International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 6 (Nov-Dec 2016), PP.93-98

Data Storage Security Using Steganography Techniques

[1] Nancy Garg, [2] Kamalinder Kaur
[1,2] Computer Science Of Engineering And Technology, Chandigarh Engineering College , IK Gujral Punjab Technical University, LANDRAN, INDIA
[1] nancygarg04@gmail.com

***Abstract*— Cloud computing is an advanced technology throughout the world. As cloud computing is based on Internet which is a computer technology. The computer store in the available space and whenever it is requested by the authenticated user it retrieve the stored information. Measures of security that are assumed in the cloud should be made available to the customers for gaining their trust. Steganography is used to hide data. First acquire an image from various sources and will read the required details of an image. After that secret data is read and is converted into integer values. Then it is encrypted and embedded with the cover image with the use of transform method. Security of the embedded data can be enhanced by the steganography model. The main problem with conventional key cryptography is that it is a very hard job to keep symmetric key safe from people other than sender and receiver. The single layered XOR operation based encryption model is considered very weak against several cryptanalysis attacks to decode the encrypted data without using the encryption key. The frequency embedding method has been designed to overcome all such problems.This technique has implemented using Progressive Exponential Clustering algorithm. The performance parameters such as Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) are used for the result evaluation of the proposed model.**

***Keywords*— Steganography, Least Significant Bit, Embedding Algorithm, Pseudo Random, Progressive Exponential Clustering algorithm.**

I. INTRODUCTION

Cloud computing is an advanced technology throughout the world. As cloud computing is based on Internet which is a computer technology. Firms like Amazon, Microsoft and Google to speed up their business have implemented the "CLOUD". Cloud computing has given a new shape to the (SaaS, PaaS and IaaS) and provide cheaper powerful processor with these computing architecture. The computer store in the available space and whenever it is requested by the authenticated user it retrieve the stored information1. We can store any kind of data that we use in our day to day life such as photographs, songs, or movies and huge amounts of confidential data. These are the basic service which is offered by cloud computing. So Cloud is a pool of computing service on large scale .Now days users can subscribe even high quality data and software services that reside on remote data centers due to the increasing network bandwidth and reliability yet flexible networkconnections2.

The Steganography helps in hiding the message in such a way that it cannot be seen .However, Cryptography systems can be classified into public-key systems and symmetric-key systems .Public key system uses two keys that is public key which is known to everyone and private key which is used by only the recipient of messages. Symmetric key system use a single key that both the receiver and the sender have .In process of Cryptography, a cipher message, may provoke suspicion on the behalf of the recipient while message which is invisible created with method of steganography will not. However, when the use of cryptography is illegal ,then steganography is useful .However, cryptography and steganography are judged in a different way. When the "enemy" can access the data Cryptography fails, while when the "enemy" detects in the steganographic medium that there is a message that is secret is present then steganography fails 3. Security of the embedded data can be enhanced by the combination of these two methods. This combination of two methods will satisfy the various requirements as , security, capacity and robustness for secure transmission of data over channel that is open. Although both methods are providing the security individually , to provide strong security we proposes to combine both method steganography and cryptography into one system, by using data encryption at two levels . After the encryption of data is done, the encrypted text will be hidden behind the image using steganographic technique that is least significant bit(LSB).

A. Steganography

Steganography is mostly confused with method of cryptography, though they are two different fields. Cryptography is the process of using a key or password making the message in the readable format. Steganography hides the fact of presence of message that is secret. In the world of today due to lack of privacy Steganography field is a very important. People communicate with each other without scrutiny of each other through Steganography, because everyone involved in communication unaware about the encoding of secret message.

B. Hiding data using steganography

For hiding a message along a digital message, we take use the least significant bit within each image pixel. Value of color in each image is stored in each pixel of image which is made of three eight bit integers. For example, 255 green, 255 red,and 0 blue makes the yellow color. It is possible to hide a secret message by replacing in each of the color values the LSB.It is also possible to hide a message that is secret, without changing the values of color too much,bit by bit.

C. Types of steganography

.

