JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Securing GPS and GIS data using Steganography

**Rajkumar Yadav**
Assistant Professor
Department of Computer Science & Engineering, UIET
Maharshi Dayanand University, Rohtak, India

**Abstract:**

Today's era of technology there is need of fast communication. Everyone wants concrete, valuable and precious information in very less time. GIS and GPS are such kind of systems which provides valuable information in very less time for various types of applications like whether forecasting , agriculture etc. . GIS and GPS take data from various sources and after processing that data they provide valuable information which can be used in various applications. If the data is altered by some intruder then the user will get wrong information and no information about anything is always better than wrong information. So, there is demanding need to secure the data on which GIS and GPS systems will work. In this paper, we showed that how we can secure the data for these systems using steganography.

Keywords: GIS, GPS, Steganography etc.

## 1.Introduction:

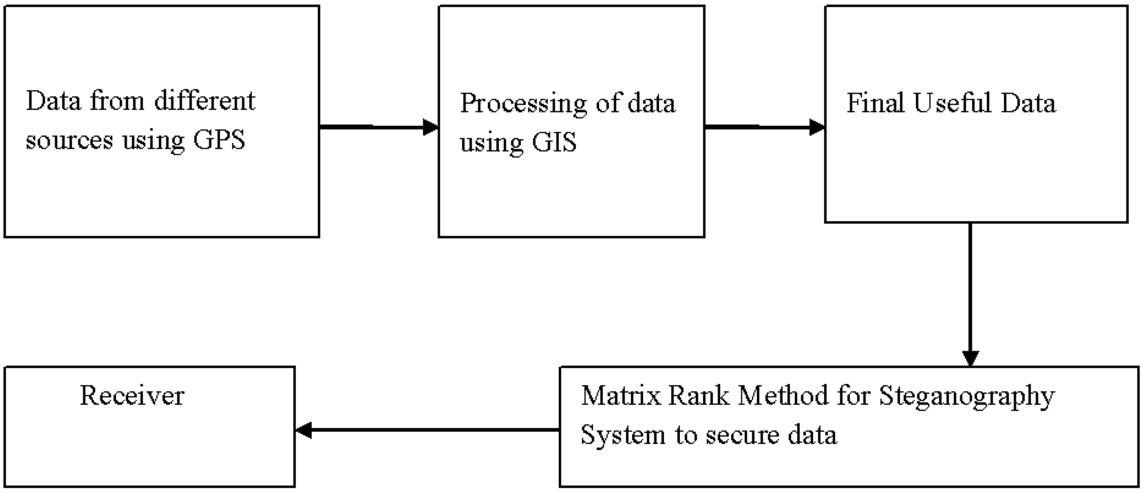
Making decisions based on geography is basic to human thinking. Where shall we go, what will it be like, and what shall we do when we get there are applied to the simple event of going to the store or to the major event of launching a bathysphere into the ocean's depths. By understanding geography and people's relationship to location, we can make informed decisions about the way we live on our planet. A geographic information system (GIS) is a technological tool for comprehending geography and making intelligent decisions. GIS organizes geographic data so that a person reading a map can select data necessary for a specific project or task. A thematic map has a table of contents that allows the reader to add layers of information to a basemap of real-world locations. For example, a social analyst might use the basemap of Eugene, Oregon, and select datasets from the U.S. Census Bureau to add data layers to a map that shows residents' education levels, ages, and employment status. With an ability to combine a variety of datasets in an infinite number of ways, GIS is a useful tool for nearly every field of knowledge from archaeology to zoology.

The Global Positioning System (GPS) is a navigation and precise-positioning tool. Developed by the Department of Defense in 1973, GPS was originally designed to locations world-wide. Today, the uses of GPS have extended to include both the commercial and scientific worlds. Commercially, GPS is used as a navigation and positioning tool in airplanes, boats, cars, and for almost all outdoor recreational activities such as hiking, fishing, and kayaking. In the scientific community, GPS plays an important role in the earth sciences. Meteorologists use it for weather forecasting and global climate studies; and geologists can use it as a highly accurate method of surveying and in earthquake studies to measure tectonic motions during and in between earthquakes.

