ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Hiding Human Information into Encrypted Image

G.Anitha[1], Mr. Kannan Subramanian[*2]

[1] Assistant Professor, Master of Computer Application, Jerusalem College of Engineering, Chennai, India

[2*] Associate Professor, Master of Computer Application, Bharath University, Chennai, India

ABSTRACT*:* Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the extreme property that the original cover can be loss less recovered after Converting data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. 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

KEYWORDS: reversible data hiding (RDH),Peak signal to noise ratio(PSNR),Least Significant bit(LSB)

I INTRODUCTION

To achieve secure data sharing for using cover image reserving room before encryption method. Reserving room means allocate some location based on the file size. First, we have to reserve some LSB bit in the input image. And then we have to encrypt the image using encryption key. The next step, we hide the data using data hiding key on the reserved place of that image. Those processes done by the sender side and then send to receiver. But, the receiver side reverses the above processes that means first get the data from the image and then decrypt the image using the decryption key. Extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved

Earlier no system existed to cater to the needs of 'Secure Infrastructure Implementation System'. The current system developed is technically feasible. It is a browser based user interface for audit workflow. Thus it provides an easy access to the users. The database's purpose is to create, establish and maintain a workflow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified.

II PROBLEM DEFINITION AND DESCRIPTION

Steganography ,it is defined as the art and science of hiding information, which is a process that involves hiding a message in an appropriate carrier for example an text file [1]. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message.

Steganography is a general term referring to all methods for the embedding of additional content into some form of carrier the choice of the carrier is nearly unlimited; it may be an ancient pieces of parchment, as well as a network protocol header .Present day methods are far more sophisticated than their ancient predecessors, but the main principles had remained unchanged [2].

III REVIEW OF LITERATURE

A)Message /Information Formats

1. Physical Steganography- Hidden message within wax tablets, on messenger's body [3].
2. Digital Steganography- Concealing messages within the lowest bits of noisy images or sound files, image bit-plane complexity segmentation steganography

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

3. Network Steganography- The concealment ofmessages in Voice-over-IP conversations.
4. Printed Steganography- The plaintext, may be firstencrypted by traditional means, producing a ciphertext.
Then, an innocuous covertext is modified in some wayso as to contain the ciphertext, resulting in thestegotext [4].
5. Text Steganography- Data compression.

B)Noise floor consistency analysis

In some cases, such as when only a single image is available, more complicated analysis techniques may be required [5].

In general, steganography attempts to make distortion to the carrier indistinguishable from the carrier's noise floor. In practice, however, this is often improperly simplified to deciding to make the modifications to the carrier resemble white noise as closely as possible, rather than analyzing, modelling and then consistently emulating the actual noise characteristics of the carrier [6].

In particular, many simple steganographic systems simply modify the least-significant bit (LSB) of a sample; this causes the modified samples to have not only different noise profiles than unmodified samples, but also for their LSBs to have different noise profiles than could be expected from analysis of their higher-order bits, which will still show some amount of noise [7]. Such LSB-only modification can be detected with appropriate algorithms, in some cases detecting encoding densities as low as 1% with reasonable reliability.

C)Hiding information inside image

It is a popular technique nowadays. An image with a secret message inside can easily be spread over the world wide web or in newsgroups [8].

The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited [9].

To hide a message inside an image without changing its visible properties, the covers Source can be altered in ”noisy” areas with many colors variations, so less attention will be drawn to the modifications [10].

The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformation the cover image. These techniques can be used with varying degrees of success on different types of image files [11-12].

IV.SYSTEM DESIGN

The users or nodes involved are Sender, Intermediate and Receiver. In order to send file, the sender has to find out the list of nodes which are connected with the sender [13].

From that available list he can choose receiver. According to the figure 4.1 the sender has to analyze the performance of each and every node which is connected with the sender.

The performance analysis list will return the priority based result so that sender can choose the intermediate to send the file. The Intermediate will receive the file from sender then it will analyze the performance so that it can send data to another intermediate or receiver [14-15].

