ISSN: 2321-7782 (Online)
Volume 2, Issue 5, May 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Novel Approach for Reversible Data Hiding

Shilpy Mukherjee[1]
Research Scholar
Department of Computer Science and Engineering,
Priyadarshini Institute of Engineering & Technology
Nagpur University, Maharashtra – India

A R Mahajan[2]
Professor and Head
Department of Computer Science and Engineering,
Priyadarshini Institute of Engineering & Technology
Nagpur University, Maharashtra – India

Abstract: ***Nowadays, with the rapid development of information technology more and more images and data are available on the internet. So there is a need to provide some kind of authentication to such important data. With the increase in technology, the reversible data hiding (RDH) in encrypted images, has gain lots of importance. The reversible data hiding [1] is also known as the new watermarking technique which is used to authenticate an image by embedding some data on it as a watermark. A novel method is proposed by reserving room for embedding data before encryption of the image takes place with the available RDH algorithm and methods. Now the authentic person can hide the data easily on the image to provide authentication. This is the review paper about the current reversible data hiding algorithms available.***

Keywords: Reversible data hiding (RDH), Image encryption.

I. INTRODUCTION

With the growth of information technology large number of images and data are found on the internet. So there is a need to provide security to such important data. When the sender transmits the image to the receiver, there may be intruders present in between who may capture the image. After capturing the image the image the intruder may view the meaningful content in the image. This may not be the problem in some cases. But if we consider medical and military images then such distortion is unacceptable. Watermarking technique can be classified into two different types. In the first type the watermark is visible i.e. different logos or text can be inserted which is visible. This technique can be seen in Microsoft MS Word where we apply watermarks on the pages which are visible. The second technique used for applying watermarks to the images, videos, is invisible. This invisible technique is called as digital watermarking. The digital watermarking technique can be used for a wide range of applications, like for providing copyright protection to the films, videos, etc. The digital watermark is a more secured technique because the watermark is not visible, So if the intruder view the content of the image he will not be aware of the watermark which is already present in the image. So if the intruder performs any modification in the image it will be known to the receiver after receiving the image. The receiver after receiving the image will see that the watermark has been changed and will be aware that the image has been modified. The watermarking technique can be made more secure by encrypting the watermarked image. Various methods of encryption can be used to encrypt the image. Encryption is a technique by which the image is changed or modified by using keys. The encryption technique can be classified into two type's i.e. symmetric key encryption in which the same key is used for encryption and decryption and asymmetric key encryption in which different keys are used for encryption and decryption. Sender will use the public key for encryption and receiver will use the private key for decryption. But whatever technique is used, the original quality of the image must be recovered at the receiver i.e. the receiver must get the original image after removing the watermark and after decrypting the encrypted image.

Reversible data hiding[2] is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten[3]. This would make the images acceptable for legal purposes. Reversible data hiding (RDH) [17][18] has the capability to erase the distortion introduced by embedding step after cover restoration. It is an important property that can be applied to many scenarios, such as medical

imagery, military imagery and law forensics. For this reason, RDH becomes a hot research topic and is extensively studied over the years. Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted.

Data hiding technique aims to embed some secret information into a carrier signal by altering the insignificant components for copyright protection or covert communication. In general cases, the data-hiding operation will result in distortion in the host signal. However, such distortion, no matter how small it is, is unacceptable to some applications, e.g., military or medical images. In this case it is imperative to embed the additional secret message with a reversible manner so that the original contents can be perfectly restored after extraction of the hidden data. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods,[7] difference expansion (DE)methods[5][16], and histogram modification (HM) methods[9].The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate additional secret data.

II. Related Work

The previous reversible data hiding techniques were based on the concept of emptying room after encryption. The reversible data hiding were carried out using reversible data hiding algorithms. The different algorithms can be classified as given below.

