Current Trends in Technology and Science
ISSN : 2279-0535
8thSASTech 2014 Symposium on Advances in Science & Technology-Commission-IV Mashhad, Iran

Steganography of Metadata in Satellite Images Using Insignificant Bits

Mohammad Reza Mobasheri
Associate Prof., Remote Sensing Engineering Dept., KNToosi University of Technology, mobasheri@kntu.ac.ir

Moslem JafariKouranTurkish
MSc. Student,Khavaran Institute of Higher-education (KHI), morsal_jafari@yahoo.com

***Abstract* — Due to the recent development in remote sensing technology and the increase in the application as well as the resolution of satellite images, the data volume and the space they occupy have increased considerably. Moreover, auxiliary data and metadata, which are used in geo-referencing satellite images, atmospheric and radiometric corrections, need to be accompanied with the to satellite images. Besides, in order to prevent illegal access and to reserve copyright, the data should be encrypted to increase their security. In this article, a technique is proposed to conceal auxiliary data and metadata and to increase the data security by use of low bit values. By means of this technique, the insertion error rate is reduced while some security layers are added. Using statistical parameters such as abundance and dispersion curves the results were assessed. Accordingly, it is found that the changes caused by the insertion of information in low bit values, in comparison to atmospheric and other noises, as far as PSNR is larger than 40db will be negligible.**

***Keyword* — Steganography, Security, Volume Reduction, Satellite Images, Remote Sensing.**

Nomenclature
DN (Digital Number).
PSNR(Peak Signal-to-Noise Ratio)

1. Introduction

Steganography is the art of concealing secret data in ordinary data to prevent illegal access by a third party. In fact, steganography aims at hiding secret data from hackers and digital spies, leading to a safe channel for transferring data [1] [6] [7].

Auxiliary data and metadata are data which are used in geo-referencing of satellite images, radiometric and atmospheric corrections. These data are normally sent to the target station individually or as the header of satellite images. Both methods lead to the occupation of the bandwidth and the reduction of data security coefficient [2].

The simplest method of insertion is the increase of the data or image volume. Generally in this method, the inserted data are saved separately from the image data, increasing the image volume [3]. Another method of insertion is saving as metadata in the header of the image. These information, which are generally called EXIF or expanded information file, includes data related to image properties like the camera brand, the type of lens, the name of the photographer, the date and so on [4].

Both methods are defective. First of all, in both methods, the insertion of information which changes the size of the image file is easily identifiable because the actual file size can simply be determined. Secondly, they are vulnerable to any kind of undesired change.

This article aims at showing a way to provide more space for the insertion of the data in the covered medium, with the slightest change, and to increase the security of the hidden messages as well as to reduce the data volume. In case the insertion error rate is higher than the threshold limit, the insertion is not done or is done in fewer bits. The method of the insertion of data has a specific code which can be submitted to the end users.

2. Methodology

To carry out the steganography, the following steps are followed:

2.1 Converting Metadata into Binary Format

Metadata are data in the form of English texts, numbers or signs. In order to insert information in the covering medium, data have to be converted into binary or ASCII code, and to enhance security, more security layers are added to the information bit string by encoding and compressing the data.

2.2 Compressing and Adding Security Layers

In steganography of information in digital images by allocating more space to the insertion of information in the least significant bits will result in poor quality of the covering medium. Therefore, one should offer techniques that in addition to enhancing data insertion capacity, leave less effect or noise in the covering medium. So a technique is offered which in addition to lossless compressing, can encode data, adding a new security layer in a way that if an adversary has access to the inserted data in the image, he/she will not be able to decode the secret data easily. These steps are figuratively represented in figure (1).

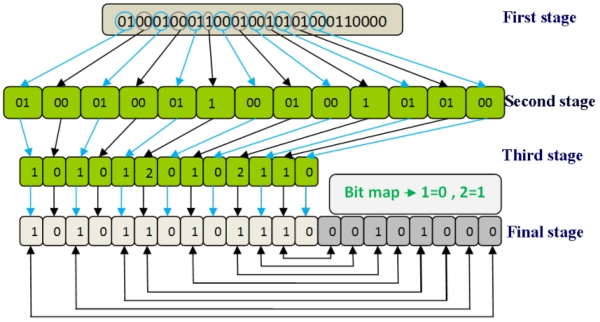

Figure (1): compressing and adding a security layer to the information

In the first step, metadata are converted into binary format. In the second step, these bit strings are grouped in two bitsets, provided that no two bits start with bit with value 1. Therefore, 00 and 01 are acceptable. In other cases, single bitsets are formed with value 1. In the third step, equivalent quantities are assumed for two bit and single bitsets, replacing two bit 00 with 0, two bit 1 with 1 and 1 with 2. In the final step, to avoid confusing 1s and 2s, a bitmap as great as the number of 1s and 2s is added to the end of the data bit strings figure (1). By this technique, in addition to compressing the information, a good security layer can be added to secret data so that if an adversary has access to the steganographized information, he/she will not be able to access to the main information easily. Figure (1) shows that the length of data has reduced from 24 to 21 bits, meaning that compressing was successful, without loss of even a single bit. New security layers are also added to the secret data.

