# STEGANOGRAPHY SYSTEM USING SUCCESSIVE LOGICAL AND OPERATION OF LAST FOUR BITS

Shivani Yadav[1], Deepak Goyal[2]

*[1]M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
*[2]Associate Prof., Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[1] shivaniyadav17@gmail.com
[2] deepakgoyal.vce@gmail.com

***Abstract-*** **Steganography is a technique of hiding information in some cover media i.e. image, text, audio, video . The main purpose of steganography is to conceal the existence of the message while communicating. In this paper, a new Steganography technique is presented, implemented and analyzed. The proposed method uses the 5th, 6th, 7th & 8th bit of pixel value of cover image. The main idea is to apply successive Logical AND operation on last four bits of pixel value.**

***Keyword:*** **Steganography**

## I. INTRODUCTION

Steganography is a technique to hide the message in digital objects such as image, video, music, or any other computer file. This idea was first described by Simmons in 1983. More comprehension theory of steganography is given by Anderson [1]. Steganography is hiding secret information within a medium in an invisible manner. It is one such pro-security innovation in which secret data is embedded in a cover [2]. Steganography and cryptography are closely related. Cryptography is about protecting the content of messages while steganography is about concealing their very existence [3].

Steganography means Cover medium + Secret message + Stego key. The general model of data hiding can be described as follows. The embedded data is the message that one wishes to send secretly. The message is hidden in a cover-text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the hidden data to parties who know it [4].

The objective of steganography is to hide the information into the cover image such that the existence of payload in the cover image is invisible to the human beings [5]. In case, if the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered [6]. According to Johnson & Jagodia [1], “Steganography’s main purpose in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection.”

Watermarking and Fingerprinting are two different applications of steganography used for different purposes as atermarking allows a person to provide hidden copyright notices or software piracy and fingerprinting uses each copy of the content and make it as unique to the receiver [7]. Digital watermarking is the special case of information hiding and Febriano, Italy is considered as its birth place [8]. Tirkel et al [9] introduced the world “water marks” which became “watermarks” later on, digital water marking is the process of embedding information into digital media content such that the information (the watermarks) can later be extracted or detected for a variety of perposts including copy prevention and control. Digital watermarking is becoming an important area of research and development. It helps in addressing some of the challenges faced by the rapid explosion of digital content. Water marking is emerging as an efficient method for protecting digital elements such as image, video and sound [8], [9], [10]. Finger printing technique was introduced to prevent the piracy of digital objects or we can say, illegal copying of digital objects such as software, multimedia objects. In this technique, a fingerprint (a distinct mark) is inserted in each digital object, which is some way related to buyer. In future, if an unauthorized copy of digital object is found then its origin can be recovered by retrieving the unique fingerprinting contained in it. The fingerprint is embedded into digital a object which makes it difficult for buyers to make any changes in it. This technique has emerged with some problems which were firstly introduced by Wagner [11] and still the work is going on for making it best technique.

