Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Method for Steganography in Spatial Domain

M. Ravi Shankar Reddy
M .Tech (C.S.E),
G.Pulla Reddy Engineering College (Autonomous),
Kurnool, Andhra Pradesh, India.

Sri. J. Swami Naik
Associate professor Dept of C.S.E,
G.Pulla Reddy Engineering College (Autonomous),
Kurnool, Andhra Pradesh, India.

Abstract— Message hiding in some cover media has very important utility in the real world. This phenomenon is known as Steganography. Many approaches came into existence to hide message securely in cover media such as audio, video and images. In this paper we explore the hiding of text messages into a digital image in spatial domain. In our approach in each pixel two bits of message part is embedded. The process of hiding these bits is bit different here. We embed in such a way that the fourth bit place, second bit plane and also the least significant bits are allowed to modify in order to achieve the embedding process. However, only one change is allowed at a time in each embedding process. When compared with LSB-Matching, the proposed approach is every effective. We build a prototype application to demonstrate the proof of concept. The experimental results revealed that the proposed message hiding approach is robust and very useful in real world applications.

Keywords— Steganography, stego image, cover image, LSB matching, bit plane, steganalysis.

I. INTRODUCTION

Communication over Internet or any network is vulnerable when sufficient care is not taken. Secret sharing of messages has been around for many years to secure the message sent across the network. Cryptography has contributed a lot to this process. Cryptography is a branch of computer science which deals with security. Encryption is the process which converts plain text into cipher text which can't be understood. In the same fashion decryption is a process of converting cipher text to original plain text. However, the traditional cryptography has a limitation. The adversaries can view the cipher text and may try to decrypt it using their own approaches for monetary of other reasons if any. This is also not possible in Steganography. Steganography is gives more security than cryptography. Often these two are together used in order to provide high security to data to be transmitted. In Greek language "stagos" means hidden writing [1]. The steganography is the art of hiding secret messages into some multimedia covers. The cover media may include digital images, videos and audios. The messages embedded can't be taken by adversaries. Even if they are able to take them, they can't decrypt. Therefore multiple level of security is possible with Steganography. The technologies like cryptography and steganography can be used together for best results. As discussed here, the steganography is of three types, image steganography, audio steganography, and video steganography. In order words Steganography can be categorized into transform domain methods and special domain methods. In case of special domain LSB is used for replacing bits in order t1o hide. The transform domain methods try to hide data in another domain such as wavelet domain [2], [3]. In this paper, our focus is on hiding images into digital image in spatial domain. The text images that are embedded into images can't be viewed by the naked eye. This weakness of human eye is taken as advantage in Steganography. An image is made up of pixels. Each pixel value can be between the range 0 and 255. Each pixel can be represented using a binary number of 8-bits. It is a well known fact that the least significant bit of any pixel has some information that can't make any visual change to image even if it is altered [4]. This is an important feature that helps in hidden communication. This method is known as least significant bit method [5]. However, this method is not secure as the adversaries can use histogram of this approach to know where the information is embedded. LSB matching [6] solves this problem and it has been explored by many researchers [7], [8], [9]. Later on Mielikainen proposed an algorithm that behaves different from that of LSB. This is named as LSB-M [10]. Further improvement to this approach is made in [11]. In our approach ¼ is the probability of changing bit plane in order to hide two bits into each bit place. However, we allow three bit planes such as LSB, 2nd bit plane and fourth bit plane. The rest of the paper is structured as follows. Section II reviews literature. Section IIII provides information about the proposed approach to Steganography. The section IV presents experimental results while section V concludes the paper.

II. PROPOSED APPROACH TO STEGANOGRAPHY

In this paper our approach to steganography is to embed two bits of information in each pixel of cover image. Our approach allows modification of lease significant bit, fourth bit plane and second bit plane to make it more secure and robust to attacks. In the embedding process, overall, less number of pixels is modified. For this reason, our approach also reduces distortion. Distortion is a process of making visual change in the process of Steganography. The more distortion, the less efficient the method is. When human eye can't find the difference between the cover image and stego image, then we say that there is no distortion. When humans are able to find some difference, then we call it distortion. Less

distortion is desirable. Therefore our method is capable of reducing distortion also. The proposed approach is visualized as shown in figure 1.