A .Text Steganography This process considers the various letters positions . The amount of content that is hidden in text type is too less and can be easily made recoverable by letters frequency. There are many methods which are used as text steganography such as Oldest technique in which Text is used as a cover medium . Message which is Secret can be detected by taking the file's every word first letter.Hiding of text in hypertext mark-up languages (HTML),Text Steganography in word's specific characters, method of Line shifting ,Open spaces ,Shifting of Word , Encoding of Character 4 .

B. Image Steganography Various calculations are used by people now a days. Image pixels are selected randomly and then replacing the text ASCII values is unbreakable algorithm. Cryptography and Steganography joins its hand to make the Steganography of image more robust .We see that human get attracted towards images more than text. Pages of Internet are popular due to its attractive pictures. Change in the LSB of the image goes unnoticed by an human eye .Using this concept secret information is hidden in the images5.

C. Audio Steganography This is another method where Steganographers focus in these audio files for their secret message. Digital files are used to conceal message. In the day today life people hears music. People downloads free music from internet through mobile phones ,PDA, and pc which the popular music files . There are few techniques for embedding the data secretly into digital audio such as Phase coding,LSB coding, spread spectrum,Parity coding.

D. Protocol Steganography Protocol is defined as a set of rules which is used for governing the communication . Some of the protocols are IP, TCP, UDP which are used for communication. This protocols are used by Steganographers to hide their secret data. Parts of the protocol packet header which are unused are efficiently used for hiding the message6.

D. METHODS OF STEGANOGRAPHY

Images are categorized according to the number of bits in a pixel. In monochrome images there is one bit per pixel . The message are hidden in images. Gray scale images can be displayed by using two bits per pixel. Pictures with 256 colours can be displayed with eight bits per pixel. Full colour or true colour system with twenty four bits per pixel is used to display millions of colours .Various image steganography techniques are as follows7.

A Spatial Domain To hide the message LSB technique is widely used. Image pixels are either selected sequentially or randomly. Steganography is made stronger by the encrypting the data and hiding in the LSB. Pixel values are changed in spatial domain technique of image Steganography. To hide the secret data Least Significant Bits (LSB) are changed. Change in the LSB which results in the image distortion is not noticed by the human eye. To hide the data which is based on the value of intensity MSB are used. To make it difficult for the intruder for recovering the text from message key is also embedded in the image.

B Masking and Filtering During early days only gray scale images are used. In this type MSB bits are used. Lossy compression of images are efficiently used.

C Transform Domain Technique This method uses the MSB for data hiding. There is no dependency on the image formats7. The technique Transform domain is more robust than LSB because it focus on the parts of the image that are not changed by editing of image like resizing ,cropping. This technique works in both lossless and lossy compression images.

II. RELATED WORK

Premkumar Jain,Manoj Kokane, Poonam Sarangdhar [2013]: In this paper some services are proposed for security of data and access control of data which is sensitive and outsourced on server of cloud for sharing. In this paper two issues are addressed which are policies for accessing attributes of data is defined and enforced and other owner of data is allowed for assigning the task of computation to the cloud server which is untrusted without disclosure of any content of data. For further achieving a secure and dependable service of cloud storage, in this paper a auditing mechanism for flexible storage integrity which is distributed in nature, using the token which is homomorphic and data which is distributed coded is proposed. Dynamic operations of data is supported effectively. It is important to locate the server which misbehaves so that users could access the sensitive data without doing any changes. This system is fullproof for crash of data and attack on server.

Nikita pathrabe, Deepali khtawar [2014]:In this paper mechanism is proposed to prevent unauthorized access of data which is stored on cloud server.For providing the data security in cloud distributed scheme using token that is homomorphic is used.Security mechanisms for ensuring the data integrity means as the cloud supports redundancy of data where user can insert ,update or delete the data.This paper also proposed the scheme for securing the data when server misbehaves. The main focus is on ensuring the security of data storage on cloud which is the essential aspect of QOS.

