International Journal of Advance Research in Engineering, Science & Technology(IJAREST), ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2,Issue 8, August- 2015, Impact Factor: 2.125

Dual Steganography Implementation Using LSB Technique

[(1)]Divya Makwana (CSE Department)

[(2)] Shrikant Lade (CSE Department)

RKDF Institute of Science and Technology, Bhopal

Abstract: - *Now a day's hiding the message is normal thing but this implementation provides two times security on image so it is called as "Dual Stegnography". Stegnography means message is remain unseen using various methods and techniques so we are used lsb technique. In previous implemented paper they can only hide the message so its must necessary to provides more security using lsb insertion techniques. Single time stegnography gives good enhancement to lsb technique in consideration of both security and image quality. Now its time to change the requirement so dual Steganography is needed.*

Keywords*:* Stegnography,4-bit LSB,Image Processing, Security Encoding.

Introduction: - Steganography is the practice of hiding secret messages (invisible text) within every day, seemingly innocuous object (cover text) to produce a stego text[2]. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text [3]. The target of steganography is to grant parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation [2]. This sets steganography apart from cryptography which, although providing for private communication, can spark disturb based solely on the fact that it is being used.

Steganography is data invisible within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing[5]. Image Steganography methods can be categorized into two groups: spatial domain and frequency domain. In the first case, the secret message is embedded directly in the pixels, while in the second case, first images are converted to frequency domain and then, the secret message is embedded in the transform coefficients[5].

In this paper the original image without the embedded secret data is named cover image, while the image resulting from embedding is named stego image.

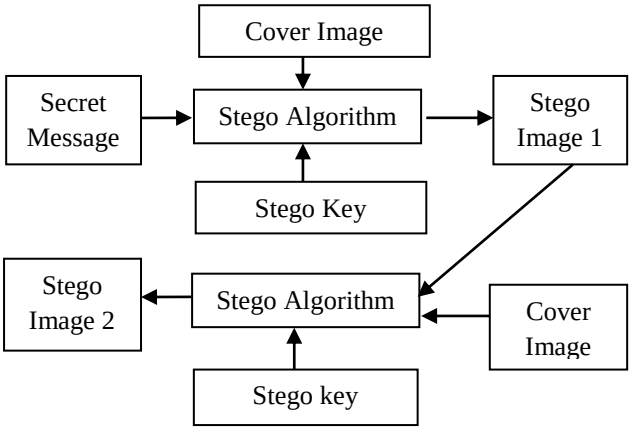
Implementation

In Steganography , The basic concept is that it has a cover object that is used to cover the original message image, a host object that is the message or main image which is to be transmitted, a stego-key which is used to hide the message image into cover image, and the steganography algorithm to bring out the required object. The output is an image called stego-image which has the message image inside it, hidden[5]. This stego image is then directed to the receiver where the receiver retrieves the message image by applying the de-steganography[5].

Encryption Process:-

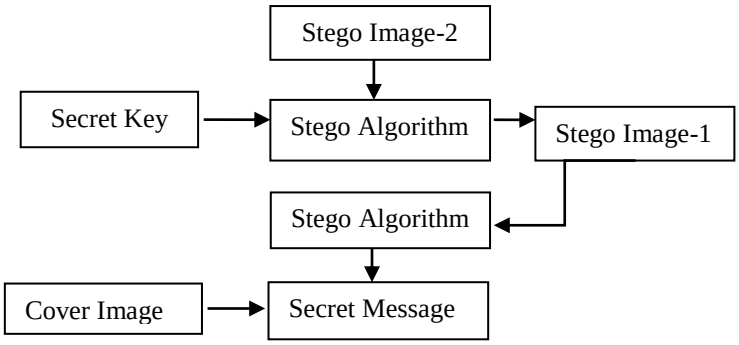
In dual steganograpgy the secret information and cover image is taken and then apply stego algorithm [1]. The secret message or information can be converted into 8 bit binary value. And do operation on it using AND and OR gate. By using AND gate, we are encrypt the 8-bit binary value. Now these bits are ready to embed into an image using LSB insertion. By using AND gate, we are encoding the 8-bit binary value. Now these bits are ready to embedded into an image using LSB insertion. Finally generated output of it is Stego image-1. This process is done two types so the

information is secured and storage capacity of it is increased [1].