In the receiver side, the receiver has to select the file path to receive the file from sender or intermediate. Then the receiver can view the received file.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

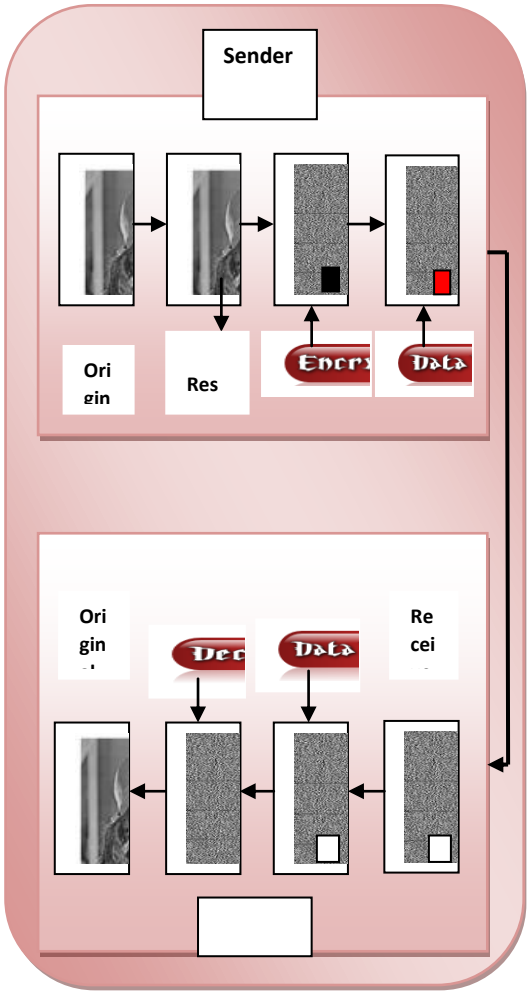

Fig 4.1 Design View of Encryption

V .PROCESS DESCRIPTION

A) Authentication

User want to register the personal details in the database and get the authentication processes to go forward. In the fig 5.1 User want to give the database to admin all the registration process is done by a admin [16]. After the registration process completed User can get the authentication permission, by using username and password login website. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

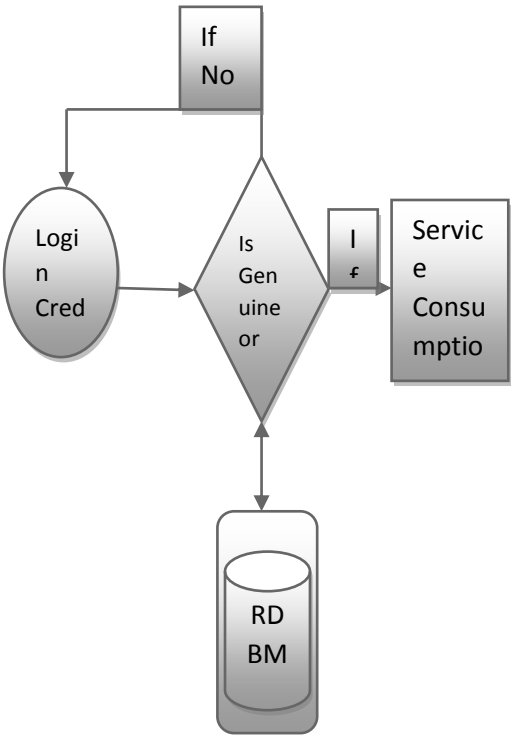

Fig 5.1 Authentication view

B)Choose Image and Reserve Location

After login the user application, it will enter to choose image window as shown in the fig 5.2. So we have to browse the images from the Database. And then reserve some pixel of that image

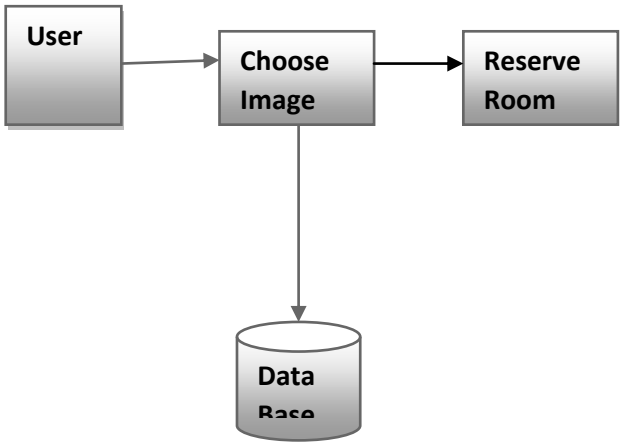

Fig 5.2 Image and Reservation view

C) Reserve room

After login the user application, it will enter to choose image window. So we have to browse the images from the Database shown in the fig 5.3. And then reserve some pixel of that image