Steganography is an art and science of hiding information by embedding messages within other, which are seemingly harmless messages [1]. Steganography is derived from Greek where “steganos” means covered and “graphie” means writing. It means covered or hidden writing. The advantage of steganography is that the message in which sensitive data is hidden does not attract attention to interceptors. This process needs the cover image and secret image. The cover image hides the data of the secret image. In this paper we combine the features of above three techniques.

## 2.Proposed Work

In this paper we will show how to secure the GIS and GPS data using steganography. The security system is shown by the following figure.


Data from different sources using GPS
Processing of data using GIS
Final Useful Data
Matrix Rank Method for Steganography System to secure data
Receiver

In the above figure, it has been shown that the initial data has been come from different sources. GPS and GIS provide the precious data which is sent to the receiver. This data can be made secure by using Steganography so that intruder cannot read or alter the precious information.

In the above proposed steganography method, we used the concept of rank of matrix for insertion and Retrieval of the message. Firstly, select the random pixel on which we want to hide the information bit. Now make the matrix for the selected pixel as shown by eq. (1):

$$\text{Designed Matrix} = \begin{matrix} b_0 & b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 & b_7 \end{matrix} \quad \text{------------------------------------------} \; (1)$$

Now, calculate the rank of the Designed Matrix denoted by R(D.M.). The maximum value of R(D.M.) will be 4 because the no. of columns in the Designed Matrix is 4, which is larger than the number of rows in the Desired Matrix. $b_0$ is the least significant bit and $b_7$ is the most significant bit. If we want to insert 0 at a pixel position then check whether the rank of the matrix is odd. If the rank of the matrix is odd then no change in pixel value is required otherwise change some pixel bits optimally such that rank of the matrix will become odd. Similarly, if we want to insert 1 at a pixel position then check whether the rank of the matrix is even. If the rank of the matrix is even, then no change in pixel value is required otherwise change some pixel bits optimally such that the rank of the matrix will become even. The insertion of 0 is shown by figure 1 and the insertion of 1 is shown by figure 2. The retrieval process is shown by figure 3.

