International Journal of Engineering Research
Volume No.5, Issue No.6, pp : 434-438
ISSN:2319-6890)(online),2347-5013(print)
1 June 2016

Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography

Alok Ranjan, Mansi Bhonsle
PG Scholar, Department of Computer Engineering,
G. H. Raisoni College of Engg. & Mgmt. Pune, India-412 207
alok22.ranjan@gmail.com , mansi.bhonsle@raisoni.net

Abstract*: *Now-a-days, the growth of cloud data may be various problems that to be addressed in terms of service, management and privacy etc. To make sure robust data privacy, this paper introduce the technique to save your data by concealing the encoded data with multimedia files using multi-layer steganography and cryptography.

Keywords - Cloud Computing, Hash-LSB (Least Significant Bit), Steganography, Third Party Auditor (TPA), Advance Encryption Standards (AES).

I. INTRODUCTION

In recent years, the rapid growth of data in cloud computing data storage may be a vital issue of the complete information reside over a group of interconnected pools that permits via virtual machines. The basic need of each growing space in today's world is communication. Everybody desires to stay the within data of work to be secret and safe. It tend to use several insecure pathways in our everyday life for transferring and sharing data mistreatment internet or telephonically, however at a precise level it isn't safe. There are various problems that require to be addressed with respect to the service, management and privacy of data etc. To make sure privacy of data in cloud computing, this paper introduce an effective unique approach to make sure information security in cloud computing by means of encrypting and concealing the info with multimedia exploitation thought of multi-layer steganography and advanced encryption standard. The main goal of this paper is to forestall information access from cloud data storage centres by unauthorized users. Steganography and Cryptography are two strategies that can be accustomed share data in much concealed manner. Steganography is be a Greek work which suggests the covered writing. Steganography is associate art of concealment secret knowledge in an extremely coated media (image, audio, video, text). (Cryptology is that the Greek root for secret or hidden. It includes modification of a message during an exceedingly in a method that can be in digesting or encrypted kind guarded by an cryptography key that is understood by sender and receiver only and while not using secret writing key the message couldn't be accessed. The cover image containing the secret key message is then transferred to the recipient. The recipient is in a position to extract the message with the assistance of retrieving method and secret key provided by the sender. Also, system has implement the concept of external and internal user access where data owner has full control over the data in terms of sharing, securing and retrieving the data. This theme perfectly stored information at cloud data storage centres and retrieves data from it once it's required. This give the terribly high level knowledge security for online virtual system and save the fraud users to use your knowledge.

II. LITERATURE SURVEY

2.1. Brief Review

The most preferred techniques were analysed in this survey in steganography that has high responsibility and glorious security for cloud information.

Table I: Comparison between different algorithms and Techniques

Methods	Benefits	Efficiency
Steganography	Data stored in the form of images	Excellent
cryptographic	Maintained data integrity	Good
Preserving multiple keywords	Easy Data Retrieving	Good
Fully homographic encryption	Data Secured, Since it's not visible	Better
Fully disk encryption	Encryption applied to whole disk	Good
Hybrid cloud technology	Private data stored at user's end	Good
Pervasive developmental disorders (Pdd)technique	Reduced storage space, dependability	Good

it's associate art of hiding information in associate degree extremely coated media (image, audio, video, text) and also the technique of embedding hidden messages in such the simplest way that nobody, except the sender and meant receiver(s) will observe the existence of the messages. The most goal of steganography is to cover the key message or data in such a way that eavesdroppers aren't able to observe it. In step with our

observation, It tend to created associate degree analysis supported their performance and advantages. Every technique has its own pros and cons with it.

III. SYSTEM DESIGN

3.1. Existing System

The existing system affords security for the selling of cloud data security services in terms of privacy and data sharing protection. One of the most important problems is data security issue to be solved.

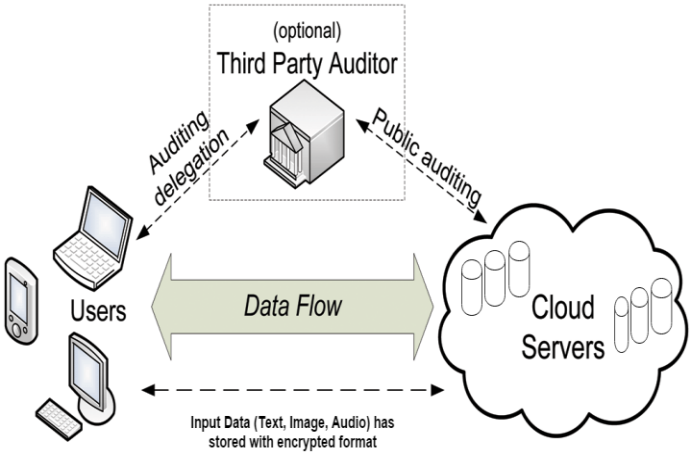


Fig. 1. Data storing process in existing System structure.