Decryption Process:-

In de-steganography process the 4 bit LSB data (Stego Image-2) and the secret information or message is added to the algorithm is called as stego algorithm. This Stego algorithm creates another 4 bit LSB Data in RGB form is stego image-1. Stego Image-1 and cover image is added to second time in stego algorithm so we get our original message [1].



Now in Dual Steganography encoding side take a first cover image as input and then separate the RGB color (Red, Green and Blue). Separate the cover image into 8 bit of RGB color. When 8 bit RGB color are separated then apply AND and OR operation on it and make 4 bit LSB is called as stego image-1.

Take a secret message convert it in Binary form and store that message into 4 bit LSB or in RGB. Take a Secret key and stored it in matrix B.

Take a second cover image store the stego image in second cover image and finally the output is produced as stego image- 2.

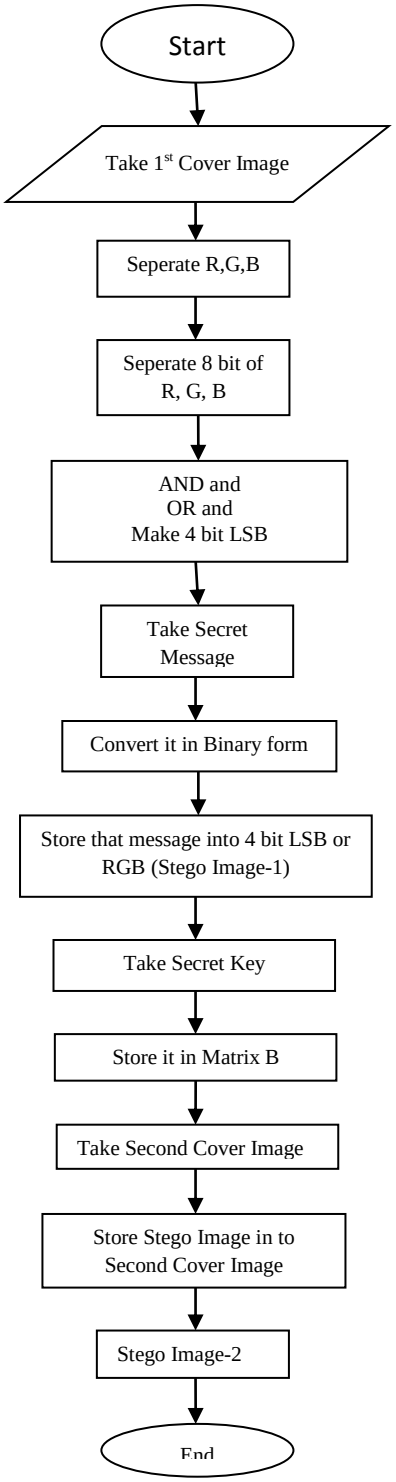


Fig.1 Encoding Side

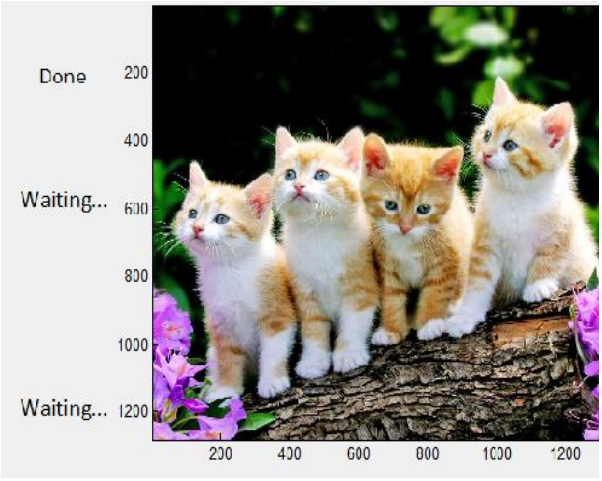
And Decoding side is reverse procedure of it.