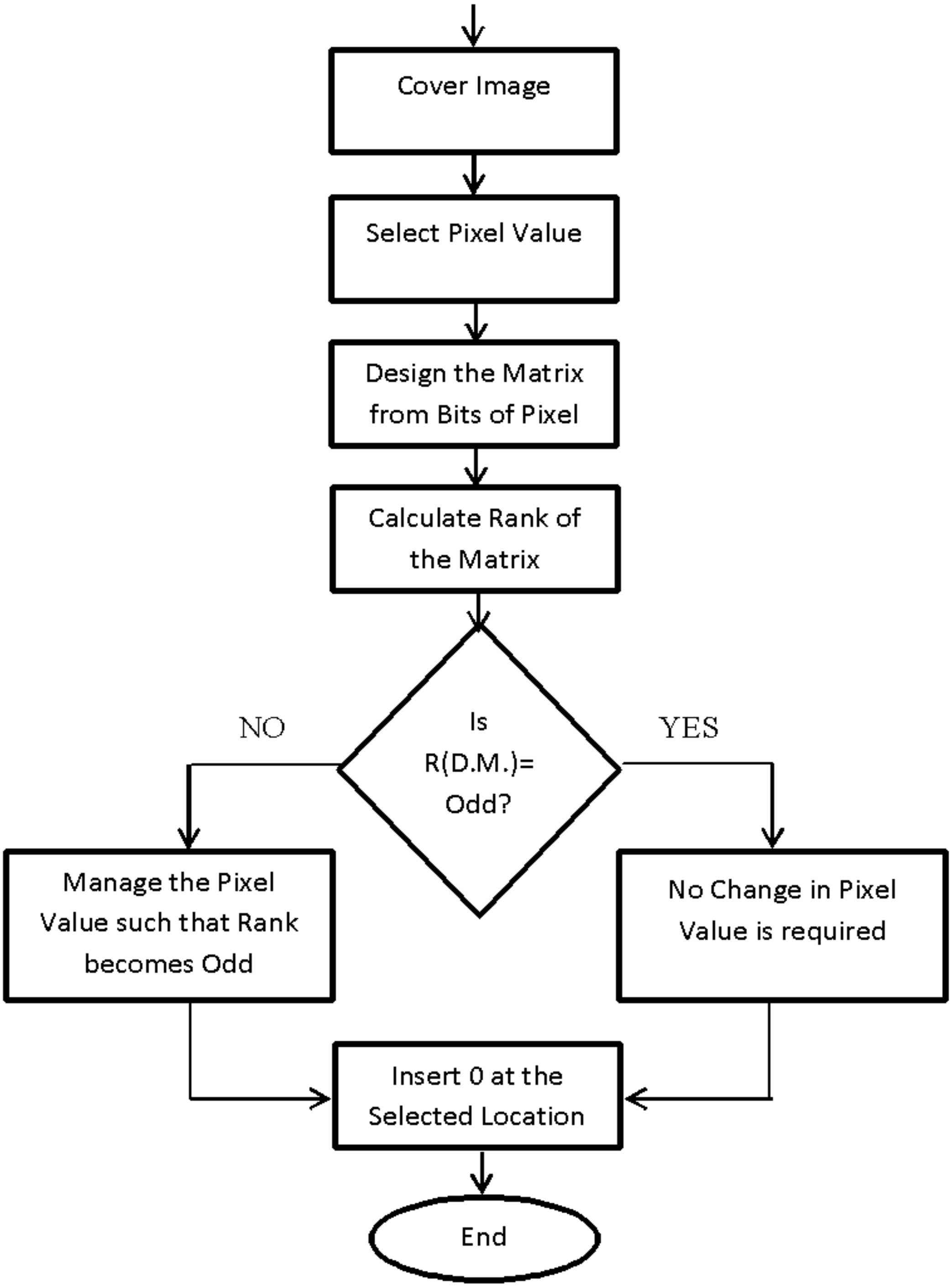

Cover Image
Select Pixel Value
Design the Matrix from Bits of Pixel
Calculate Rank of the Matrix
Is R(D.M.)= Odd?
NO
YES
Manage the Pixel Value such that Rank becomes Odd
No Change in Pixel Value is required
Insert 0 at the Selected Location
End