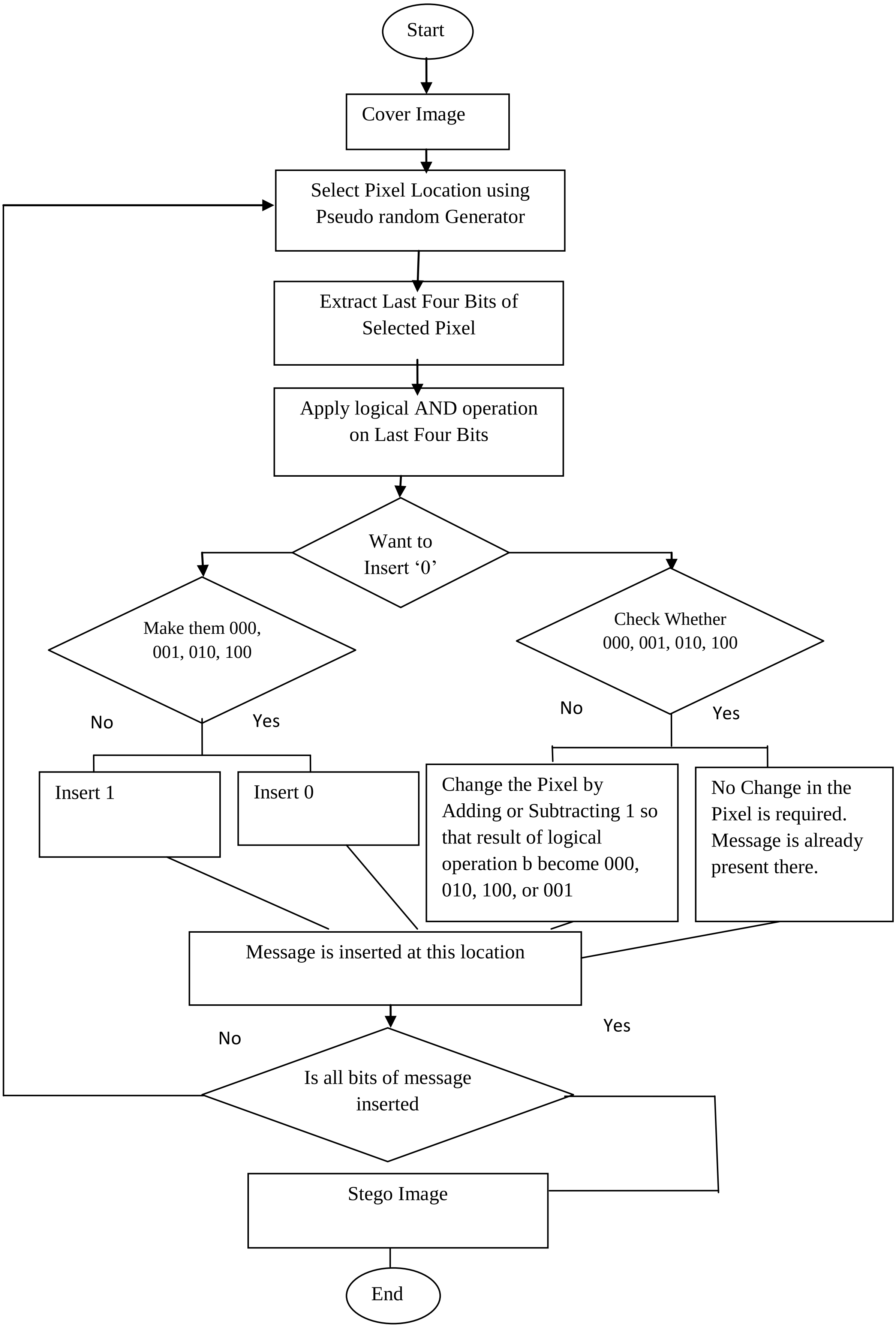
## II. PROPOSED WORK

A new Image Steganography method based on the spatial domain is proposed. It uses the last four bits to embed the message. It uses the bit 5th, 6th, 7th & 8th bit of pixel value of cover image. The main idea is to apply successive Logical AND operation on last four bits of pixel value. After applying the Logical AND operation on last four bits the result of