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

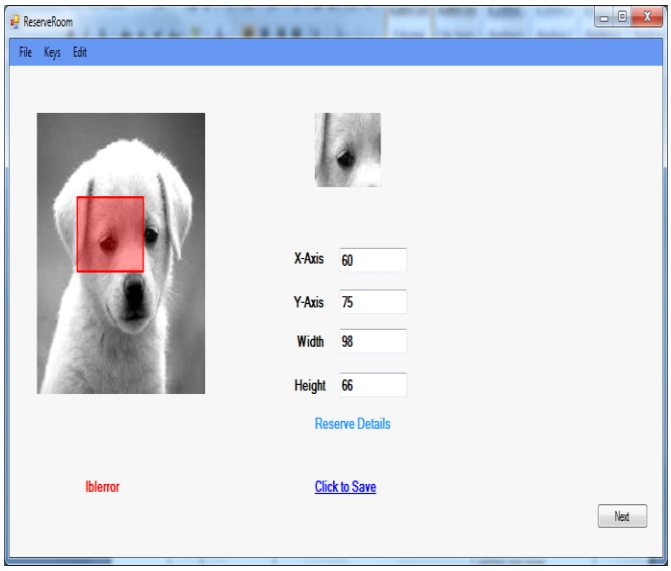

Fig 5.3 Reserve Room process

D)Encrypt the Image

In the fig 5.4the encryption image having the reserve location, so we have to embed the data in that location using the data hiding key

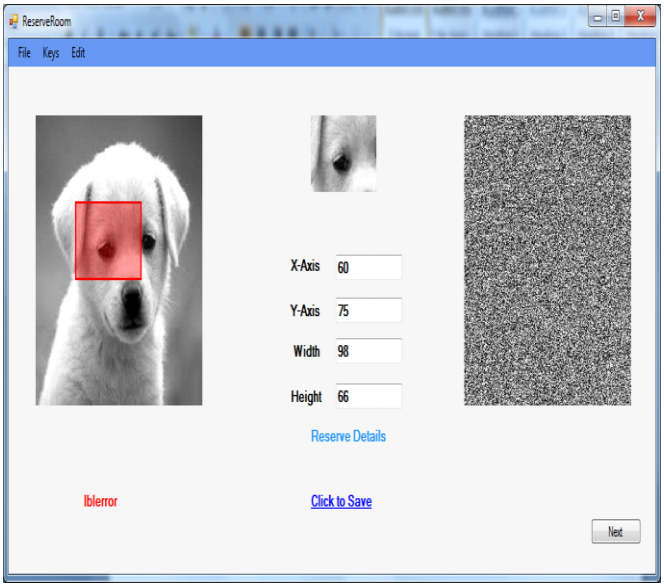

Fig 5.4 Encrypt image

Here is a simple algorithm for binary (black and white) visual cryptography that creates 2 encrypted images from an original unencrypted image.

The algorithm is as follows: First create an image of random pixels the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color.

Where a pixel of the original image is different than the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the same color as the corresponding pixel of the first encrypted image. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.