Figure 1

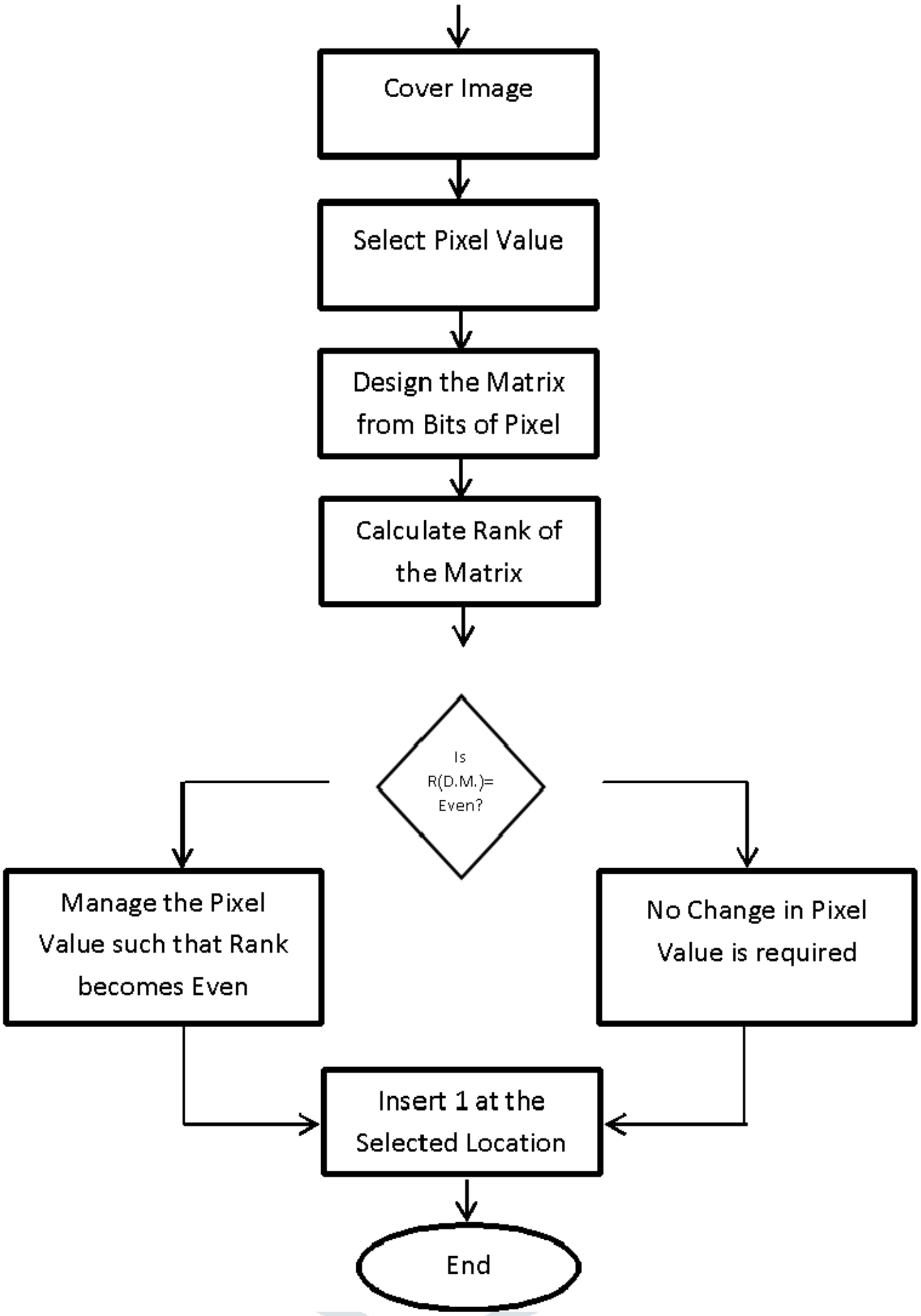

Cover Image
Select Pixel Value
Design the Matrix from Bits of Pixel
Calculate Rank of the Matrix
Is R(D.M.)= Even?
Manage the Pixel Value such that Rank becomes Even
No Change in Pixel Value is required
Insert 1 at the Selected Location
End