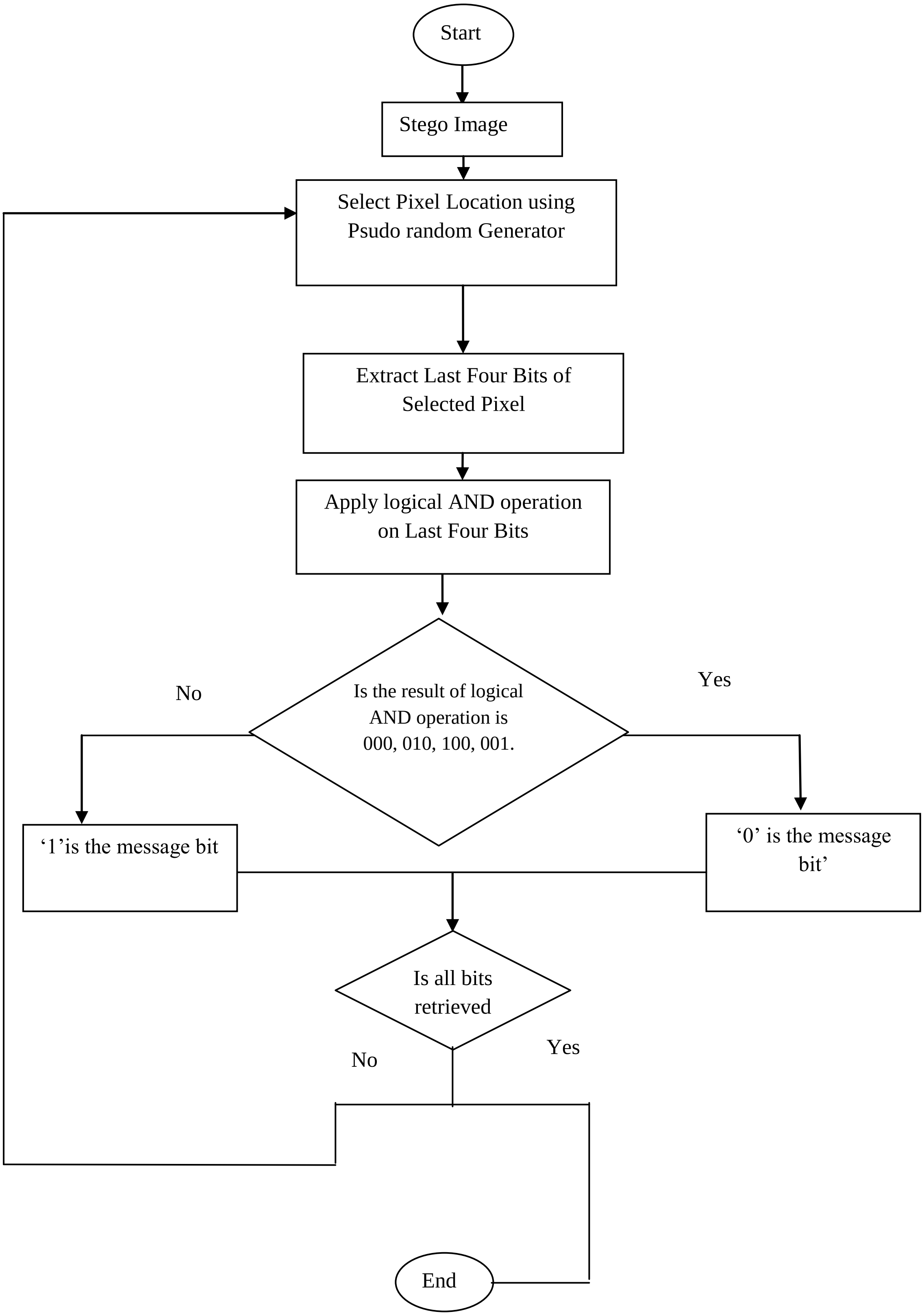
Logical AND operation is checked. If we want to insert 0 at the pixel value then check whether the result of Logical operation is 000,010,100 or 110. If the specified combination comes as result of Logical AND operation then it is Ok. Message bit is present over there otherwise make change of +1/-1 to the pixel value such that result of successive Logical operation becomes 000,010,100 or 110. If we want to insert 1 at the pixel value then check whether the result of Logical operation is 001,011,101 or 111. If the specified combination comes as result of Logical AND operation then it is Ok. Message bit is present over there otherwise make change of +1/-1 to the pixel value such that result of successive Logical operation becomes 001,011,101 or 111. Our method is imperceptible to HVS because it provides minimum degradation in image quality due to only +1 or -1 change at a pixel value. Our method also provides 99.21% chances of message insertion at a pixel value which is near about optimal solution. This method has been compared with other methods in spatial domain by using various image steganography parameters.

In this method, the pixel value of cover image has been changed in accordance with the message. The message has been masked in such a way that changes in the cover image and stego image remains imperceptible to Human Visual System (HVS).

Insertion of message


Start
Cover Image
Select Pixel Location using Pseudo random Generator
Extract Last Four Bits of Selected Pixel
Apply logical AND operation on Last Four Bits
Want to Insert '0'
Make them 000, 001, 010, 100
Check Whether 000, 001, 010, 100
No
Yes
No
Yes
Insert 1
Insert 0
Change the Pixel by Adding or Subtracting 1 so that result of logical operation b become 000, 010, 100, or 001
No Change in the Pixel is required. Message is already present there.
Message is inserted at this location
No
Yes
Is all bits of message inserted
Stego Image
End

Retrieval of message


Start
Stego Image
Select Pixel Location using Psudo random Generator
Extract Last Four Bits of Selected Pixel
Apply logical AND operation on Last Four Bits
Is the result of logical AND operation is 000, 010, 100, 001.
No
Yes
'1'is the message bit
'0' is the message bit'
Is all bits retrieved
No
Yes
End

## III. HYPOTHESIS AND ASSERTIONS

1. Sender and Recipient should agree on the one cover object in which message is supposed to be hidden.
2. Sender and Recipient should agree on the same secret key to decide the pseudo-random location in the cover object.