At present, it's still not being totally accepted that to manage data by a third party, allow to store the data only in encrypted format, especially for large enterprises, government departments, PHP and Confidential document such as (Credit/Debit card info, images, Audio and video).

3.2. Proposed Idea

To overcome the present system problems, the proposal system states about the solution for cloud computing security is a novel method, where it is using image or part of image and encryption key to encrypt the data and information. Once data will converted into encrypted then apply one time Password and Secret Key to merge with some multimedia file such as (image, Audio and Video). Once done, the combined file will again convert into the encrypted format and stored into the database. The complete work flow of the method is as explained in fig. 2.

3.3. System Architecture

The goal of development of this system "Enhanced Data Protection of Cloud Storage using Multi-Layer Steganography and Cryptography" is to introduce the technique to design the system which can help to secure and save the user confidential information into Cloud, which will be accessible in any location.

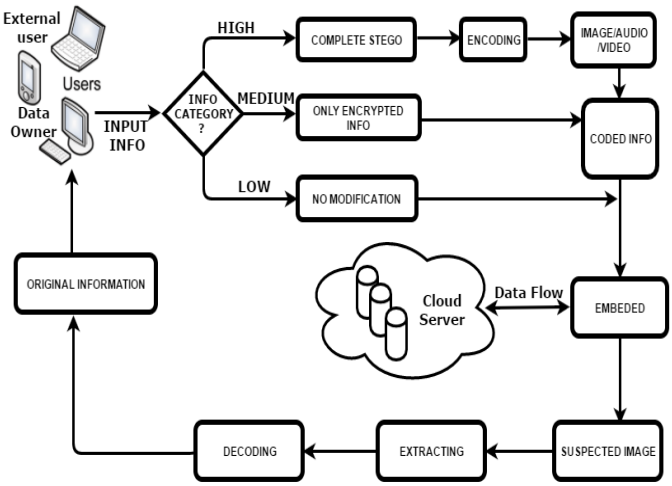


Fig. 2. System Structure of proposed system.

For getting back, reverse process will be applied to see the actual information. This model to be conferred is predicated on the principle of securing data each throughout transmission and while data-at rest at servers. The cloud design being used is as shown fig.2. Also, the same approach will work apply with other with other multimedia files such as Audio and Video steganography technique.

3.4. System Implementation

For implementing this system, it need to used here Java 8 for writing the system actual logic, HTML5 for Graphical User Interface (GUI), MySQL 6.35 for database management, Spring 4 used for security and database pool connection management. It used Tomcat 8 for web container where application will get deployed and run. Also, used Eclipse Kepler IDE for code implementation.

For implementing these all system, also required standard hardware such as at least 512 MB RAM, 80 GB Hard disk, std. Keyboard, Std. Mouse, std. Monitor with any operating system. Finally required the public cloud space where need to do same setup and deployed this application.

IV. PROBLEM FORMULATION AND WORK METHODOLOGY

The problem statement consists of embedding the key message within the LSB of every RGB pixels value of the cover image. Before embedding the key message ought to be regenerate to cipher text using AES algorithmic rule to reinforce the secrecy of the message. During this approach it tend to enforce a method referred to as Hash-LSB derived from LSB insertion on pictures. During this Hash-LSB, it tend to are using a hash perform to judge the positions wherever to hide the info bits or to be embedded. It's a difficult method which is able to lead us to mix the two technologies, one in all them is AES algorithmic rule from cryptography and other is Hash-LSB from steganography. Our analysis has targeted on providing an answer for transferring and sharing necessary information with none compromise in security. All the acknowledged organizations whereas causing

ISSN:2319-6890)(online),2347-5013(print)
1 June 2016

business documents over the internet forever use coding of the info to guard outflow of data regarding their organization from their rivals or intruders. It used Hash-LSB and AES algorithm to create a secure steganography algorithm that is way safer than several systems being employed for the aim of secretly sending the data.

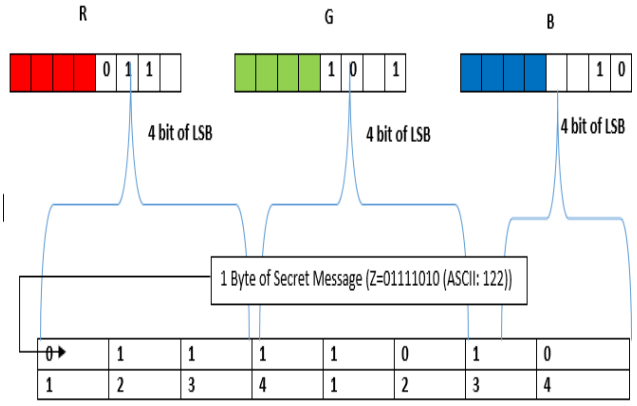


Fig. 3. Hash process to find LSB of RGB pixels value

4.1. Cover Image/Audio/Video and Secret Message

In our projected system, first of all need to have a tendency to choose a real color image of size 512 x 512 for to that as cover image and a secret message which can be embedded within the cover image.

