ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Secure Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption

Prof. Kanchan Deshmane[1,] Jaymala Hipparkar[2]

Assistant Professor, Dept. of CSE, Shri Vithal Education & Research Institute's COE, Pandharpur, Solapur University, Maharashtra, India[1]

M.E Student, Dept. of CSE, Shri Vithal Education & Research Institute's COE, Pandharpur, Solapur University, Maharashtra, India[2]

ABSTRACT: Today reversible data hiding in encrypted images by reserving room before encryption is a very important technique is use in various application of security. Where data security is primary very important. This mechanism are primary use in inelegancy agency. Sometime when we deal with a data and that data is observed ob third party user and that situation you want to hide data in particular mechanism that time we can use this reversible data hiding in encrypted images by reserving room before encryption technique. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR dB.

KEYWORDS: Reversible data hiding, image encryption, privacy protection, histogram shift.

I. INTRODUCTION

This is technique which can use to recover original image without any data loss. we can put cover on original image and extract this cover ant get a original data. Now we can introduce about the system. This is a technique in which we can recover original image after the embedded message is extracted. This is use in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since rest introduced, RDH has attracted considerable research interest.

Thus , technique of reversible data coloring is on encrypted data is preferred. Suppose a medical image database is stored In a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its integrity without having the knowledge of the original content, and thus the patient's privacy is protected.

In this Existing System, since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for Encrypted Images? The method in compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration.

Disadvantage:

1 Low error rate
2 Data extraction and image restoration problem
3 Required time to extract data
4 Its lengthy process

II. RELATED WORK

In theoretical aspect, Kalker and Willems established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memoryless covers and pro- posed a recursive code construction which, however, does not approach the bound. Zhang *et al.* improved the recur- sive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction.
To separate the data extraction from image decryption, Zhang emptied out space for data embedding following the idea of compressing encrypted images Compression of encrypted data can be formulated as source coding with side information at the decoder [14], in which the typical method is to generate the compressed data in lossless manner by ex- ploiting the syndromes of parity-check matrix of channel codes. The method in compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images.
All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads or generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration. Al- though the methods in can eliminate errors by error- correcting codes, the pure payloads will be further consumed.
Hong *et al.* reduced the error rate of Zhang's method by fully exploiting the pixels in calculating the smoothness of each block and using side match. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smooth- ness of unrecovered blocks, which is referred to as side match.

III. PROPOSED TECHNIQUE

Proposed technique is very simple method of reversible data hiding and extracting original data.

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)"

Advantage

Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- ✓ Real reversibility is realized, that is, data extraction and image recovery are free of any error.
- ✓ For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

MODULES

1. Encrypted Image Generation
   a) IMAGE PARTITION
   b) SELF REVERSIBLE EMBEDDING
2. Data Hiding In Encrypted Image
3. Data Extraction and Image Recovery

4. Data Extraction and Image Restoration

MODULES DESCRIPTION:

ENCRYPTED IMAGE GENERATION

In this module, to construct the encrypted image, the first stage can be divided into three steps:

a) IMAGE PARTITION,

b) SELF REVERSIBLE EMBEDDING followed by image encryption.

At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

a) IMAGE PARTITION

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition.

b) SELF REVERSIBLE EMBEDDING

The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We simplify the method in to demonstrate the process of self-embedding.

DATA HIDING IN ENCRYPTED IMAGE

In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

DATA EXTRACTION AND IMAGE RECOVERY

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

DATA EXTRACTION AND IMAGE RESTORATION

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image.