1. Separable Reversible Data Hiding in Encrypted Image

This technique proposes a novel scheme for separable reversible data hiding in encrypted images [4The scheme proposed in this paper is made up of encryption of image, data embedding and recovery of original image phases. The sender also known as the content owner encrypts the original uncompressed image using the image encryption algorithms using a key known as the encryption key to produce an encrypted image. Then, the server compresses the least significant bits (LSB) of the encrypted image using a data-hiding key for creating a sparse space to store the additional data or the watermark information. At the destination side, the data embedded in the image can be retrieved easily from the encrypted image containing additional data according to the data-hiding key. Since the embedding of data only affects the LSB, a decryption of the image with the encryption key can result in an image that is similar to the original version of the image. When we use both keys i.e the encryption and data-hiding keys, the additional data embedded can be extracted successfully and the original image can be recovered perfectly by exploiting the spatial correlation in natural image.. The disadvantages of this technique were eliminated by proposing a new scheme known as the seperable reversible data hiding scheme. This technique proposes the scheme of seperable reversible data hiding by removing the disadvantages of non seperable scheme. The disadvantages of the non seperable scheme was that at the receiver side it was necessary to first decrypt the image and take out the watermark information and the only the receiver can view the content of the original image by decrypting it further. It was necessary for the receiver to first know the data hiding key ,without which the image could not be decrypted. This disadvantage of non seperable reversible data hiding was eliminated in seperable reversible data hiding as the receiver can decrypt the image by using data hiding key to view the watermark information and the receiver can also decrypt the image using the encryption key to view the original contents of the image.

2. Reversible Data Hiding in the Spatial and Frequency Domains:

In this technique lossless combinational data hiding in the spatial and frequency domains is considered [11]. In the spatial domain, watermark information or the secret message is embedded in the sender's image using the min-max algorithm to generate a stego-image. Afterwards, the stego-image is partially decomposed into the frequency domain via the transform known as the integer wavelet transform (IWT)[12][13]. Subsequently, a watermark information is hidden in the low-high (LH) and high-low (HL) sub bands of the integer wavelet transfer domain using new approach called as a coefficient-bias approach.

3. Reversible Data Hiding With Optimal Value Transfer:

In reversible data hiding techniques, the values of sender image are modified. According to some constraints the original content of the image can be correctly restored after extracting the watermark data on the receiver side. According to this technique, the optimal constraint of value modification using a payload-distortion criterion is founded by using the iterative procedure, and a reversible practical data hiding scheme was proposed. The secret watermark data, as well as the additional information used for recovering the content, were carried out by the differences between the original pixel-values and the corresponding values estimated from the neighbors. In this, the errors estimated [8] were modified according to the optimal value transfer rule. Also, the original image was divided into a number of subsets of the pixel and the additional information of the subset was always embedded into the errors estimated in the next subset. The receiver could successfully extract the content i.e. the embedded secret data and recover the original content of the image in the subsets with an inverse order.

