Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 9 (2017) pp. 2737-2744
© Research India Publications
http://www.ripublication.com

A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography

D.Suneetha

Research Scholar, Krishna University, A.P, India.

Dr. R. Kiran Kumar

Asst Professor, Krishna University, A.P, India.

Abstract

The Cloud Computing is a dynamic term, which provides dispute free data outsourcing facility which prevent the user from burdens of local storage issues. However, security is perceived as a biggest issue and poses new challenges related to providing secure and reliable data archive over unreliable service providers. To provide the solution to these issues there are n number of ways. Steganography is one of the most powerful and existing technique to conceal the existence of secret data inside a cover object. Images are the most popular and useful cover objects for steganography and in this work image steganography is adopted. There are several existing techniques to conceal information inside cover image. The least significant bit (LSB) is the one of the main technique in spatial domain image steganography. In this work a new technique of LSB steganography has been proposed by considering LSB and MSB pixels for hiding and retrieval of the data which is an improvised version of one bit LSB technique. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

Keywords: Cloud Computing, Data Storage Security, LSB, Data hiding, Steganography, PSNR, MSE

I. INTRODUCTION

Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. The pioneer of cloud computing vendors, Amazon Simple Storage Services (S3) and Amazon Elastic Compute Cloud (EC2) are well known example. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It also allows developer to access the highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network web services. From the viewpoint of data security which has been an important aspect of quality of services, cloud computing unavoidably poses new challenging security threats for number of reasons. Firstly, we cannot adopt the traditional cryptographic primitives for the purpose of data security in cloud computing as the user' loss their data control. So, we need a data verification strategy but without explicit knowledge of the whole data, it is very hard to verify the correct data. Considering various kinds of data for each user, stored in the cloud and demand of the long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, it is not a just third-party data warehouse. The data stored in the cloud may be frequently updated by the user, including insertion, deletion, modification, appending, recovering, etc. So, for this dynamic operation, it needs to be more advanced technology to prevent data loss from the cloud data storage centers. Last but not the least data centers are running in a simultaneously, cooperated and in distributed manner. Every user' data is stored in multiple physical locations randomly. Therefore distributed protocols for storage correctness assurance will be most importance in achieving a robust and secure cloud data storage system in the real word.

Steganography is the process of hiding of a secret data within an ordinary message and the extraction of it at its destination. Steganography takes a step farther by hiding an encrypted message so no one suspects than cryptography. Steganography and cryptography are two different information hiding techniques, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. It relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye.

II. EXISTING METHODS

The least significant bit steganography is one such technique in which LSB of the image is replaced with data bit. Several algorithms have been proposed to address the problem in this section we discuss some of these algorithms Vignesh Kumar Munirajan, Eric Cole, Sandy Ring in Steganography is a means of data hiding in images for covert transmission. Even though these alterations may not be captured by visual observation, they do manifest themselves for detailed analysis Random least significant bit embedding (RLSB): In this the data is hidden randomly i.e. data is hidden in some random selected pixel. Random pixel is selected by using Fibonacci algorithm. The fatal drawback of RLSB embedding is every one well familiar with Fibonacci series and easy to decrypt the original message.

EDGE least significant bit embedding (ELSB): In ELSB we use all the edge pixels in an image. Here we consider two LSB bits in the cover image, then we identity the edge pixel based on that insert original message on to it. The values of PSNR and MSE ratio were very high. The proposed method reduces the noise ratio when compared to previous existing algorithms.

III. PROPOSED METHOD

In this method, odd pixels are extracted, first and last bits of image are extracted from pixels values of an image. The possible combination of these two bits are 00, 01, 10 and11. If we want to embed 0 and the combination are 01 and 10 then 0 is embedded but if the combination are 00 and 11 then they are made 00 or 11 by adding or subtracting 1 from the least significant bit.If the data bit is 0 and the combinations are 01 and 10 then the data bit is embedded otherwise if the combinations are 00 and 11 they are made 01 and 10 by performing bitor operation. If the data bit is 1 and the combinations are 00 and 11 then the data bit is embedded otherwise if the combinations are 01 and 10 they are made 00 and 11 by performing bitxor operation.

III.1. ALGORITHM FOR INSERTION OF MESSAGE

Step1: Start.

Step2: Import image using imread() function

Step3: Select image and convert into gray scale using formula rgb2gray.

Step4:Get the pixel location and select odd pixel

Step5: select the first and last bit of the pixel

Step6: If we want to insert 0 then go to step7 (a) otherwise step 7 (b)

Step 7: (a) If bits are 01or 10 then insert then no change is required message bit is already there.

(b) If bits are 00 and11 make them 01or 10 by adding or subtracting 1.

Step8: If we want to insert 1then go to step9(a) otherwise step9(b)

Step 9:(a) If bits are 00or 11then insert then no change is required message bit is already there.

(b) If bits are 01 and10make them 00or 11 by adding or subtracting 1.

(v)stop

III.2.ALGORITHM FOR RETRIEVAL OF MESSAGE

Step1: Start

Step2: Import stego image using imread() function

Step3: Select image and convert into gray scale using formula rgb2gray.

Step4:Get the pixel location and select odd pixel

Step5: select the first and last bit of the pixel

Step6: if first and last bits are 00 or 11 then message bit is 1

b) If first and last bits are 01 or 10 then message bit is 0

Step7: Repeat the process until all bits retrieved.

Step8: stop

IV. RESULTS

There are mainly different steps involved in implementation Conversion of image to matrix from. In this process of image to matrix first we convert the input cover image into matrix values which is stored in a text file. Firstly an image is read from computer, the original image is in the form of RGB which is converted into gray scale image.