4.2. Hash-LSB Process

The Hash primarily based least vital Bit (H-LSB) technique for steganography during which position of LSB for activity the key information is set using hash function. Hash function finds the positions of least vital little bit of every RGB pixel's then message bits are embedded into these RGB pixel's severally. Then hash function returns hash values consistent with the least vital bits present in RGB pixel values. The cover image are broken down or fragmented into RGB format. Then the Hash LSB technique can uses the values given by hash function to insert or conceal the info. during this technique the key message is regenerate into binary type as binary bits; every eight bits at a time are embedded in least significant bits of RGB pixel values of cover image within the order of three, three, and two respectively. According to this methodology three bits are embedded in red constituent LSB, three bits are embedded in inexperienced constituent LSB and a couple of bits are embedded in blue constituent LSB as illustrated in fig.3. These eight bits are inserted in this order as a result of the chromatic influence of blue color to the human eye is quite red and green colors. So the distribution pattern chooses the two bits to be hidden in blue pixel. So the standard of the image are not sacrificed. Following formula is used to find positions to cover knowledge in LSB of every RGB pixels of the cover image.

$$K = p \,\%\, n \qquad (1)$$

Where, k is that the LSB bit position at intervals the pixel; p represents the position of every hidden image pixel and n is that the number of bits of LSB which is four for the current case. When embedding the information in cover image, a stego image are going to be made. The recipient of this image should use the hash operate once more to extract the positions wherever the info has been kept. The extracted data are going to be in cipher text. When decoding of it, combining of bits into data can turn out the secret message as needed by the receiver.

4.3. AES Encryption and Hash-LSB Encoding

This approach of image steganography is using AES encryption technique to encipher the key knowledge. Encoding includes a message or a file encoding for changing it into the cipher text. Encryption method can use recipient public key to encipher secret knowledge. It provides security by changing secret data into a cipher text, which is able to be tough for any interloper to decipher it while not the recipient private key. At the beginning of this method, need to have a tendency to take cipher text encrypted from the secret message to be embedded within the cover image.

4.3.1. Embedding Algorithm:

Step 1: select the cover image and secret message.
Step 2: Encipher the message using AES rule.
Step 3: Realize four least important bits of every RGB pixels from cover image.
Step 4: Apply a hash function on LSB of cover image to induce the position.
Step 5: Embed eight bits of the encrypted message into four bits of LSB of RGB pixels of cover image within the order of three, three and two respectively using the position obtained from hash function given in equation one.
Step 6: Apply Secret Key and send stego image to server.

4.4. Hash-LSB Decoding and AES Decryption

In the decryption method it got again used the hash function to observe the positions of the LSB's wherever the information bits had been embedded. Once the position of the bits had been such that, the bits are then extracted from the position within the same order as they were embedhded. At the top of this method it's going to get the message in binary type that again converted into decimal type, and with same method it tend to get the cipher text message. When retrieving the positions of LSB's that contain secret information, the receiver can decode secret information using AES algorithm. To use AES algorithm receiver can use his/her private key as a result of the secret information are encrypted by recipient public key. Using receiver private key cipher text are converted into original message that is in decipherable type.

4.4.1. Retrieval Algorithm:

Step 1: Receive a stego image.
Step 2: Realize four LSB bits of every RGB pixels from stego image.
Step 3: Apply hash function to induce the position of LSB's with hidden knowledge.
Step 4: Retrieve the bits using these positions in order of three and a couple of respectively.

ISSN:2319-6890)(online),2347-5013(print)
1 June 2016

Step 5: Apply AES algorithmic rule to decode the retrieved information.
Step 6: Finally scan the secret message.

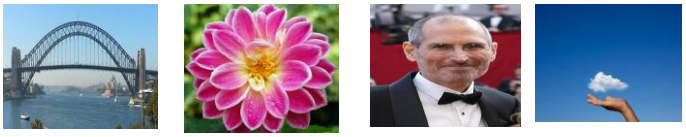
V. RESULTS ANALYSIS

5.1. Outcome of Proposed System

To evaluate the most effective obtainable system for cloud primarily based information security in any kind of information like image, audio and video. As per this situation, the cloud based information may be monitored by third party, they will observe and see your data simply. Only a few of the cloud supplier, they used to apply cryptanalytic technique to cover the particular data however still it's not much secure because any unauthorized user will simply cheat your confidential information.