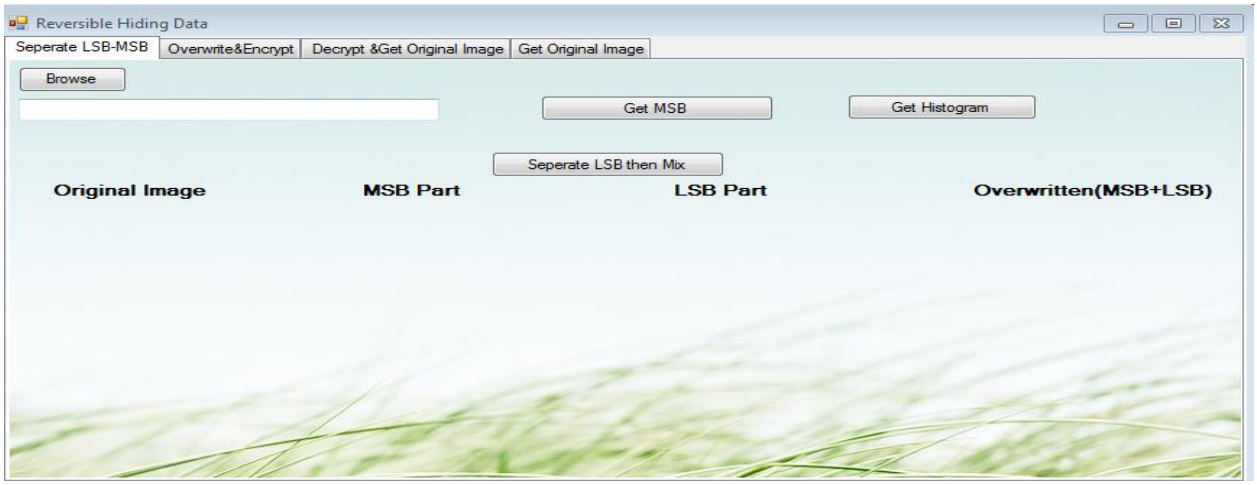
4. Histogram Shifting Method

Ni et al. [23] utilizes zero or minimum point of histogram. If the peak is lower than the zero point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. When embedding is done, the whole image is searched. Once a peak-pixel is found, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Similarly, if the peak is higher than the zero point in the histogram and using the algorithm the pixel value is decreased by one from lower than the peak to higher than the zero or minimum point in the histogram, and to embed bit '1' the found peak-pixel value is reduced by 1. The process of decoding is quiet simple and opposite of the embedding process. The advantages of this method are it' simplicity, a constant PSNR 48.0Db is obtained, distortions are low, and higher capacity is obtained.

III. PROPOSED WORK

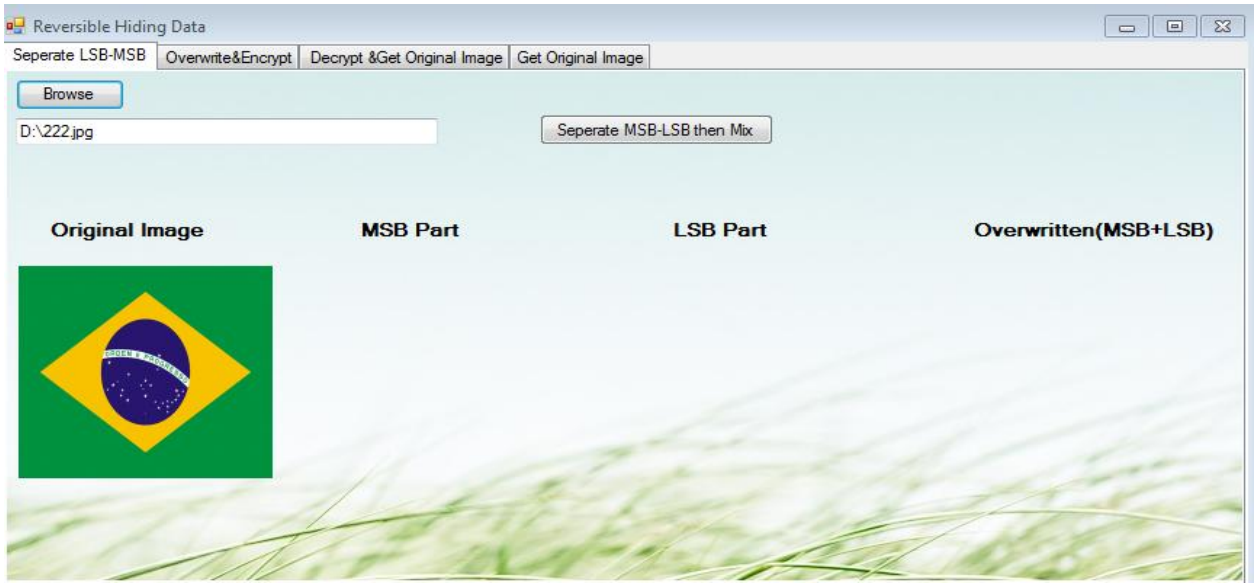
A new reversible data hiding technique is proposed based on the concept of reserving the space for embedding data before encryption. According to the new technique the sender who wants to transmit the image first divides the image. The sender will first divide the image into two parts known as least significant bits i.e. LSB and MSB [1]. The LSB part of the image can be embedded on the MSB portion of the image. After embedding the LSB portion on the MSB portion the image is encrypted using encryption key and then the image can be transmitted. Now the watermark is embedded on the encrypted image. After embedding the watermark the image is further encrypted [2] and then can be transmitted. Now the receiver will receive the image and decrypt the image to receive the data and the original image. The various snapshots of the proposed work are explained below.