Figure. 2

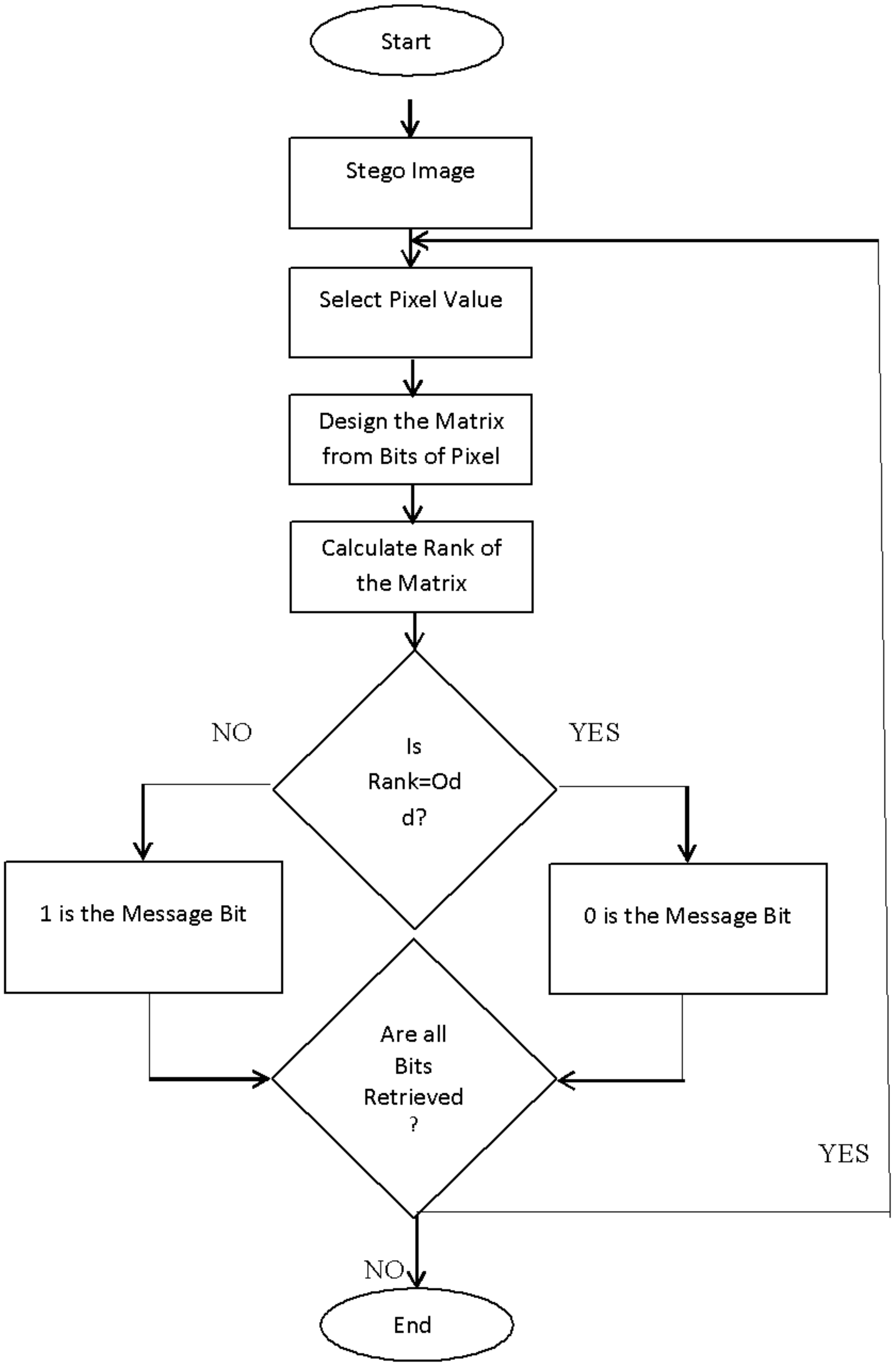


Figure 3

## a) Insertion Algorithm

i. Select the pixel by using some shared key.
ii. Extract the bits of the pixel.
iii. Design the matrix from the bits of pixel as given by eq.(1).
iv. Calculate Rank of the Designed Matrix.
v. If want to insert 0 then go to the next step, else go to step (vii).

vi.If rank of the designed matrix is odd then go to END, else change bits of the pixel such that rank becomes odd and go to END.

vii.If rank of the Designed Matrix is even then go to END, else change the bits of the pixel such that rank becomes even and go to END.

viii.END.

### b) Retrieval Algorithm

i.Select the pixel by using the shared key.

ii.Extract the bits of the selected pixel.

iii.Design the matrix from the bits of the selected pixel.

iv.Calculate Rank of the Designed Matrix.

v.If the rank is odd then 0 is the Message bit else 1 is the Message bit.

vi.END.

## Conclusion

So, by using the steganography we can secure the GIS and GPS data which are very useful for collecting the information.

## 3. REFERENCES

1. R Sridevi, DR. A Damodaram, DR. Svlnarasimham,” Efficient method of audio steganography by Modified LSB algorithm and strong encryption Key with enhanced Security”, Journal of Theoretical and Applied Information Technology,(2005)

2. Neil F Johnson, Sushil Jajodia, “Exploring Stenography: Seeing the Unseen”, IEEE Computer, Feb 1998, pp 26-34.

3. D.C. Wu and W.H. Tsai. “A steganographic method for images by pixel-value differencing”. Pattern Recognition Letters, 24: 1613-1626, 2003

4. Vidyasagar M. Potdar, Elizabeth Chang, “Grey Level Modification Stegnography for Secret Communication”, 2nd IEEE International Conference on Industrial Informatics INDIN 2004 June 24th, 26th June, Berlin, Germany, Submitted Tuesday, May 25, 2004.

5.Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, “A new Steganography Method for Gray Level Images using Parity Checker”, International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.

6.Khan, D.(1967), “The code breakers”, Macmillan.

7.Lee Y.K.,Chen L.H., “A Secure Robust Image Steganography Model”, 10th National Conference on Information Security, Hualien, Taiwan, pp 275-284, May 2000.

8.Bender, W., Gruhi, W., and N. Morimota, A., “Techniques for Data Hiding”, IBM Systems Journal, Vol. 35, No. 3 & 4, 1996

9.Anderson, R.J. “streching the limit of stegnography”, 1st information hiding workshop, Springer Lecture Notes in Computer science,Vol.1174,pp.39-48,1996