2.3 Steganography of Information

In the insertion of the information in the covering medium, the error rate that the insertion causes in the various image DNs, is different. To reduce the error of the insertion in the whole image, the insertion must be limited so that if the insertion error rate is higher than the threshold limit, the insertion is stopped or is done in fewer bits. In this way, the error rate in the whole image can be reduced and even more security layers can be added to the insertion of the information [5].

Eq.(1). $$Error(\%) = \frac{|DN(after) - DN(before)|}{DN(before)} \times 100$$

2.4 Analysis of the Results

Illustration in the MATLAB software environment was done in order to insert in various bits and different status in the Landsat image. To assess the results, the following statistical parameters, histograms and dispersion curves were used [8].

Eq.(2). $$\mathrm{PSNR}=10\log_{10}\left[\frac{\max(\mathrm{I})^2}{\mathrm{MSE}}\right]$$

Eq.(3). $$\mathrm{RMSE}=\sqrt{\frac{\sum_{MN}\left[I(m,n)-I'(m,n)\right]^2}{M\times N}}=\sqrt{MSE}$$

Eq.(4). $$\mathrm{CV(RMSE)}=\frac{\mathrm{RMSE}}{\mathrm{average(I)}}$$

It is worth mentioning that the results of the illustration of algorithms in different Landsat image bands were approximately close to each other. Therefore, the result of band 1 is just illustrated in this article.

2.4.1 CaseI: Limitless Insertion

In this case, information bit string is inserted in the least significant bits of image DNs, provided that the number of selected bits for the insertion in various DNs be the same. Table (1) shows the result of statistical parameters for various bits.

Table (1): statistical parameters for the insertion of information in various bit of band 1 of Landsat image

Size(byte)	PSNR(db)	RMSE	Cv(RMSE)	Num.bit
32768	51.1315	0.7079	0.6279	1bit
65536	44.1423	1.5828	1.4039	2bit
98304	10.5022	3.2407	2.8744	3bit
131072	31.8767	6.4969	5.7625	4bit

Figure (2) shows the image and theresulted histogram after the insertion of information in three least significant bits for band 1 of the Landsat image in limitless insertion.

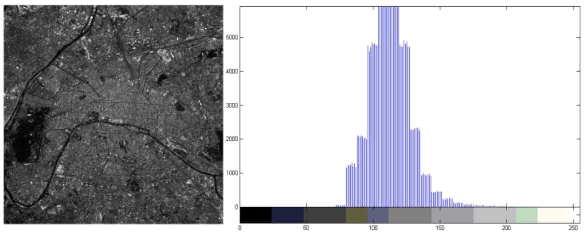

Figure (2): insertion of information in three least significant bits for band 1 of the Landsat image in limitless insertion

Figure (3) shows the scatter plot of the band1 image before vs after the insertion of the information in three least significant bits in limitless insertion.

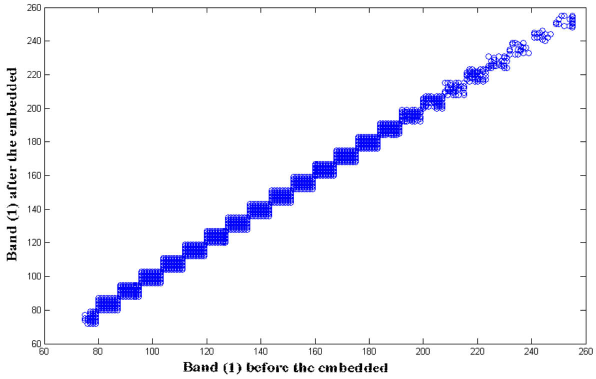

Figure (3): the scatter plot of the band1 imagefor insertion of (information) in three least significant bits in limitless insertion.

2.4.2 CaseII: Limited Insertion without Bitmap

In the first case, the number of bits in each DN was fixed. It means that there was no difference between low and high quantity DNs in terms of the number of bits in insertion. However, value pixel DNs was more subject to noise than the high value DNs. In the second case, to solve the problem, the insertion of the information for different DN values is limited. This means that the insertion in low DNs is either stopped or done in fewer bits, while the insertion in high quantity DNs is done in more bits. Hence, the error rate caused by insertion in the image will be reduced.