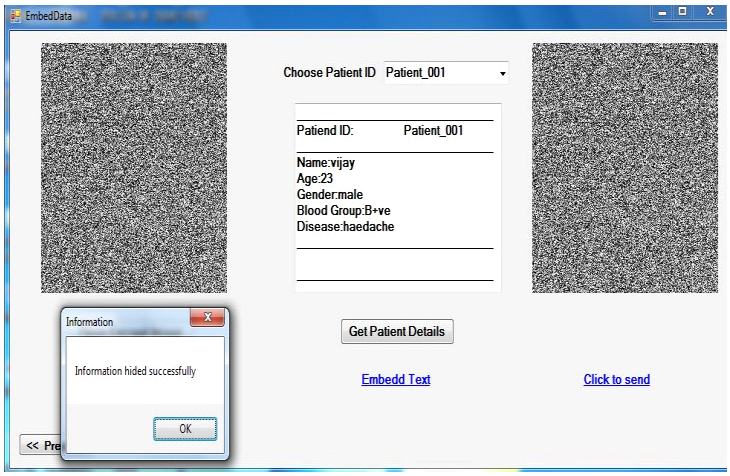

Fig 5.5 Human information Details

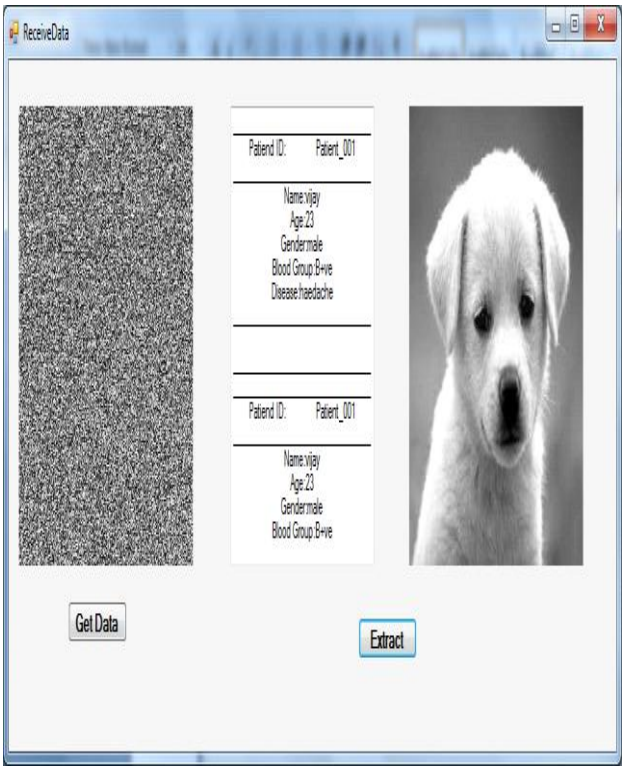

Fig 5.6 Receiving Image format

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

VI CONCLUSIONS

Thus vacate room technique that the system result is inefficient because embedded data and cover images loss some information. The present we have to use reversible reserve room before encryption. The proposed method can take advantage of RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, in this method achieve real reversibility and lossless data. extend this work in several directions. In proposed system we have to hide the data in the reservation room. But, in our future, before hiding the data we have to encrypt the text and then hide. So it will be improve the security level.

REFERENCES

[1] 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.
[2] Niranjan U., Subramanyam R.B.V., Khanaa V., "Developing a Web Recommendation System Based on Closed Sequential Patterns", Communications in Computer and Information Science, ISSN : 1865-0929, 101() (2010) PP.171-179.
[3] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.
[4] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[5] Beula Devamalar P.M., Thulasi Bai V., Srivatsa S.K., "Design and architecture of real time web-centric tele health diabetes diagnosis expert system", International Journal of Medical Engineering and Informatics, ISSN : 1755-0661, 1(3) (2009) PP.307-317.
[6] 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.
[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[8] Lydia Caroline M., Vasudevan S.,"Growth and characterization of l-phenylalanine nitric acid, a new organic nonlinear optical material", Materials Letters, ISSN : 0167-577X, 63(1) (2009) pp. 41-44.
[9] 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.
[10] 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.
[11] Das S., Das M.P., Das J., "Fabrication of porous chitosan/silver nanocomposite film and its bactericidal efficacy against multi-drug resistant (MDR) clinical isolates", Journal of Pharmacy Research, ISSN : 0974-6943, 6(1) (2013) PP. 11-15.
[12] 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. "Distributed Steganography". IEEE. October 2011.
[13] "Method and apparatus of performing distributed steganography of a data message". US Patent Office. 3 September 2013.
[14] Sharmila S., Jeyanthi Rebecca L., Saduzzaman M., "Biodegradation of domestic effluent using different solvent extracts of Murraya koenigii", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) PP.279-282.
[15] Jane Wakefield (9 January 2014). "Cicada 3301: The dark net treasure trail reopens". BBC News. Retrieved 11 January 2014. 1129–1143, 2009
[16] Data Hiding Using Steganography For Network International Journal of Advanced Research in Computer and Communication EngineeringVol. 3, Issue 2, February 2014Copyright to IJARCCE www.ijarcce.com 5740
[17] B Karthik, TVU Kirankumar, MS Raj, E BharathKumaran,Simulation and Implementation of Speech Compression Algorithm in VLSI, Middle-East Journal of Scientific Research 20 (9), PP 1091-1092, 2013
[18] M.Sundararajan & R.Pugazhanthi," Human finger print recognition based biometric security using wavelet analysis", Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).
[19] .M.Sundararajan & E.Kanniga," Modeling and Characterization of DCO using Pass Transistor", proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)
[20] .M.Sundararajan & C.Lakshmi, "Wavelet based finger print identification for effective biometric security", Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.
[21] .M.Sundararajan, "Optical Instrument for correlative analysis of human ECG and Breathing Signal" Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-I
[22] M.Sundararajan, C.Lakshmi & D.Malathi, "Performance Analysis Restoration filter for satellite Images" Publications of Research Journal of Computer Systems