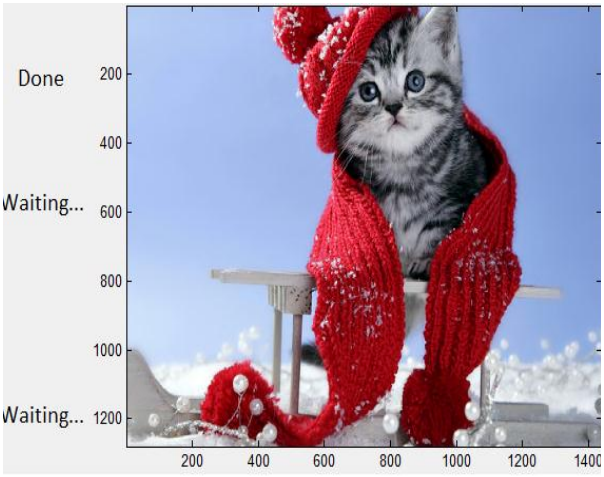
A good technique of image steganography aims at three aspects. First one is capacity (the maximum data that can be stored inside cover image). Second one is the imperceptibility (the visual quality of stego-image after data hiding) and the last is robustness.

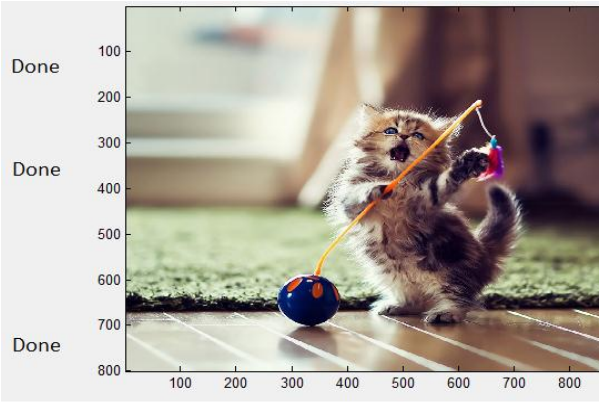
EXPERIMENTAL RESULT

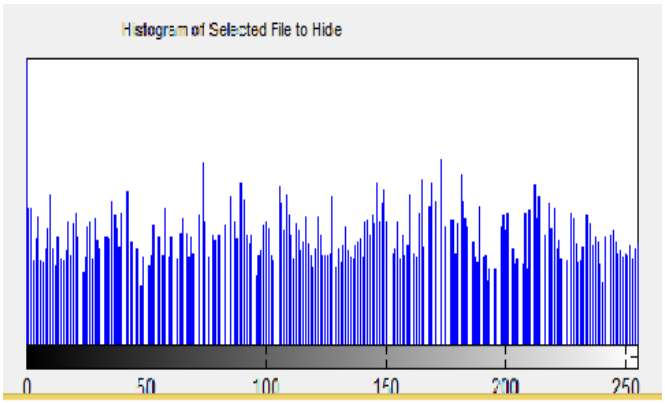
In this paper for implementation of dual Steganography we use the matlab software. After implementation of two types encoding and decoding we gets security over the information.

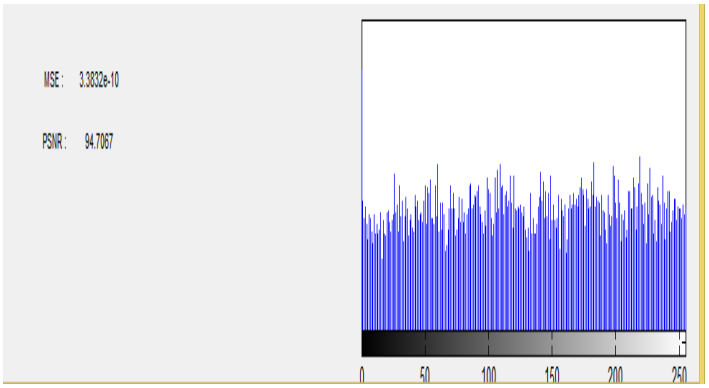
Below the figure represent the output of implementation.











CONCLUSION

In Proposed work of dual Steganography we can easily improve the quality of image after applying LSB insertion technique. 4 bit LSB are the stego image which is not easily hacked by unauthorized person. Storage capacity is also increased and image resolution is decreased.

The proposed bit inversion method enhances the stego-image quality. The enhancement in PSNR is not surrounded.

The improvement in PSNR may be very large for any image. For given a infomation image, a set of cover image can be treated and that cover image is selected for which the improvement is largest. The bit inversion method and use of random locations together makes the steganography better by improving its security, image quality and robustness.

REFERENCES

[1] Makwana Divya, Shrikant Lade "Dual Steganography Using LSB Method", (IJAREST), ISSN (O):2393-9877, ISSN (P): 2394-2444, Volume 2, Issue 6, June- 2105, Impact Factor: 2.125.

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

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

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

[5] 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.

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

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

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

[9] 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.