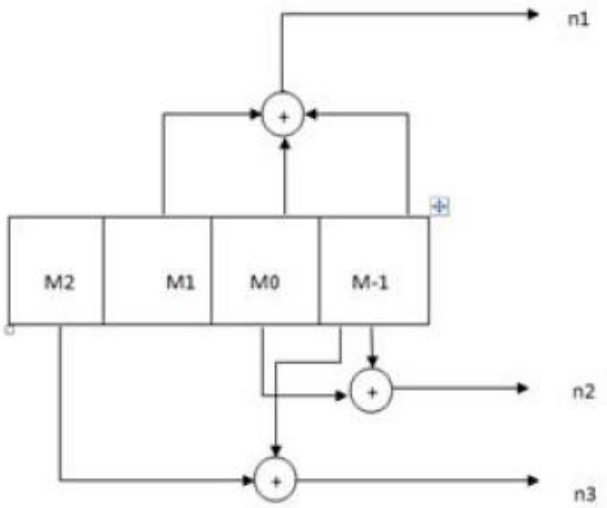

Fig. 1 –Transformation machine from cover to stego

As can be seen in figure 1, it is evident that there are inputs and outputs. The inputs are bits and cover image while the output is stego image. Cover image is the digital image into which text message or secret message is embedded. There are three XOR operations that can produce three outputs. If n2 and n3 are similar to hidden information, then there is no need to change image pixels. If notthe original image has to be modified. In this paper only one bit is allowed to change at each embedding process. There are only three ways in which pixel is allows to get modified.

1. Least significant bit is modified (Only one level of gray is increased or decreased)
2. The second bit plane is modified (two levels of gray is increased or decreased)
3. The fourth bit place is modified (eight levels of gray is increased or decreased)

The conversion procedure is as shown in table 1. The table shows first four less significant bit planes, decoder output, two message bits that come out of the decoder, cover image is changed to stego image, and gray level differencebetween stego and cover images.

First four less significant bit plane of a pixel	Decoder output	Two message bits coming out of Decoder	How cover Image should change in order to results in the desired message message → Stego pixel	Gray level difference between Stego and Cover pixel
0 0 0 0	0 0 0	0 0	0 1 → 1 0 0 0 1 0 → 0 0 1 0 1 1 → 0 0 0 1	8 gray levels 2 gray levels 1 gray level
0 0 1 0	1 1 0	1 0	0 0 → 0 0 0 0 0 1 → 0 0 1 1 1 1 → 1 0 1 0	2 gray levels 1 gray level 8 gray levels
0 0 0 1	1 1 1	1 1	0 0 → 0 0 0 0 0 1 → 0 0 1 1 1 0 → 1 0 0 1	1 gray level 2 gray levels 8 gray levels
0 0 1 1	0 0 1	0 1	0 0 → 1 0 1 1 1 0 → 0 0 1 0 1 1 → 0 0 0 1	8 gray levels 1 gray level 2 gray levels
0 1 0 0	1 0 0	0 0	0 1 → 1 1 0 0 1 0 → 0 1 1 0 1 1 → 0 1 0 1	8 gray levels 2 gray level 1 gray levels
0 1 0 1	0 1 1	1 1	0 0 → 0 1 0 0 0 1 → 0 1 1 1 1 0 → 1 1 0 1	1 gray level 2 gray levels 8 gray levels
0 1 1 0	0 1 0	1 0	0 0 → 0 1 0 0 0 1 → 0 1 1 1 1 1 → 1 1 1 0	2 gray levels 1 gray level 8 gray levels

Table 1–Procedure to convert cover into stego image

As can be seen in table 1, the first column shows four lest significant bits. Out of them first bit, second and fourth bit planes are allowed to be modified in order to embed messages. The last column shows that difference in gray levels between cover and stego images.

III. PROTOTYPE IMPLEMENTATION

We built a prototype application in Microsoft .NET platform to demonstrate the proof of concept. The application is built with graphical user interface to make it user friendly. The GUI is built using WinForms while the functionality is given in C# programming language. Visual Studio 2010 is the IDE used to build the application. The environment used to build the application include a PC with core 2 dual processor, 2 GB RAM and running Windows XP operating system. The main user interface of the application is as shown in figure 2.