Insertion Algorithm:-

```
i)    Find the pseudo-random location (l) in cover object using secret key for insertion of message bit.
ii)   Apply logical AND operation on the last four bits of the pixel value on successive bits. (i.e. Apply Logical AND operation on 5th & 6th Bit, 6th & 7th Bit, 7th & 8th Bit).
iii)  Check the result of logical AND operation.
iv)   For Insertion of 0,
        Check if the result is 000,001,010,100 then it is Ok.
        Else
        Add or subtract 1 to the pixel so that result of Logical AND operation on last four bits become 000,001,010,100.
v)    For Insertion of 1
        Check if result is 011,101,110,111 then it is Ok.
        Else
        Add or subtract 1 to the pixel so that result of Logical AND operation on last four bits become 011,101,110,111.
vi)   End
```

Retrieval Algorithm:-

```
1)  Find the pseudo-random location (l)of stego image using the same secret key as used for insertion of message.
2)  Apply logical AND operation on the last four bits of the pixel value on successive bits. (i.e. Apply Logical AND operation on 5th & 6th Bit, 6th & 7th Bit, 7th & 8th Bit).
3)  Check the result of logical AND operation.
4)  If the result is 000,001,010,100 then 0 is the message bit else 1 is the message bit.
5)  End
```

Comparison Table of Proposed Method with Other Existing Investigated Methods

| Method | Message bit Insertion at pseudo random location at first chance | No change in pixel value when message bit is inserted |
|---|---|---|
| 6th & 7th bit | 50% | 50% |
| 6th, 7th & 8th bit | 85.93% | 43.18% |
| Proposed Method | 99.21% | 50% |

## IV. EXPERIMENTAL RESULT

PSNR (in dB) comparison with other identified methods

| Method | Image1 | Image 2 | Image 3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Proposed Method | 45.2 | 38.4 | 39.8 | 41.2 | 41.5 |
| LSB Method | 32.1 | 33.4 | 32.7 | 31.7 | 31.8 |

| | | | | | |
|---|---|---|---|---|---|
| 6th & 7th bit Method | 32.8 | 31.2 | 33.8 | 31.5 | 31.9 |
| GLM Method | 33.4 | 35.3 | 36.1 | 34.4 | 34.2 |
| Parity Checker Method | 30.3 | 28.4 | 29.0 | 29.4 | 30.1 |

The larger the value of PSNR, the better will be the technique. From above table, it has been concluded that this method provide better PSNR values than other methods. For all the five pictures, proposed method provides larger PSNR values than some existing investigated methods. The results show that our method is better than some existing investigated methods.

## V. CONCLUSION

In this paper, one new method of digital image steganography in spatial domain has been proposed. The proposed method is Steganography System using successive Logical AND operation of last four bits. In this method, 5th, 6th, 7th and 8th bit of pixel value is used for insertion and retrieval of message. The Logical AND operation is applied successively on last four bits of pixel for insertion and retrieval of the message. Subjective Test applied on this method also shows that this method did not generate any indication of correct identification of the original image.

## REFERENCES

[1]. N.F.Johnson and S.Jagodia, “Exploring Steganography: Seeing the Unseen”, IEEE Computer, Vol. 31, no 2, pp. 26-34, Feb. 1998.

[2]. S.Katzenbeisser and F.A.P.Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[3]. S. Katzenbeiser and F.A.P.Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security Series, Boston, London, 1999.

[4]. F.A.P.Petitcolas, R. J.Anderson and M.G.Kuhn, “Information Hiding – A Survey”, in *Proc. Of IEEE,* Special Issue on Protection of Multimedia Content, pp.1062-1078, 1999.

[5]. K.S.Babu, K.B.Raja, K.K.Kumar, T.H.M.Devi, K.R.Venugopal, and L.M.Patnaik, “Authentication of Secret Information in Image Steganography”, TENCON 2008 - 2008 IEEE Region 10 Conference, pp 1-6.

[6]. P.Goel, “Data Hiding in Digital Images: A Steganographic Paradigm” M.Tech thesis

[7]. R.Poornima and R.J.Iswarya ,” An Overview Of Digital Image Steganography”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, pp. 23-31, February 2013.

[8]. T.Y.Nakamura, and K. Matsui, “Embedding secret information into a dithered multilevel image”, in *Proc. Of IEEE Military Communication Conference*, pp. 216-220, 1990.

[9]. K.Tanaka, Y.Nakamura, and K.M. Members, Embedding the attribute information into a dithered image, Syst. Comput. Japan, Vol. 21, no. 7, pp. 43-50, 1990.

[10]. A. Tirkel, G. Rankin, R. Van Schyndel, W. Ho, N. Mee, and C. Osborne, “Electronic water mark”, in *Proc. DICTA*, pp. 666-672, Dec. 1993.

[11]. N.R. Wagner, “ Fingerprinting”, *Proc. Of the Symposium on Security and Privacy, IEEE Comp. Society*, pp. 18-22, 1983.