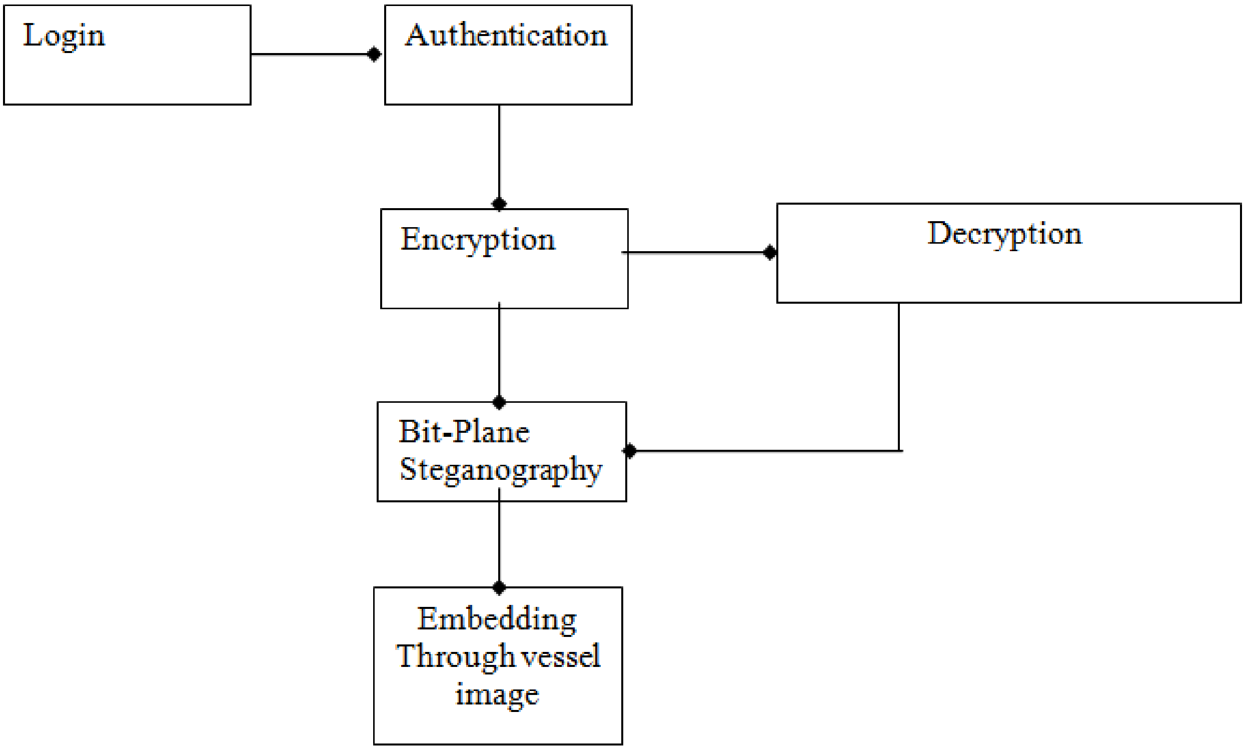
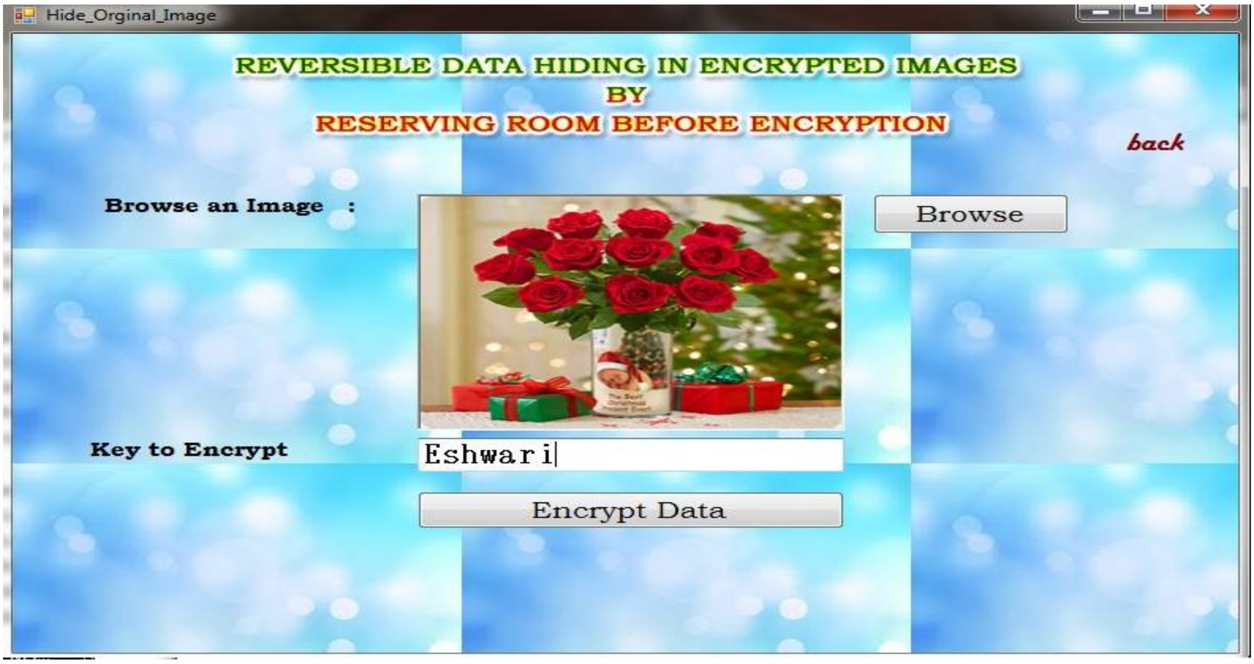