1.



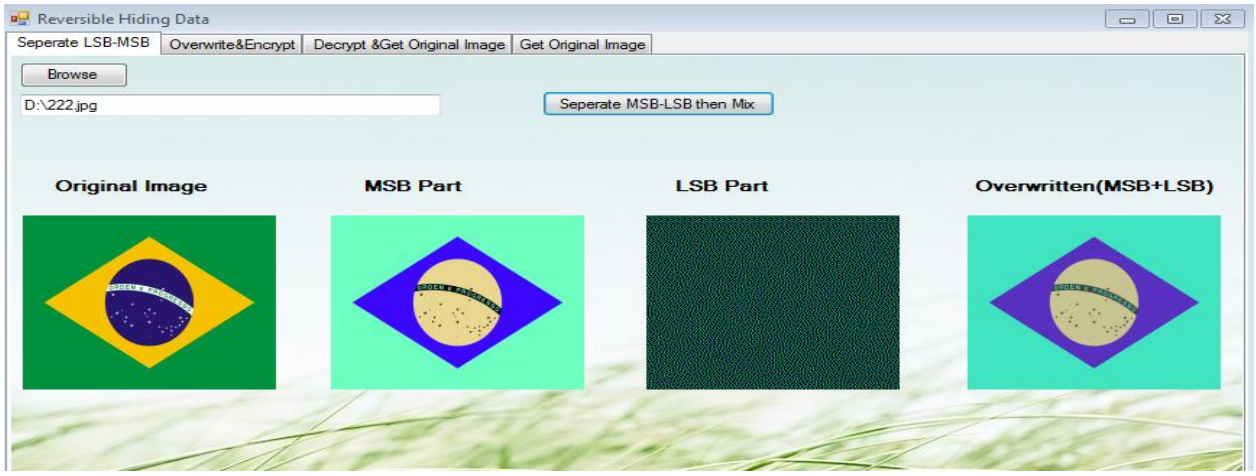
This is the main form of the project. It consists of various buttons which must be selected for various functions.

2.



First of all by clicking on the browse button we have to browse the image.

3.



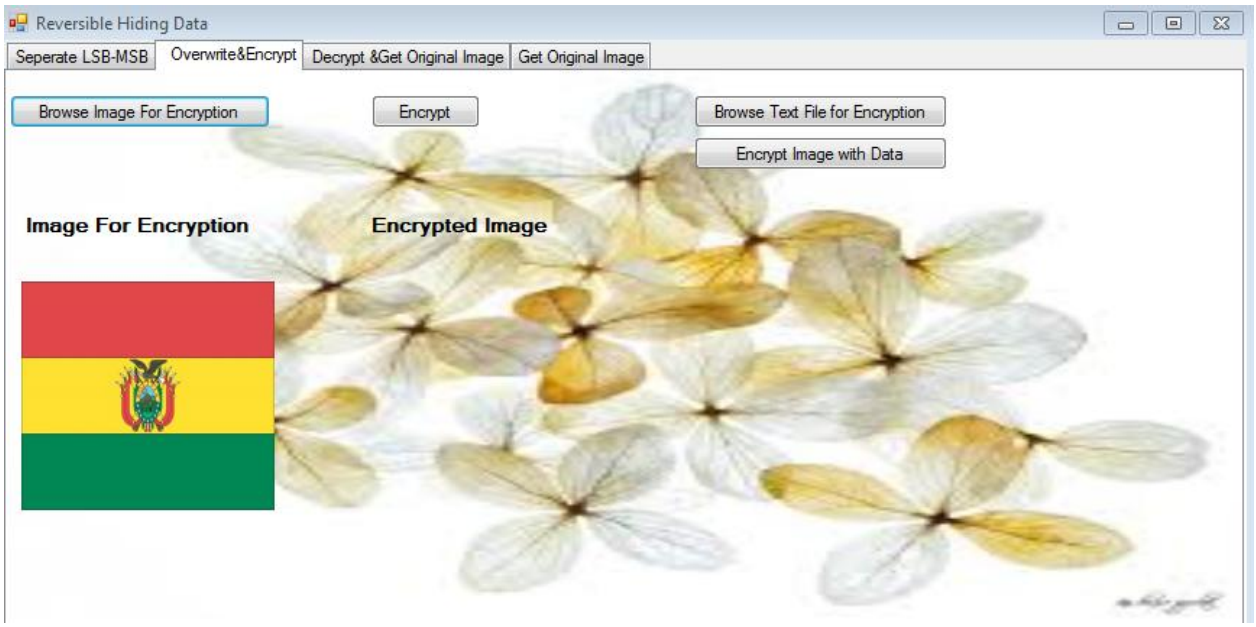
Now after browsing the image, by clicking on the separate MSB-LSB then Mix button we will get the LSB, MSB, and LSB embedded on the MSB.

