse LSB on cover picture 1 to attain the stego picture.

We will analyze the advanced work with the work in base paper on the support of PSNR and MSE code.

5. RESULT AND DISCUSSION

In this, we have taken two images for steganography process. We have taken two host images. One is host 1 image, second is host 2 image and the another is message image. The message image hides the host 2 image then this process is known as first encryption.Then the host 2 image is taken into host 1 image. The overall process of host 2 image and msg image is declared as a box as considered as a first encryption and host 1 image is inculded in it then this overall process is known as final encryption. In the decryption process, we need a password. Th host 1 image is directed to the host 2 image. The host 2 image is directed to the message image.Then the comparison of the encryption and decryption process is continued.

Figure 2. shows host 1 image is taken for steganography process.

Figure 3. shows the host 2 image and message image.

For first level encryption the message image will be hide in host 2 image, that is called level 1 encryption.

Figure 4. shows for first level encryption the message image will be hide in host 2 image, that is called level 1 encryption.

Figure 5. shows host 2 stegano image will be hide in host 1 image, that is called level 2 encryption.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Figure 6. shows After the encryption part, receiver have to apply a password to decrypt the message image. After that the vice versa process will take place.

Figure 7. shows final message after second decryption.

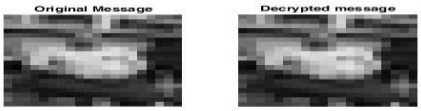


Figure 7. shows finally we will get the original message at the receiver end.

Figure 8. shows intermediate original image and intermediate decrypted image.

Value	PSNR	MSE	MAXERR	L2RAT
0	44.7858	42.4269	44.0014	40.7094

Table.1. shows the following values of PSNR, MSE, MAXERR, L2RAT are shown below of the final image.

6. CONCLUSION

In this paper allow about audit of different steganographic advent and classified of steganography which have been examined in the literature. We have detailed belief different examined way which demonstration that the recognized character of the image is condensed when closed information is develop upto compensated cutoff using LSB traditional structure.

7. REFERENCES

1. Vijay Kumar Sharma, V Shrivastava," A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by minimize Detection," Journal of Theoretical and Applied Information technology, 15th February 2012, Vol.36, No.1.
2. Mehdi Hussain and Mureed Hussain," A Survey of Image Steganographic Techniques," International Journal of Advanced Science and Technology, Vol.54, May, 2013.
3. E.P.Musa, S.Philip," Secret Communication Using Image Steganography," African Journal of Computing & ICT,Vol 8. No.3-September, 2015.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4. Shashikala Channalli, Ajay Jadhav," Steganography An Art of Hiding Data," Shashikala Channalli et al/ International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.
5. C.P.Sumanthi, T.Santanam and G.Umamaheswari," A Study of Various Steganographic Techniques Used for Information Hiding," International Journal of Computer Science and Engineering Survey(IJCSES) Vol.4, No.6, December 2013.
6. Babloo Saha and Shuchi Sharma," Streganographic Techniques of Data Hiding using Digital Images," Defence Science Journal, Vol.62, No.1, January 2012, pp. 11-18,DOI: 10.14429/dsj.62.1436.
7. Samir KumarBandyopadhyay, Indra Kanta Maitra," An Alternative Approach of Steganography using Reference Image," International Journal of Advancements in Technology, http://ijict.org/ , ISSN 0976-4860.
8. V.Mahalakshmi, S.Satheeshkumar, Dr.S.Sivakumar,"Performance of Steganographic Methods in Medical Imaging,"International Journal of Computational and Applied Mathematics. ISSN 1819-4966 Volume 12, Number 1 (2017).
9. Anil Kumar, Rohini Sharma," A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, july 2013, ISSN: 2277 128X.