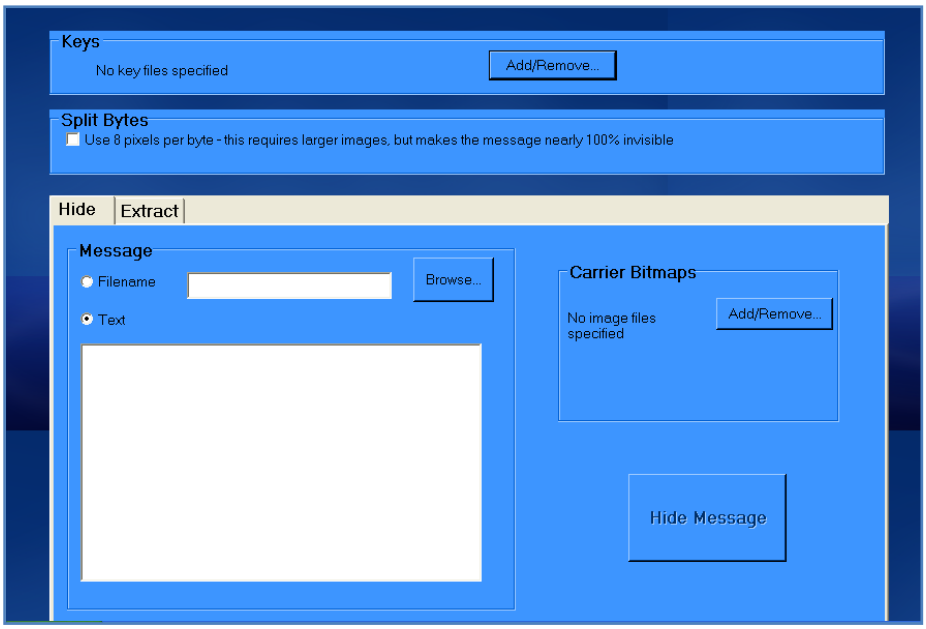

Fig 2. – Graphical user interface of the prototype

As can be seen in figure 2, the proposed prototype has provision for hiding and extracting text messages into images. The text and image selection and hiding and extracting messages are demonstrated using this application.

IV. EXPERIMENTAL RESUTLS

We made experiments in terms of finding differences between our method and also LSB matching. We also focused on finding fast positive rate at different bit planes. The correct detection rate is presented in figure 2.

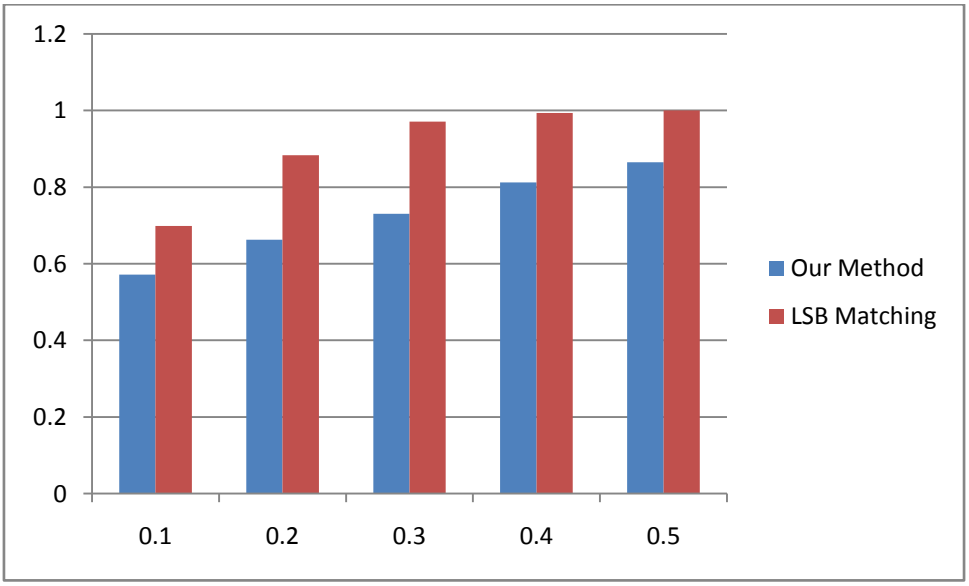

Fig. 2 –Correct detection rate with different bits/pixel

As can be seen in figure 2, our method outperformed existing method as it shows detection performance. As the number of bits per pixel is increased, the detection rate is increased. Out approach is compared with LSB matching here. The horizontal axis represents number of bits per pixel while the vertical exist shows the detection accuracy. The detection

accuracy is considered a value between 0.0 and 1.0. The more value indicates more accurate detection. The embedding rate and PSNR comparison between our method and LSB matching is as shown in figure 3.