Fig 1:System Architecture

IV. IMPLEMENTATION OF RRBE

The figure 2 gives the data user room before encryption process in this stage the user will provide the information the image and encrypted key to the RRBE. The RRBE will process the user input will complete the encryption process this things can observe in the figure 3. The figure 4 and 5 will gives after RRBE of the user data, the user should register to the service provider, the service provider will hides the data by applying the service provider data hiding algorithms or also called as service provider encryption process.

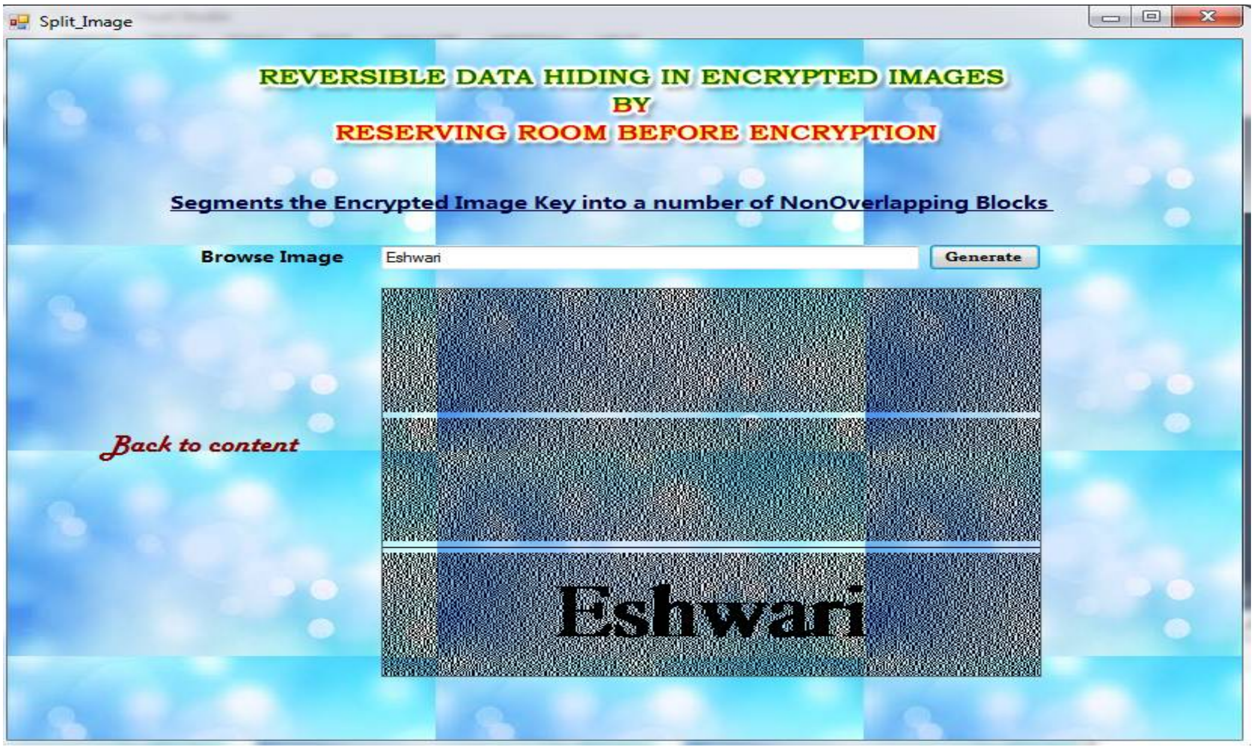


REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES
BY
RESERVING ROOM BEFORE ENCRYPTION