Deepanchakaravarthi, Dr.Sunitha Abburu and Purushothaman[2012]; The main purpose of this purpose is to prevent data from access which is unauthorized.The security of data is provided with scheme which is distributed in nature.Any tempering with the data at cloud server is identified.Attacks which are collusion are also avoided when made my users which are unauthorized.

Shwetha Bindu, B. Yadaiah[2011]:This papers deals with the study of data security problem in data storage at cloud server.To ensure the user correctness of data storage in cloud effectual scheme with dynamic support of data including erase ,block revise code and affix.The erasure correcting code technique is used for preparing the file distribution for provision of parity vectors redundancy and guarantee of data dependability.This scheme achieves the integration of insurance of storage correctness and detects the corruption of data during the verification of storage correctness across the servers which are distributed.This scheme is resilient and efficient to failure of Byzantine ,attacks of server colluding modification of malicious data .

Humanth Kumar, M.Shareef, R. P. Kumar[2013] :In this paper metbod is introduced where the technique of wavelet transform is used to compress the message message that is secret and LSB is used to embed it in the cover image where message that is secret is inserted into the image by the use of generator of random number8.

S.Ashwin, J.Ramesh, K.Gunavathi[2012]:In this paper various image steganography technologies are proposed.It represents the review of hiding message in transform and spatial domain.It also propose the technique of detecting the image or message that is secret i.e.staganalysis9.

Rosziati Ibrahim and Teoh Suk Kuan [2011]: In this paper there is proposed a system with security mechanisms of two layers by procedure of login, in which first username and password is needed and once done with login , for embedding the secret data key is used. For this, privacy and integrity is maintained10.

Danwei Chen,Yanjun He [2010]:The strategy for secure data storage in cloud computing is proposed in this paper.Based on algebra's k equations theory,In theory of elementary number ,principle of surplus of n congruence and abhishek's algorithm for storage of data online.Based on fundamental theories of k equations in algebra, n congruence surplus principle in theory of elementary number , and the Abhishek's algorithm for online data storage .In this strategy algorithm of data splitting is used for splitting the data d into k sections , it ensures high security of data by simplifying solutions of k equation , and reliability of data is guaranteed using the coefficients which is generated by splitting algorithm.

Shailender Gupta, Ankur Goyal and Bharat Bhushan[2012]: In this paper the technique is proposed by author using cryptography and LSB steganograph where the information that is secret is encrypted using Diffie Hellman or RSA algorithm before embedding in image with the help method of LSB. With this technique, complexity of time is increased but at that cost high security is achieved 15.

K.Sakthisudhan , P.Prabhu [2012]: In this paper author used the idea of dual security, in which firstly secret data is converted to form that is encrypted and then steganography technique LSB is used for embedding it in cover object.With this method, message is transferred with high security and can be easily retrieved without any data loss 17.

III. PROBLEM FORMULATION

The main problem with the exiting model exists in the Steganography application and the data encryption process. The existing model has been evaluated thoroughly for its core problems. The main problem with conventional key cryptography is that it is a very hard job to keep symmetric key safe from people other than sender and receiver. If sender and receiver are far away from each other and they have not shared secret key, then third party or courier must be trustworthy to transfer the key to the intended receiver only. Also the existing model is based upon the sequential bit encoding with the fixed pattern, which always makes it vulnerable to staganalysis attacks. In the case of encryption, this model is not secure as it uses the single layered XOR operations for the encryption process. The single layered XOR operation based encryption model is considered very weak against several cryptanalysis attacks to decode the encrypted data without using the encryption key. The frequency embedding method has been designed to overcome all such problems.This technique has implemented using Progressive Exponential Clustering algorithm. In this algorithm,

1. The first step is that the clusters are created based on color pattern matching. For pairing up the pixel of same colour an exhaustive search is conducted within a cluster. Each pixel, is included in cluster which is similar in color within value of threshold.
2. After the clusters are created, then depending upon the cluster of color ,their table of colour is created.
3. Two or more clusters can be of same size is very rare, therefore, the cluster, with large number of pixels, is chosen so that space of embedding should be as large as possible.
4. Embedding a larger message is very useful. After embedding the message into the cluster, the generated stegno-image can be sent securily over the Internet. The general principle of this algorithm is as follows:

