International Journal of Advance Research in Engineering, Science & Technology(IJAREST), ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2, Issue 6, June- 2105, Impact Factor: 2.125

Dual Steganography Using LSB Method

Makwana Divya (CSE Department 2nd Year)

Shrikant Lade (CSE Department)

RKDF Institute of Science and Technology, Bhopal

itsdivyamakwana@gmail.com

Abstract- *Now a days we can communicate over the channel and the information is not secured. Hacker can easily hack the important information through internet. Most of information are available on the internet and we all are used it but in that risk is involved. The information will encrypt using cryptographic algorithms and the cipher text can see by a third -party adversary and by applying cryptanalysis the information can restore back. The large problem in employing cryptography is that, the cipher text is detectable to illegal user. We can avoid this by using Dual steganography. The proposed method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality. So, to overcome this type of problem we can use two times steganography.*

I. INRODUCTION

Steganography (pronounced STEHG-uh-NAH-gruhf-ee, from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Image steganography methods can be categorized into two parts. One is Spatial Domain and other is frequency Domain.

Two types of mechanisms are there to provide security for the information, they are cryptography and steganography [1]. Cryptography means converting the text from readable format to crabbed format. Steganography is used for concealing the information in an image [1]. The information is not visible.

There are three different types of steganographic techniques are available for concealing the information in an image, that is Least Significant Bit Insertion, Masking, and Transformation techniques [2].

Least Significant Bit (LSB) embedding is a simple system to implement steganography [4]. Agnate all steganographic methods, it stick the data into the cover so that it cannot be detected by a random observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to fix data into an image on any bit-plane, LSB bury is performed on the least significant bit(s). This shrinks the variation in colors that the employ creates.

Masking and Filtering is a steganography method which can be used on 24 bit per pixel images. The technique can be resort on both color and gray-scale images. Masking and filtering is akin to set watermarks on a printed image.

Transformation use mathematical functions to hide least bit co-efficient in the compression algorithm that reduces the file size of image.

II.LITRETURE REVIEW

This work is concerned with implementing Steganography for images, with an upbeat in both precaution and image quality. The one that is enforced here is a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality is amended by using bit-inversion technique. In this tactics, calm least significant bits of cover image are inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of mutated LSBs. Thus, beneath number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stego- image. By storing the bit patterns for

which LSBs are inverted, message image can be reaped correctly. To civilize the brawn of steganography, RC4 algorithm has been worn to enact the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This process randomly scatters the bits of the message in the cover image and thus, making it tough for illegal people to extract the original message [4].It was creating only single time security in steganography.

III.PROPOSED WORK

Encryption Technique:

The model of Dual Steganography uses a Cover Image (any image that can be used to hold secret information inside), the secret message (the private information that is to be sent secretly), a stego key that is worn to encode the secret message so that detection becomes difficult and a Steganography algorithm/technique (the procedure to hide secret message). The output of the process is the stego Image-1 that has the secret message hidden inside. The stego Image-1 and cover image will be applied on the stego algorithm. Then output of the process is the stego Image-2 that holds the secret message. This stego object is sent to the receiver where receiver will get the secret data out from the stego image by applying decoding algorithm/technique.

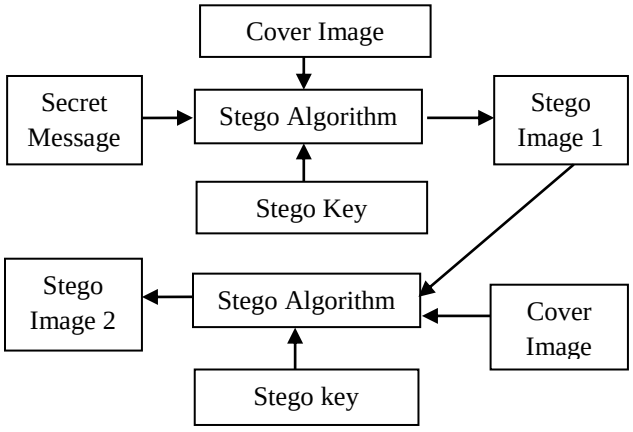

Figure 1. Dual Steganography at Sender Side

Decryption Technique

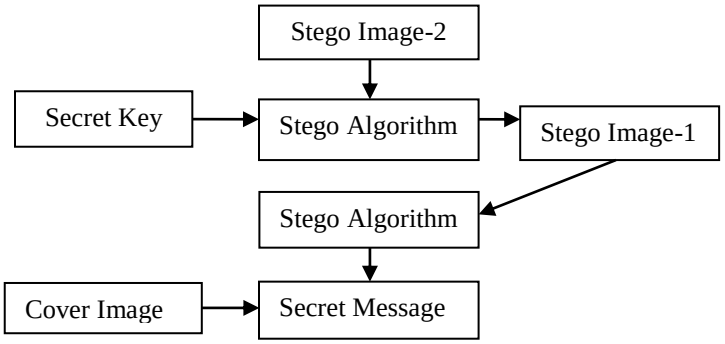

Figure 2. Dual Steganography at Receiver Side

Now in Decoding First we will take a Stego Image-2 and apply over stego algorithm and key from that we will get stego image 1 now we will take stego image-1 and apply stego algorithm so that we now get over Original secret message. Thus we conclude that it provides High Data Security and size of the secret message will be large.

IV.CONCLUSION

The Proposed method applies on security level because system cannot provide good security so we will try to solve that problem using two times encoding as well as decoding so we get high security on secret message and Third party never crack these message.

REFERENCES

[1] R Praveen Kumar,V Hemanth and M Shareef,"Securing Information Using Sterganoraphy" 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013].

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE Security and Privacy1 (3) pp. 32-44, 2003.

[3] R. C. Gonzalez and R. E. Woods, "Digital Image Proeessing", 2nd edition,P rentiee Hall, Inc, 2002.

[4] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan,"Enhancing the Security and Quality of LSB based Image Steganography" 2013 5 th International

Conference on Computational Intelligence and Communication Networks.

[5] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganography- survey and analysis of current methods. Signal Processing, 90, 727–752.

[6] R. C. Gonzalez and R. E. Woods, "Digital Image Proeessing", 2nd edition,P rentiee Hall, Inc, 2002.

[7] P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images", in Proe. ICCCNT, 2010, p p. 1-6.

[8] S. Song,J . Zhang, X. Liao,J . Du and Q. Wen, "A Novel Sec ure Communication Protocol Combining Steganography and Cryptography", Elsevier Ine, Advaneed in Control Engineering and Information Seienee,V ol. 15,p p. 2767 - 2772,2011.