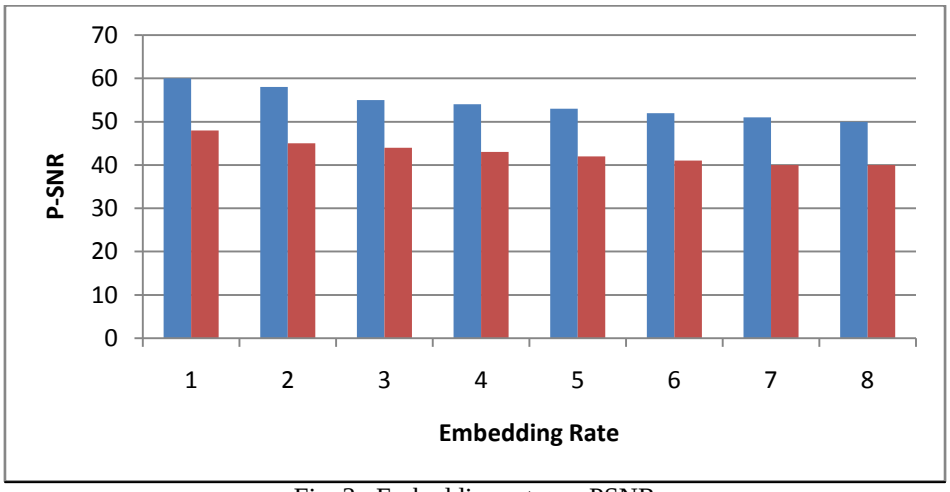

Fig. 3 –Embedding rate vs. PSNR

As can be seen in figure 3, it is very clear that with respect to embedding rate and PSNR the LSB matching has good performance. However, our method focuses on more secure embedding than that kind of performance. The horizontal axis shows embedding rate while the vertical axis shows the PSNR. The false positive rates for various embedding rate are shown in figure 3, 4, 5, and 6.

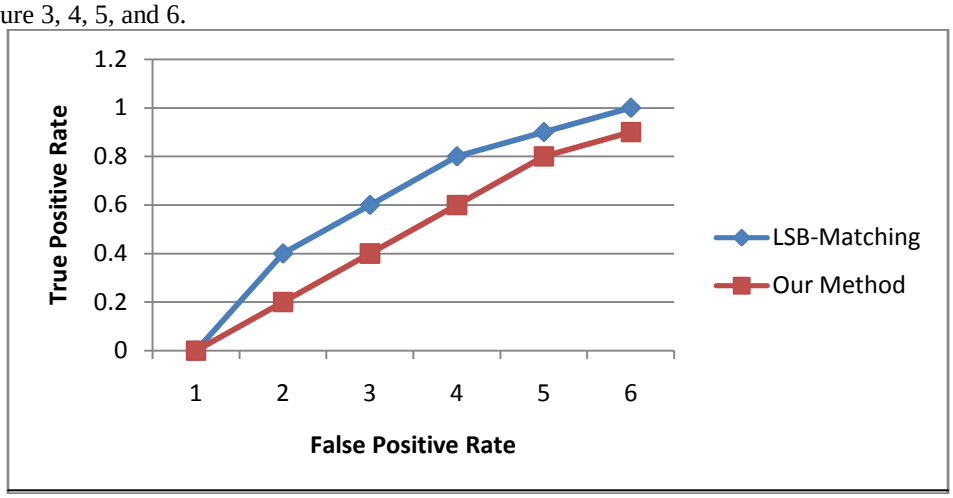

Fig. 4 -False positive rate comparison

As can be seen in figure 4, true and false positive rates are presented. This experiment is done with embedding rate 0.1 bit per pixel. The performance of our approach is better than that of LSB matching.