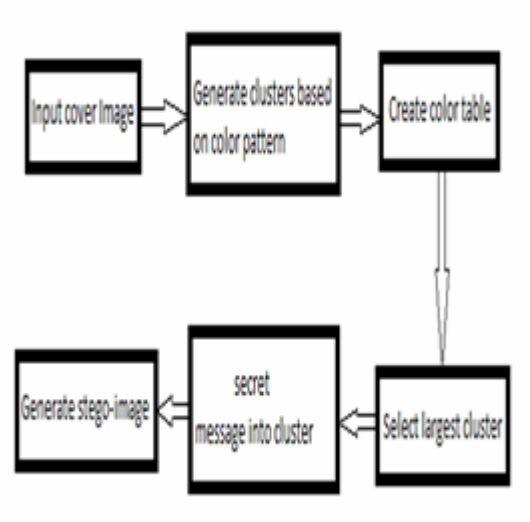


Fig.1.1: General Principle of proposed model's embedding region selection algorithm

A. Matching Pixel Selection

The frame selection is the procedure the selecting the matching pixel in the input image. The image is at first extracted into the different segments. The segments are extracted and saved in the given folder as the images. The hidden image is loaded into the memory, and matched against all of the frames one by one. The similarity matrix is prepared, which lists the frame index and similarity percentage. The frame matching and frame selection algorithm is listed as per following:

Algorithm 1: Matching Segment selection algorithm

1. Load the input Image
2. Extract the segments into small parts
3. The frames are saved in the given folder
4. Load the hidden image
5. Start the iteration with counter set at 1

6. Match the frame against the hidden image using the cross correlation
7. Update the similarity matrix
8. If it is last frame
1. Exit the iteration
9. Else
1. Go to line 6
10. End the iteration
11. Return the matching frame id

IV. PROPOSED SYSTEM

The random pattern based embedding method has implemented using Pseudo Random Embedding algorithm for the detection of the similar region to find the best match region within the given segment of the given image. In this algorithm we are primarily doing the following steps:

- At first, the image is selected and is loaded into the run-time memory.
- Then, the image data is divided into segments and the segment is loaded into the memory at read stage.
- Now the secret object is selected and will be loaded into the run time memory.
- After selecting the secret object, it is converted into the encrypted form using the symmetric XOR encryption key. After that the data that is hidden is compared against each data frame of video and will return the most similar matrix.
- Now the condition that whether the size of hidden object is more than the matching data matrix; if it returns yes, then the object is embedded in the cover object frame and will return the stegno object where the secret image is hidden.
- If it returns no, then divide the video data into parts and hide the ith part of the data into the frame.

V.SYSTEM DESIGN

5.1 Objectives of the Hybrid Data Security Model

- To hide a message in an object where the hidden message will not be visible to an observer.
- To deliver digital data with high speed speed networks.
- To implement easily encoding and decoding of message data sequentially from point of starting that is pixel in the upper left in a set of pattern unvarying to the pixels adjacent to each other.
- Pseudo-Random Decoding is less time consuming and more efficient because the grouping set of pixel location is calculated only once during the whole process instead of using counters that is ever changing during recovery.

In our research work we are using steganography of digital image because these digital images have a large amount of data that is redundant and this the reason which makes it possible for hiding the message inside file of image . Following elements are required for Image Steganography:

- Cover medium: Secret message is stored on cover medium image.
- The Secret message: The message that is to be transmitted. It can be encrypted or plain images ,text or any other data.
- The Stego-key: it is the key which is used to hide the message (It May or may not be used).

In the cover medium nobody notices the presence of data that is hidden in it .For hiding the communication existence is the main steganography motive .