Limitations and conditions of insertion in this status:

- for DNs 144 to 255, insertion is done in 3 bits format
- for DNs 56 to 143, insertion is done in 2 bits format
- for DNs 28 to 56, insertion is done in 1 bit format
- finally for DNs less than 28, no insertion is done.

Table (2) shows the results given by the statistical parameters in limited insertion without bitmap

Table (2): the statistical parameters for limited insertion in images without bitmap

Size(byte)	PSNR(db)	RMSE	Cv(RMSE)	Error(%)
66557	43.7284	1.6600	1.4724	0.0052

Abundance and scatterplot curves after the insertion of information in the image are shown in figure (4) and figure (5) respectively.

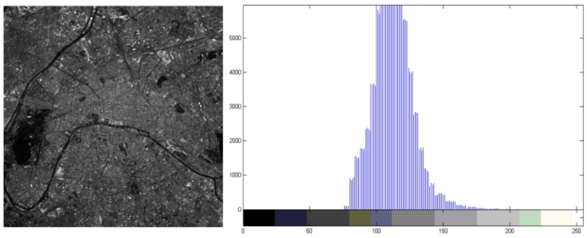

Figure (4): steganography of information by limited insertion without bitmap in band 1 of the Landsat image and its histogram

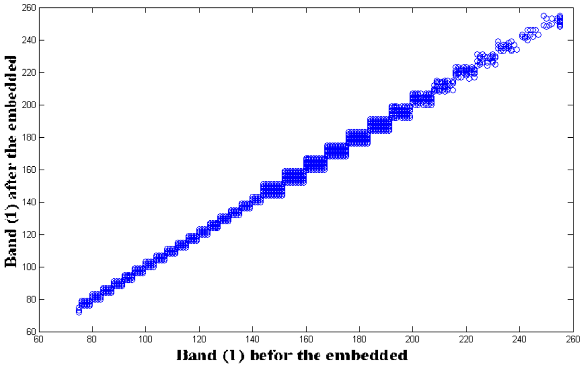

Figure (5): scatter plot of insertion of information by limited insertion without bitmap in band 1 of the Landsat image

2.4.3 CaseIII: Limited Insertion with Bitmap

A comparison between the scatterplot curves of the two images (Fig. 5) reveals that there are quantities in the scattered curve of the second image which fall away from the bisector. Reducing these quantities can decrease the error due to insertion in the image. However placing a bitmap in the insertion may remove this problem. Prior to each insertion in the DN, the error will be estimated; if the imposed error is reasonable, then the insertion will be implemented; if not, it is stopped. Insertion or not insertion will be registered in a bitmap. By means of this method a condition can be imposed in which no error in the image can occur. It means that the insertion can happen only in places where information bits are the same as image bits. So the bitmap will be a key to discover the secret data.

Limitations and condition of insertion in this method are:

- for DNs 144 to 255, insertion is done in 3 bits format
- for DNs 56 to 143, insertion is done in 2 bits format
- for DNs 28 to 56, insertion is done in 1 bit format
- finally for DNs less than 28, the insertion is done when there is no change in DN. According to this condition, the insertion is done when the relative error is less then 3%. Doing or stopping the insertion will be registered in the bitmap. Table (3) shows the results of the statistical parameters of the limited insertion with bitmap.

Table (3): statistical parameters of the limited insertion of information with bitmap

Size(byte)	PSNR(db)	RMSE	Cv(RMSE)	Error(%)
64599	44.3118	1.5522	1.3767	0.0037

Figure (6) shows the details and steps of the above algorithm.

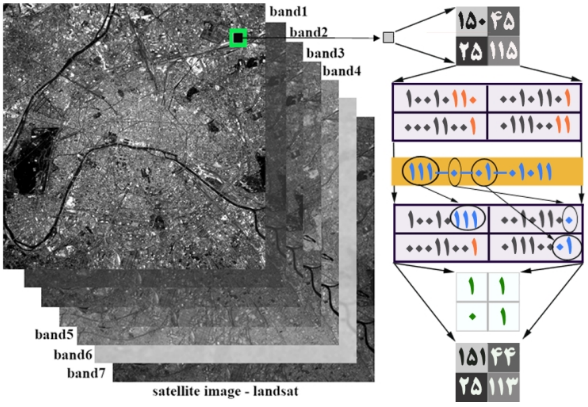

Figure (6): the steps of limited insertion of metadata with bitmap in the Landsat image

Abundance and scatterplot curves after the insertion of information in the image are shown in figure (7) and figure (8) respectively.