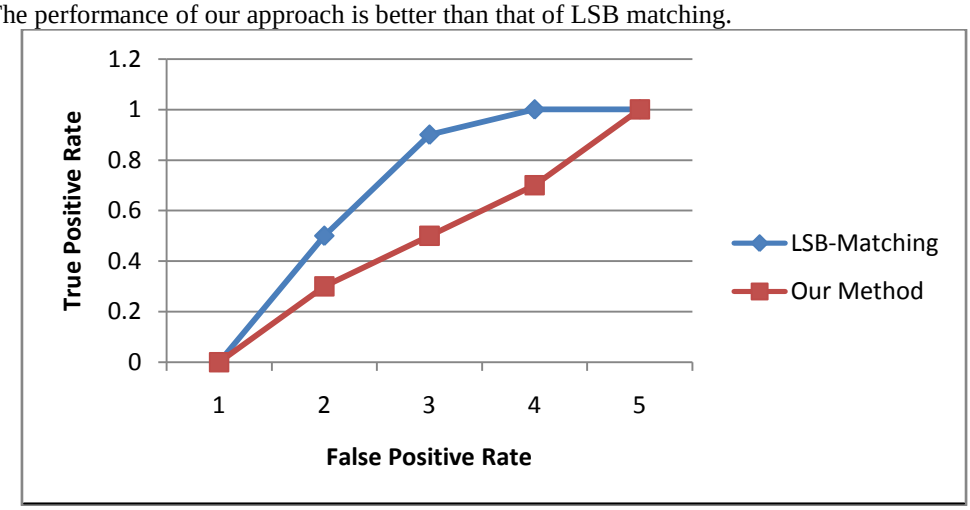

Fig. 5 - False positive rate comparison

As can be seen in figure 5, true and false positive rates are presented. This experiment is done with embedding rate 0.2 bit per pixel. The performance of our approach is better than that of LSB matching.

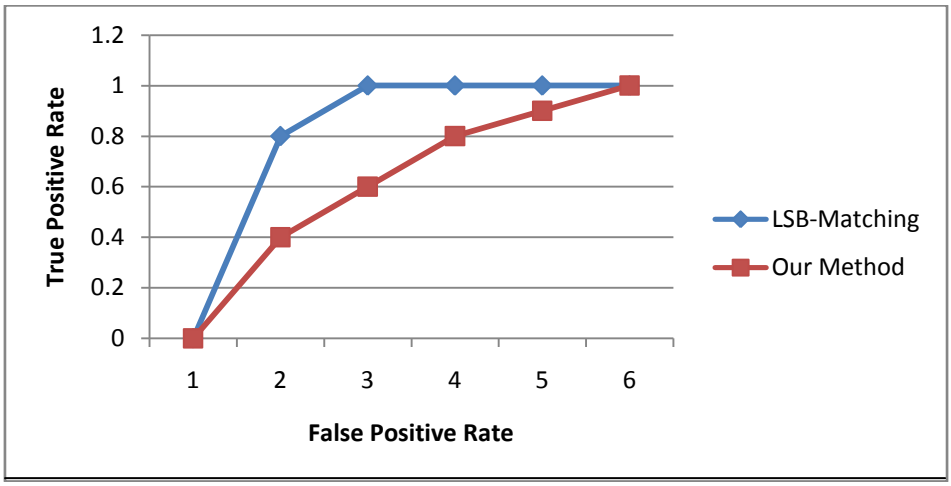

Fig. 6 - False positive rate comparison

As can be seen in figure 6, true and false positive rates are presented. This experiment is done with embedding rate 0.3 bit per pixel. The performance of our approach is better than that of LSB matching.