V. MAIN ALGORITHM DESIGN

The algorithm for the frequency embedding method is as described below. It consists of following primary steps:

Algorithm 1: Main Algorithm

USER INPUT: PHASE 1

1. Input the text data
2. Obtain the text data and restructure it for conversion
3. Create a white image of size 256x256 to 512x512
4. Insert the text to the white canvas of the image
5. Return the secret image

USER INPUT: PHASE 2

6. Input the image data
7. Acquire the image data
8. Convert the image data to gray scale
9. Return the secret image

MAIN ALGORITHM

10. Select the target video data
11. Acquire the video data
12. Extract the frames of video data
13. Run the validation check
14. If the size of the secret image is higher than cover frame

1.1. Segment the image into multiple blocks to satisfy the size based validation check

1.2. Return the image blocks

15. Otherwise

1.3. Return the image in single block

16. Run the iteration for each block

1.4. Run the similarity matching between the video frames and the current block i

17. Load the secret image data into the run-time memory and convert to the double type.
18. Load the image segments in the iteration to the run-time memory and convert all to the double type matrix.
19. Select the cover segment from the image data
20. Prompt the user to enter the encryption key
21. Encrypt the image data using the Elliptic Curve Cryptography
22. Prompt the user to enter the random seed pixel
23. Embed the image in the select frame
24. If it's the last block

1.5. Break the iteration

25. Otherwise

1.6. GOTO step 16

26. Reassemble the image data
27. Return the image data
28. Compute the performance parameters of PSNR and MSE.

VI. EMBEDDING ALGORITHM

The design of the data-embedding algorithm has been discussed in detail in the following algorithm:

Algorithm 2: Image-data Embedding Algorithm

1. Assign the header set
1. Create the random permutation set
2 . If the dimensions of the image are divisible by 4
1. Pass the image to the program
3 . Otherwise
1. Pad the image to satisfy the condition
2.Pass the image to the program
2. Acquire the canvas image
3. Initialize the randomizer (Random number generation) for the random pixel position based selection
4. Determine the image size of embedding
5. If the image size validation check satisfies
1. Run the program
6. Otherwise
1. Return the program
7. Create the random pixel set
8. Arrange the final pixel groupings with the 3 pixels in each group
9. Initialize Random Number Generator to a "Common" State.
10. Initialize the header holder set
11. Start the 1-bit embedding methods

1.Embed the initial 3 header values from RGB pixels
2.Embed the next 3 header values for the BGR
3.Embed the next 2 from the RG

12. Embed the data using the RGBBGRRG pattern in the randomly selected pixels.

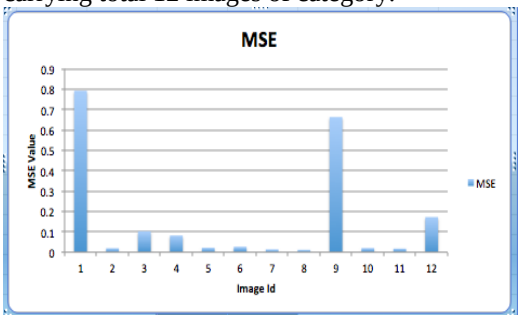
VII. RESULT AND DISCUSSIONS

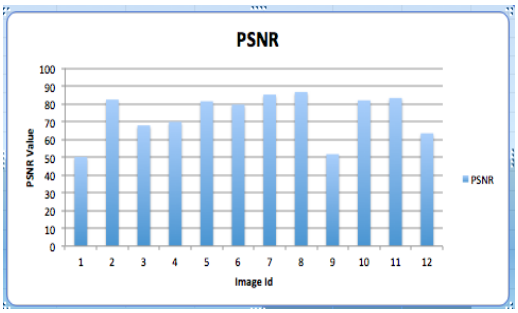
The proposed model has been proposed for the steganography of the text data into the image data obtained in the form of 2-D of 3-D images. The random embedding method has been utilized to embed the secret text data into the image data. The proposed random embedding is based upon the random embedding method, which utilizes the initial frequency based region evaluation for the decision of embedding into the cover image. The MATLAB tool has been utilized for the purpose embedding the text and images. Research work of this thesis in such a manner that outcome will be a selection of highly optimized parametric algorithm which would help to form a securable data storage.