4.

In the form given below we can see that after separating the LSB, MSB and embedding LSB On MSB of the image the image is to be encrypted, so we have to click on the browse image for encryption button to search another image for encryption.

5.

Now in the form given below, we can see that the image is browsed for encryption.

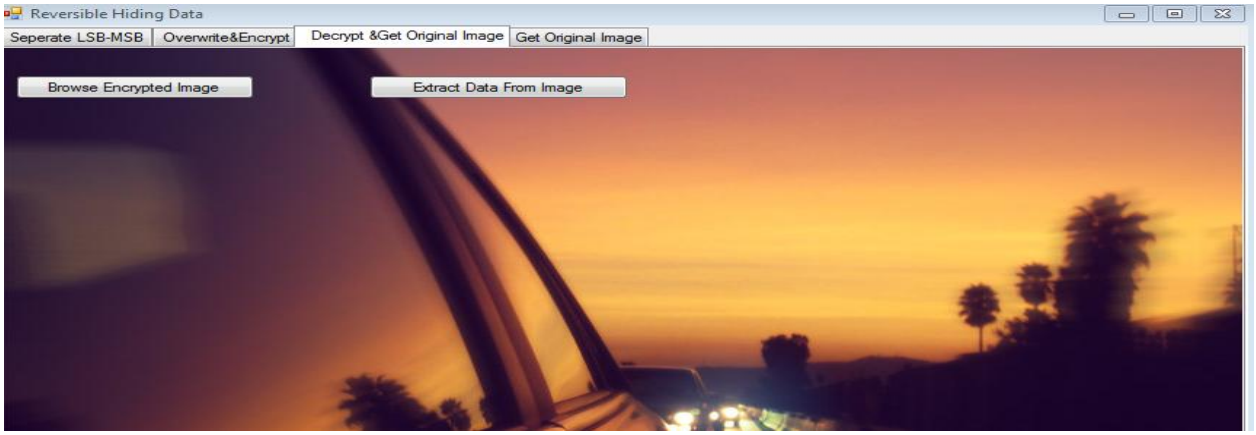


6.

After browsing the image for encryption, we have to click on the encrypt button to encrypt the image using another image. The form given below shows the encrypted image. After encrypting the image the text file is searched for embedding on the image. After searching the text file, the image is again encrypted and transferred to the receiver.