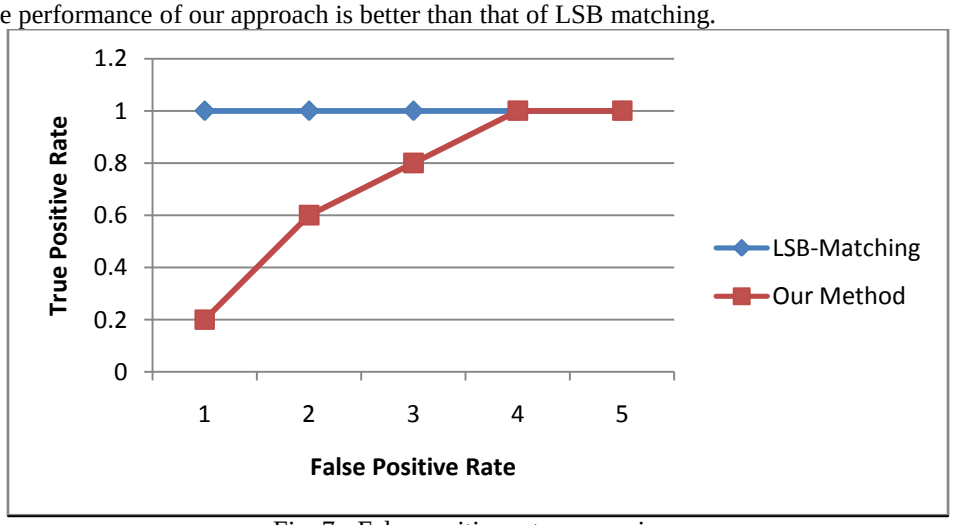

Fig. 7 - False positive rate comparison

As can be seen in figure 7, true and false positive rates are presented. This experiment is done with embedding rate 0.3 bit per pixel. The performance of our approach is better than that of LSB matching.

V. CONCLUSION

In this paper we studied hiding messages into a digital image. Our embedding approach is quite different from other approaches. We hide two bits of text message in a pixel. The embedding is done differently as fourth bit place, second bit place and the least significant bits are allowed to get modified to complete the embedding process. This has very important utility in reducing distortion. However, only one change can be made in every embedding process. This approach is proved to be efficient when compared with LSB matching. To demonstrate the efficiency of our approach we built a prototype application with graphical user interface to demonstrate the usefulness of the application. The empirical results revealed that the proposed application is robust and can be used in the real world applications.

REFERENCES

[1] E. Cole, Hiding in Plain Sight: Steganography and the Art of CovertCommunication, Wiley Publishing, USA, 2003.
[2] M. Mehrabi , H. Aghaeinia , M. Abolghasemi " Image SteganalysisBased on Statistical Moments of Wavelet Subband Histogram ofImage Least Significant Bit Planes , Congress on Image and SignalProcessing CISP 08 , CHINA , 2008.
[3] H. Sajedi and M. Jamzad, "Adaptive Steganography Method Basedon Contourlet Transform", ICSP 2008, pp. 745-748, October 2008.
[4] Rafael C. González, Richard Eugene Woods, "Digital ImageProcessing", Third edition, Pearson Education Inc 2008.
[5] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Informationhiding - A survey," Proc. of IEEE, vol. 87, no. 7, pp. 1062–1078, July1999.
[6] T. Sharp, "An implementation of key-based digital signalsteganography," in Proc. 4th Information Hiding Workshop, 2001,vol. 2137 of Springer LNCS, pp. 13–26

[7] WeiqiLuo, Fangjun Huang, Jiwu Huang, "Edge Adaptive ImageSteganography Based on LSB Matching Revisited", IEEETransactions on Information Forensics and Security, Vol. 5, No. 2.(June 2010), pp. 201-214.M.

[8] A. Ker, "Improved detection of LSB steganography in grayscaleimages," in Proc. Information Hiding Workshop, Vol. 3200, SpringerLNCS, pp. 97–115, 2004.R. Nicole, "Title of paper with only firstword capitalized," J. Name Stand. Abbrev., in press.

[9] M. Abolghasemi , H. Aghaeinia , K. Faez ,A . Mehrabi " Steganalysisof LSB-Matching Based on Co-Occurrence Matrix and RemovingMost Significant Bit planes", Intelligent Information Hiding andMultimedia Signal Processing , CHINA , 2008J. Clerk Maxwell, ATreatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford:Clarendon, 1892, pp.68–73.

[10] J. Mielikainen, "LSB Matching Revisited," IEEE Signal ProcessingLetters,Vol. 13, No. 5, pp. 285-287 May 2006.

[11] S.Sarreshtedari ," Steganography *and* Steganalysis" ,Msc thesis SharifUniversity of technology .2009