Browse an Image :

Key to Encrypt Eshwari

Fig 2:User Data Input Provider

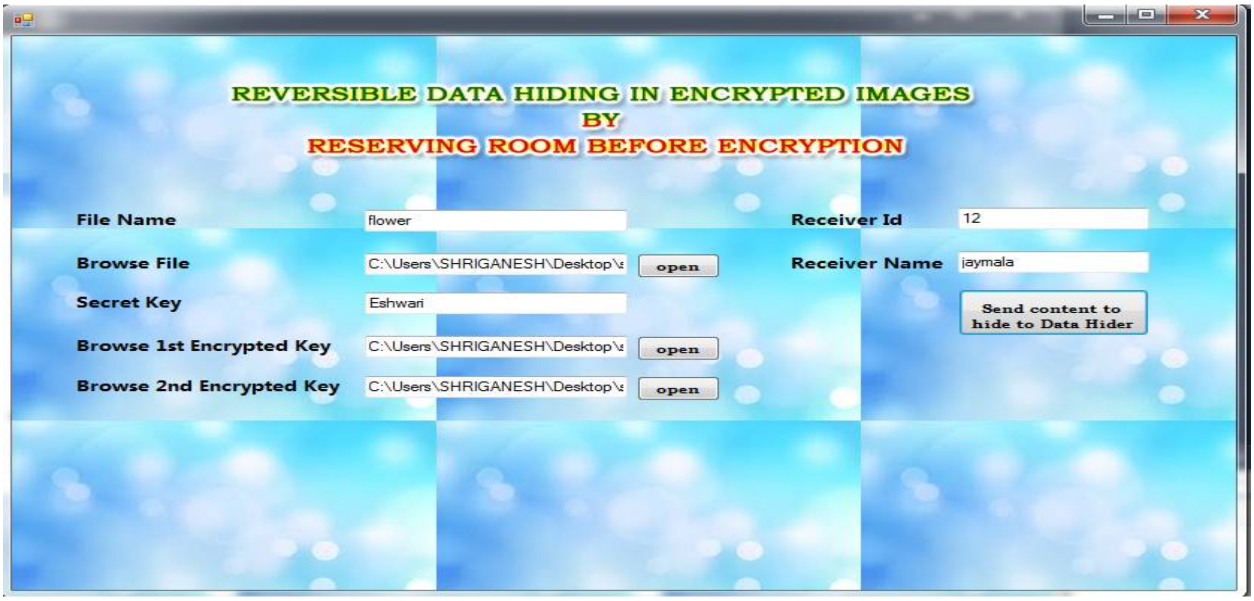


REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES
BY
RESERVING ROOM BEFORE ENCRYPTION