The results of the proposed model have been obtained of the given dataset in the form of the image quality parameters of MSE and PSNR. The dataset has been primarily divided into the three parts on the basis of the definitive distinction between the image samples. The first phase of the results covers the results obtained with the sub data type of benign tumors. The following table 1 shows the results obtained from the benign tumor dataset.

Image ID	PSNR	MSE
1	50.15345	0.79226
2	82.38428	0.019379
3	67.87628	0.102974
4	69.87347	0.081821
5	81.4081	0.021684
6	79.56421	0.026812
7	85.19488	0.014022
8	86.66014	0.011845
9	51.69801	0.663192
10	81.94987	0.020373
11	83.28821	0.017463
12	63.40088	0.172384

The above table 1 is representing the results of the proposed algorithm on the selected image dataset. The image dataset is carrying total 12 images of category.





CONCLUSIONS

Messages that are Hidden remain an evolving and important science for facilitating the transmission of information securily Techniques and process of Steganography exploits limitations of detection in the visual system of human for storing messages in redundant /underutilized bits which is used by digital media. The proposed model has been proposed for the steganography of the text data into the image data obtained in the form of 2-D of 3-D images. The random embedding method has been utilized to embed the secret text data into the image data. The proposed random embedding is based upon the random embedding method, which utilizes the initial frequency based region evaluation for the decision of embedding into the cover image. The MATLAB tool has been utilized for the purpose embedding the text and images. The data can be stored securily with the hybrid storage scheme.

REFERENCES

[1] Deepanchakaravarthi,Purushothamanaand Dr.Sunitha Abburu : An Approach for Data Storage Security in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012

[2] B. Shwetha Bindu, B. Yadaiah:Secure Data Storage In Cloud Computing, ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 63-73.

[3] R.Nivedhitha ,Dr.T.Meyyappan:Image security using steganography and cryptographic techniques, International Journal of Engineering Trends, and Technology- Volume3 Issue3- 2012.

[4] http://www.enggjournals.com/ijet/docs/IJET13-05-02-034.pdf study on image steganography techniques C. Gayatri, V.Kalpana computer science & engineering, school of computing SASTRAUNIVERSITY, Timalaisamudram.

[5] Vijay kumar sharma, Vishal srivastava "A steganography Algorithm for hiding image in image by improved lsb substitution by minimize detection" journal of theoretical and applied information technology 15th february 2012. vol. 36 no.1

[6] Mr.R.V. Kiran Kumar, Mr. T. Kishore Babu, Mr. S .Vikrama Teja: A novel method for image steganography with cryptography, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 11, November 2014

[7] Dr. Ekta Walia a, Payal Jain "An Analysis of LSB & DCT based Steganography",Global Journal of Computer Science and Technology, 4 Vol. 10 Issue 1 (Ver 1.0), April 2010,

[8] Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Pwer and Computing Technologies, March 2013, pp. 1197- 1200.

[9] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, Dec 2012, pp. 171-177.

[10] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, vol. 2, pp. 102-108, 2011

[11] N. Provos, P. Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Computer Security 2003, <http://www.citi.umich.edu/u/provos/papers/practical.pdf>.

[12] J. C. Judge, Steganography: Past, Present, Future, SANS Institute, <http://www.sans.org/reading_room/whitepapers/stenganography/steganography-past-present-future_552>

[13] S. Singh, The Code Book, Anchor Books, 2000, ISBN: 0385495323.

[14] J.Rittinghouse,J.Ransome, Cloud Computing: Implementation, Management, and Security, 2009 .

[15] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" International Journal Modern Education and Computer Science, vol. 6, pp. 27-34, 2012

[16] Prasanta GogoiB, Borah,D K Bhattacharyya, Anomaly Detection Analysis of Intrusion Data using Supervised & Unsupervised Approach, Journal of AICIT, AICIT, vol.5, no.1, pp.95-111, 2010.

[17] K.Sakthisudhan, P.Prabhu, "Dual Steganography Approach for Secure Data Communication" International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, vol. 38, pp. 412-417, 2012.