Original image:

b) Embedding Process: After completion of image to matrix the next step is to embed a message into an image . the image obtained during this process is called stego image.

Stego image:

Table 1: Change in pixel value after insertion of ‘1’

Decimal value	**Pixel value before insertion**	**Pixel value after insertion**	**Change in Pixel Value & Comment**
1	00000001	00000000	-1 insert
3	00000011	00000010	-1 ,Insert
5	00000101	00000100	-1,insert
7	00000111	00000110	-1,insert
9	00001001	00001000	-1,insert
11	00001011	00001010	-1,insert
13	00001101	000011010	-1,insert
15	00001111	000011110	-1,insert
-			
-			
127	01111111	01111110	-1,insert
-			
255	111111111	111111111	NC, Insert

Table 2: Change in pixel value after insertion of ‘0’

Decimal value	Pixel value before insertion	Pixel value after insertion	Change in Pixel Value & Comment
1	00000001	00000001	NC ,insert
3	00000011	00000011	NC ,Insert
5	00000101	00000101	NC,insert
7	00000111	00000111	NC,insert
9	00001001	00001000	NC,insert
11	00001011	00001011	NC,insert
13	00001101	00001101	NC,insert
15	00001111	00001111	NC,insert
-			
-			
127	01111111	01111111	NC,insert
-			
255	111111111	111111111	NC, Insert

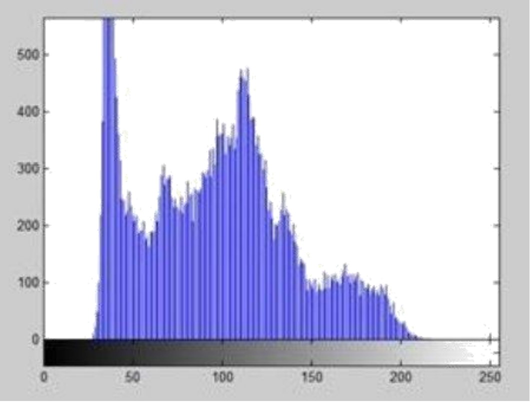

Fig 1 a) Histogram of Original Image

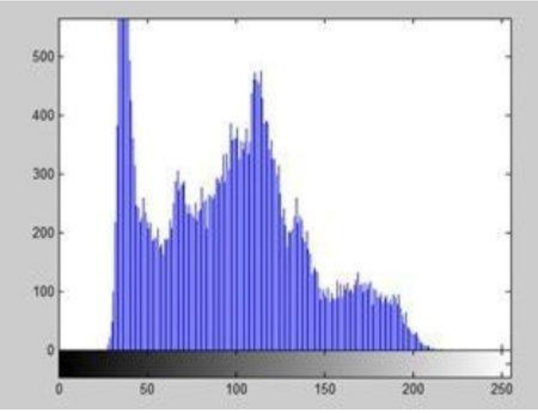

Fig 1b) Histogram of Stego Image

PSNR between Image (1) and Image (2) = +43.01

MSE between Image (1) and Image (2) = 0.0075

V. CONCLUSION

In this paper, we have investigated the problem of security in cloud computing, which is essentially a distributed storage system. To ensure the security of user data in cloud storage, we proposed an effect and efficient stenographic strategy for enhancing security on data-at-rest. So, when these images are stored in the cloud data center, no one can view the original content of the data without any proper identification. Through detailed security and performance analysis, we have seen that our scheme almost guarantees the security of data when it is residing on the data center of any Cloud Service Provider (CSP).

REFERENCES

[1] Anil K Jain, "*Fundamentals of Digital Image Processing*", University of California-Davis, Prentice Hall, 1988

[2] Ken Cabeen and Peter Gent, ―Image Compression and Discrete Cosine Transform‖, College of Redwoods. *http://online.redwoods.cc.ca.us /instruct/darnold/LAP ROJ/Fall98/PKen/dct.pdf*

[3] Chang, C.C., Chen, T.S. and Chung, L.Z., "*A steganographic method based upon JPEG and quantization table modification*", Information Sciences, 2002, 141(1-2), pp.123-38.

[4] T. Morkel, J.H.P. Eloff , M.S. Olivier,"*An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005),* Sandton, South Africa, June/July 2005 .

[5] Ankur M. Mehta, Steven Lanzisera, and Kristofer S. J. Pister, "*Steganography 802.15.4 Wireless Communication".*

[6] Peter Mell, Timothy Grance, "The NIST Definition of CloudComputing", Jan, 2011.http://docs.ismgcorp.com /files/ external/Draft-SP-800-145_cloud-definition.pdf.

[7] Amazon.com, "Amazon Web Services (AWS)", Online athppt://aws.amazon.com, 2008.

[8] Con Wang, Qian Wang, Kui Ren, and Wenjng Lou, "Ensuring Data Storage Security in Cloud Computing", 17th Internationalworkshop on Quality of service, USA, pp1-9, 2009, IBSN:978-42443875-4.

[9] B.P Rimal, Choi Eunmi, I.Lumb, "A Taxonomy and Survey ofCloud Computing System", Intl. Joint Conference on INC, IMS and IDC, 2009, pp.44-51, Seoul, Aug, 2009. DOI:10.1109/NCM.2009.218.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability",Proc. of Asiacrypt '08, Dec. 2008.

[11] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage,"Cryptology ePrint Archive, Report 2008/489, 2008, http:// eprint.iacr.org/.

[12] A. Juels and J. Burton S. Kaliski, "PORs: Proofs ofRetrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

[13] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archivedcopy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.