Segments the Encrypted Image Key into a number of NonOverlapping Blocks

Browse Image Eshwari

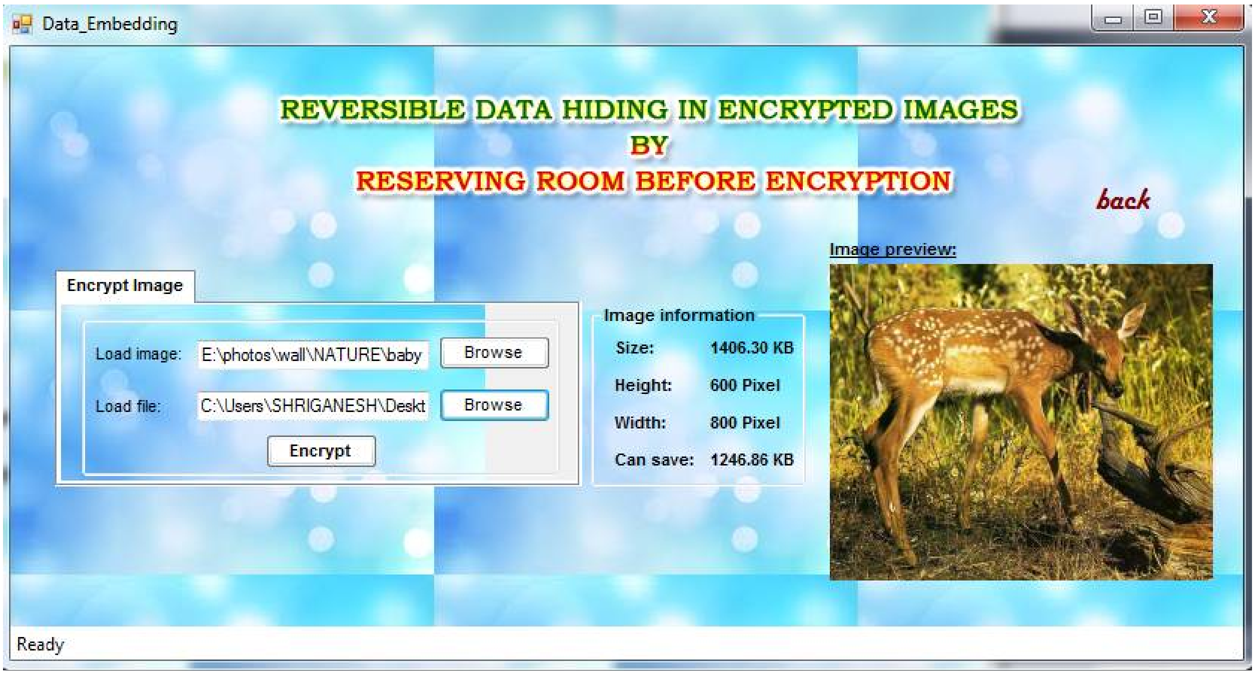
Fig 3: The Encryption process completion message displayer.



REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES
BY
RESERVING ROOM BEFORE ENCRYPTION

File Name: flower
Browse File: C:\Users\SHRIGANESH\Desktop\: open
Secret Key: Eshwari
Browse 1st Encrypted Key: C:\Users\SHRIGANESH\Desktop\: open
Browse 2nd Encrypted Key: C:\Users\SHRIGANESH\Desktop\: open
Receiver Id: 12
Receiver Name: jaymala

Fig 4: Data hiding by service provider.



Data_Embedding

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES
BY
RESERVING ROOM BEFORE ENCRYPTION

Load image: E:\photos\wall\NATURE\baby
Load file: C:\Users\SHRIGANESH\Deskt

Image information
Size: 1406.30 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB

Image preview:

Ready

Fig 5: Data Hiding Success by Service Provider.

V. CONCLUSION

In reversible data hiding method we can learn that data can be recover lossless if you can use a right technique. Data is a very important and integral part of any field and the secrecy of that is also very important in an medical and government and military operation. So this approach provides a very important approach to hide and get data with easily anywhere without loss. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent perfor- mance without loss of perfect secrecy.

REFERENCES

1. J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
2. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
3. Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.
4. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
5. M.Johnson, P.Ishwar, V.M.Prabhakaran, D.Schonberg, and K.Ramchandran, "On com-pressing encrypted data," IEEE Trans. Signal Process, vol. 52, no. 10 Oct 2004., pp. 2992-3006.
6. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
7. "The apache cassandra project," http://cassandra.apache.org/.
8. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
9. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.
10. O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems, vol. 28, no. 1-2, pp. 177 – 189, 2000.
11. Helsinger and T. Wright, "Cougaar: A robust configurable multi agent platform," in Proc. of the IEEE Aerospace Conference,2005.
12. J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, "Egg: an extensible and economics-inspired open grid computing platform," in Proc. of the GECON, Singapore, May 2006.
13. J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeating spikes with a free-market application cluster," in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.
14. C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007.
15. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on demand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.
16. M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet, 2001.
17. N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.
18. C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, "Transparent symmetric active/active replication for servicelevel high availability," in Proc. of the CCGrid, 2007.
19. J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez-Peris, "Ws-replication: a framework for highly available web services," in Proc. of the WWW, New York, NY, USA, 2006.
20. T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

BIOGRAPHY

Jaymala Kundlik Hipparkar is a M.E. student in Computer Science and Technology ,Shri Vithal Education & Research Institute's COE,Pandharpur ,413 304. Dist. Solapur ,Solapur University.