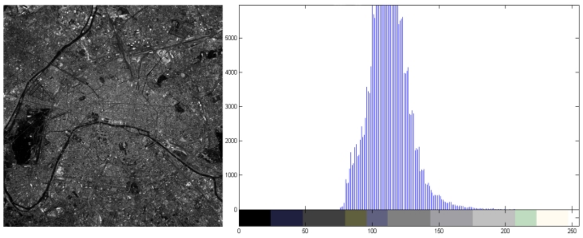

Figure (7): steganography of information by limited insertion with bitmap in Band 1 of the Landsat image and corresponding histogram

A comparison between the histograms in figure (4) and (7) indicates that the steps in either curves are identical but changes in the steps are more witnessed in the histogram of the figure (7) than that of figure (4). It means that the number of gray level DN in this case is more than previous cases and there are fewer changes in the image.

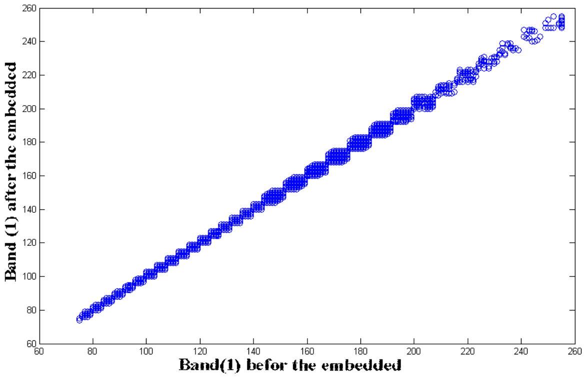

Figure (8): scatter plot of the insertion of information by limited insertion with bitmap in Band 1 of the Landsat image

A comparison between the dispersion curves in figure (5) and (8) indicates that the curves are almost identical but there are some differences: in the scatter plot in figure (8) the edges of the curve have been softened, approaching the bisector of the two images or the vertical line. It means that for image DNs more subject to noise, the insertion has not been done and the scattering has happened around the bisector of the two images.

3.0 Conclusion

In accordance with our primary goal, the insertion in the least significant bits of satellite images was done with the minimum change in the satellite images. In this way, in addition to enhancing metadata security coefficient, the bandwidth used for transferring metadata in the system was returned to the transfer channel. In other words, the insertion of metadata reduces the whole data volume and increases the system output, without any change in the satellite image volume.

The statistical parameters which controlled different steps of the insertion revealed that the best case for the insertion of the information in images encoded in 8 bits formats is insertion in two least significant bits. This case provides the best case of steganography in terms of the capacity of insertion with the minimum change in the images. With regards to the images encoded with 16 bits or more, the insertion in images continues as far as Psnr>40. Then the changes are not sensible in the inserted images, being less than 1.5%.

The preferences of this method:

The transferring equipment are not required to provide the necessary bandwidth for transferring metadata which means the reduction of volume and the increase of the output. In other words, the bandwidth volume that was previously used for transferring information to the target station, is returned to the transfer system; therefore, these information are transferred to the target station in accompany with the Landsat images, increasing the information security. This kind of insertion is called steganography.

REFERENCES

[1] Ingemar J. Cox,Matthew L. Miller,Jeffrey A. Bloom, Jessica Fridrich, TonKalker, ”Digital Watermarking and Steganography”, Second Edition2008 by Elsevier Inc.

[2] NISO:National Information Standards Organization, “Understanding Metadata,” NISO Press, ISBN 1-880124-62-9.

[3] Abbas_Cheddad, JoanCondell, KevinCurran, PaulMcKevitt,“Digital_image_steganography: Survey and analysis of current methods” , School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, UK , Signal Processing 90 (2010) 727–752.

[4] P. Alvarez, “Using extended file information (EXIF) file headers in digital evidence analysis”, International Journal of Digital Evidence, Economic Crime Institute (ECI), 2(3)(2004)1-5.

[5] Rafael C. Gonzalez, Richard Eugene Woods, "Digital image processing", Edition: 3, illustrated Published by Prentice Hall, 2007

[6] M. M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, And M.Z.I. Shamsuddin, "Information Hiding Using Steganography" , Faculty Of Computer Science & Information ystems,Universiti Teknologi Malaysia., 4th National Conference On Telecommunication Technology Proceedings, Shah Alam, Malaysia,IEEE 2003.

[7] Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview Of Image Steganography", Information And Computer Security Architecture (ICSA) Research Group Department Of Computer Science University Of Pretoria, South Africa,2005.

[8] A. A. Abdul Latef, "Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms" , Department of Computer Science ,College of Education Ibn Al-Haitham, University of Baghdad, VOL.24 (3) 2011.