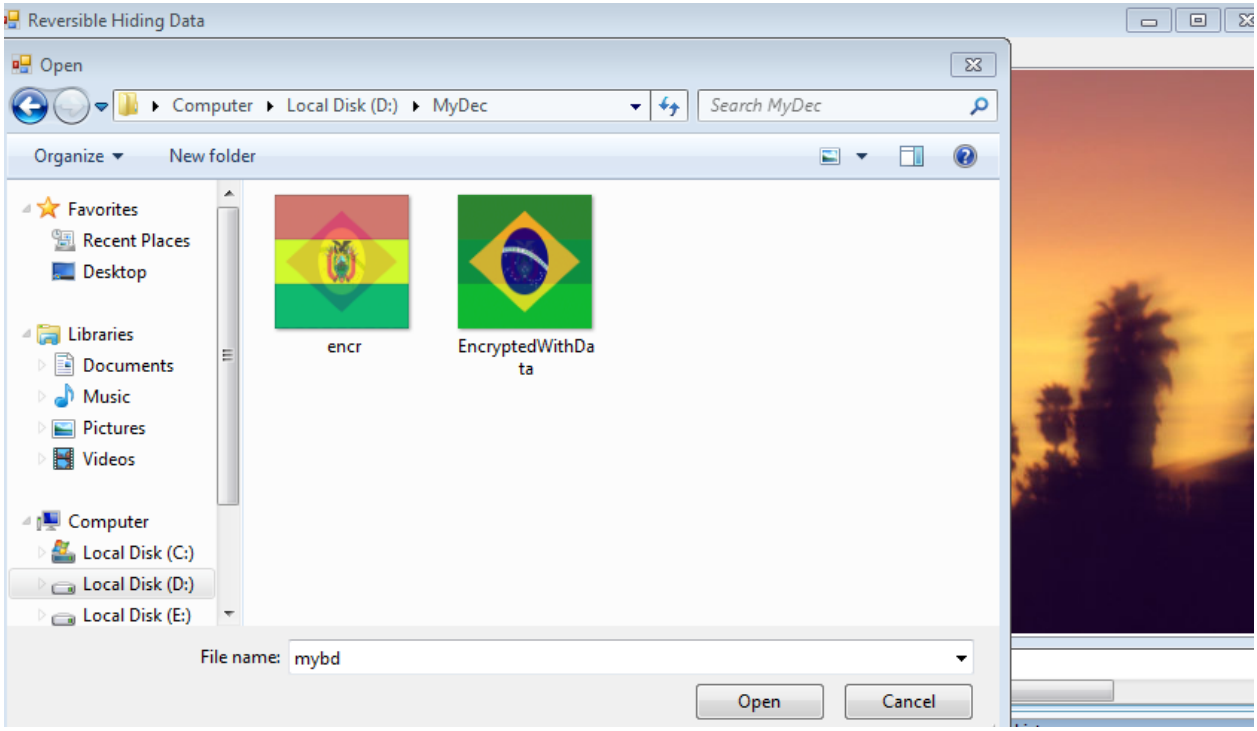
7.

Now the image is encrypted and the receiver wants to recover the original image. The receiver has to browse the original image first

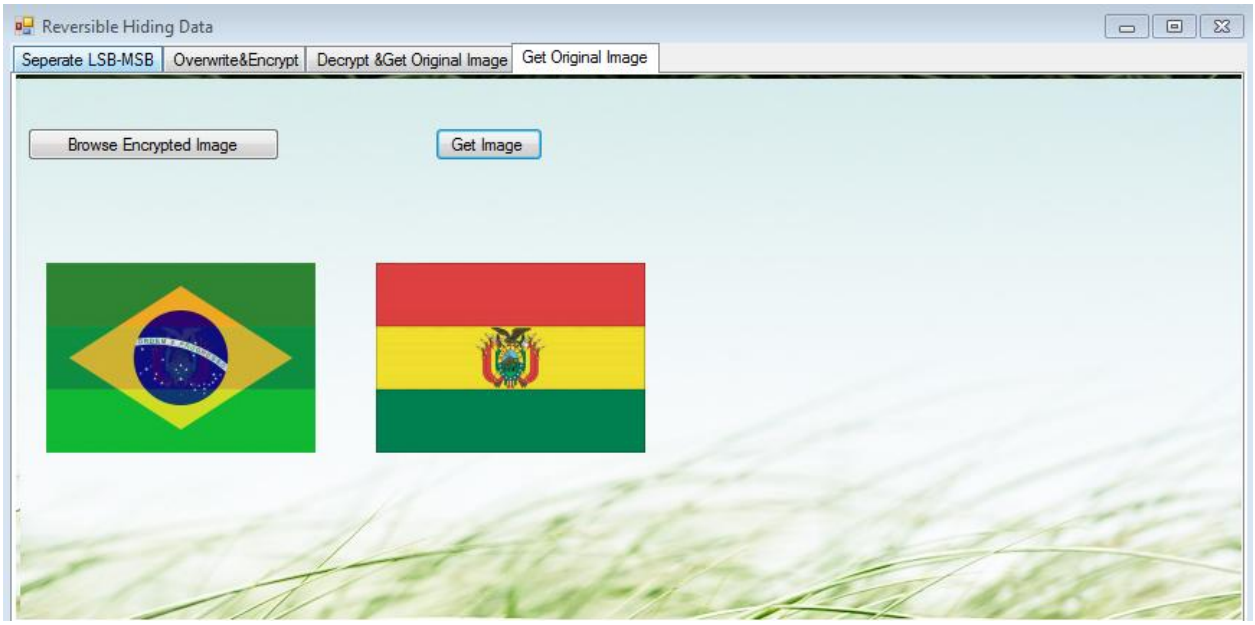


8

Now the image encrypted with data is browsed from the system.



9.



Now after clicking on the get image button the receiver can recover the original image.

IV. CONCLUSION

Image data plays vital role in every aspects of system such as social networking, Google image search, vide news, video entrainment, medical image. Several of the method proposed has been designed to implement the reversible data hiding techniques. This paper presented various existing reversible data hiding technique proposed by researchers. The new technique is implemented which can separate the image and data from the encrypted image. This is also a new technique for providing watermark to the image.

References

1. Keda Ma,W Zhang, X Zhao,"Reversible Data Hiding in Encrypted image by Reserving Room Before Encryption",IEEE Trans on Information Forensics and Security,vol 8,no 3, March 2013
2. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
3. W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
4. X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
5. J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
6. Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
7. D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
8. X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
9. P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.
10. Mohammad Awrangjeb, An Overview of Reversible Data Hiding, ICCIT 2003, 19-21 Dec, Jahangirnagar University, Bangladesh, pp 75-79.
11. J. Fridrich, M. Goljan, and D. Rui, "'Invertible Authentication", In Proc. of SPIE Photonics West, Security and Watermarking of Multimedia Contents III, San Jose, California, USA, Vol. 3971, pp. 197-208, January 2001.
12. R. Rivest, "The MD5 Message-Digest Algorithm", In DDN Network Information Center, http://www.ietf.org/rfc/ rfc1321.txt, April 1992.
13. K. Sayood, "Introduction to Data Compression", Morgan Kaufmann, 1996, pp. 87-94.
14. J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps", On Int. Journal of Bifurcation and Chaos, 8(6), pp. 1259-1284, June 1998.
15. M.U. Celik, G. Sharma, A.M. Tekalp., and E. Saber, "Reversible Data Hiding", In Proc. of International Conference on Image Processing, Rochester, NY, USA, Vol. 2, pp. 157-160, September 24, 2002.
16. J. Fridrich, M. Goljan, and D. Rui, "Lossless Data Embedding for all Image Formats", In Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, California, USA, Vol. 4675, pp. 572-583, January, 2002.

17. X. WU, "Lossless Compression of Continuous-Tone Images via Context Selection, Quantization, and Modeling", IEEE Transactions on Image Processing, Vol. 6, No. 5, pp. 656-664, May 1997.

18. G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless Data hiding based on Integer Wavelet Transform", In Proc. of IEEE International Workshop on Multimedia Signal Processing. Marriott Beach Resort St. Thomas, US Virgin Islands, 9-11 December 2002.

19. A. R. Calderbank, I. Daubechies, W. Sweldens, and B. Yeo, "Wavelet Transformations that Map Integers to Integers", In Proc. of Applied and Computational Harmonic Analysis, 1998, Vol. 5, No. 3, pp. 332-369.

20. Y. Q. Shi, and H. Sun, "Image and Video Compression for Multimedia Engineering", Boca Raton, FL: CRC, 1999.

21. J. Tian, "Wavelet Based Reversible Watermarking for Authentication", In Proc. Security and Watermarking of Multimedia Contents IV, Electronic Imaging 2002, Vol. 4675, pp. 679-690, 20-25 January 2002.

22. J. Tian, "Reversible Watermarking by Difference Expansion", In Proc. of Workshop on Multimedia and Security, pp. 19-22, December 2002.

23. Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding, In Proc. of International Symposium on Circuits and Systems, Bangkok, Thailand, Vol. 2, pp. 912-915, 25-28 May 2003.

24. M. Awrangjeb, "A Survey Report: Content Authentication with Lossless Watermarking",