5.2. Performance Analysis

The objective of the work are enforced an image steganography technique using Hash-LSB technique with AES algorithmic rule to enhance the protection of the information concealing technique. This system may be a combination of a Steganographic technique and another cryptographic technique which boosts the protection of information and data concealing technique. Our implemented Hash-LSB technique on pictures is used to cover data within the RGB pixels value of the cover image within the form of three, three and two bit order and positions to cover the information bits are calculated by hash function. The utilization of AES algorithmic rule has created our technique safer for open channel. AES algorithmic rule has been used with Hash-LSB so the original text are embedded into cover image within the type of cipher text.



(a) Bridge.jpg (b) Flower.png (c)Person.png (d) Cloud.jpg

Fig. 4. (a) to (d) four cover images.

The Hash-LSB technique has been applied to true colour pictures and which provides satisfactory results. The performance of the Hash-LSB technique has been evaluated and diagrammatically represented on the idea of two measures are – Mean sq. Error (MSE) and Peak Signal to Noise ratio (PSNR) and obtained values are far better than existing techniques. The technique known as "Enhanced Data Protection of Cloud Storage using Multi-Layer Steganography and Cryptography" has been enforced on JAVA with Eclipse Integrated Development Kit (IDE) by analysing four colour pictures of size 512 x 512 row format as chosen to cover a set size of secret information. During this method stego-image is generated using Hash-LSB and AES encoding that applied to boost the safety of hidden knowledge. For the performance analysis of the Hash-LSB technique to be enforced on four cover pictures Bridge.jpg, Flowers.png, Person.gif and Cloud.bmp are thought of and shown within the fig. 4.

The results for all stego pictures using Hash-LSB with AES technique are compared to easy LSB substitution with AES technique which supplies terribly lesser MSE values and better PSNR values. The Mean sq. Error (MSE) and Peak Signal to Noise ratio (PSNR) [13] between the stego image and its corresponding cowl image are studied and given below as eq. 2 and 3.

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i,j) - S(i,j))^2 \qquad (2)$$

Where, MSE is Mean sq. Error, H and W are height, width and P(i, j) that represents the cover image and S(i, j) represents its corresponding stego image.

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \qquad (3)$$

Where, PSNR is peak signal to noise ratio, L is peak amplitude for a colour image are taken as 255. During this technique of image steganography eight bits of knowledge are embedded in three pixels of the cover image. The mean sq. error (MSE) and also the peak signal to noise ratio (PSNR) for various stego pictures are shown within the Table II. By comparison the PSNR values of all the stego pictures, it's been analysed that only Bridge as a cover image have given the most effective PSNR value. A similar is true within the case for the MSE values whereas comparison with totally different stego images, Flowers as a cover image have given the smallest amount MSE value.

Table II. Results Obtained From LSB with RSA and H-LSB with AES.

Image Name (Size : 512 x 512 MM)	Existing System		Proposed System	
	LSB with RSA		H-LSB with AES	
	PSNR(db)	MSE	PSNR(db)	MSE
User1.png	51.1655	0.4972	73.5444	0.0029
User2.png	51. 0728	0.5097	74.0189	0.0026
User3.png	51.3453	0.477	73.822	0.0027
User4.png	51.149	0.4991	73.8528	0.0027
AVG	51.2199	0.4957	73.8095	0.0027

In fig. 5, the graphical illustration of PSNR and MSE values of various stego images. The horizontal axis shows the stego pictures and vertical shows vary of PSNR value in decibel. The PSNR values for LSB with RSA are lesser than the PSNR values of H-LSB with AES as compared in each of fig 4. This graph has clearly shown, how this system is effective for cloud users.

ISSN:2319-6890)(online),2347-5013(print)
1 June 2016

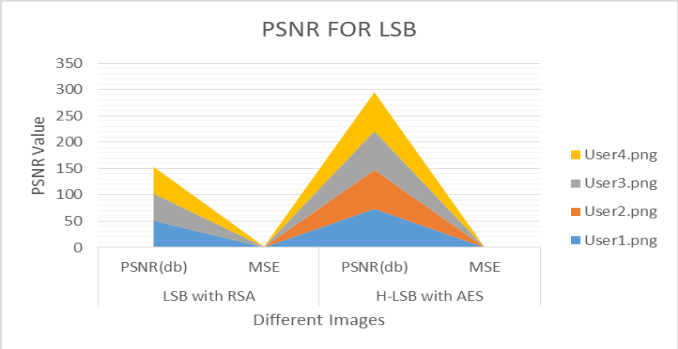


Fig. 5. The graphical representation of PSNR and MSE values.

5.3. System Efficiency

Existing system doesn't offer steganography thought before storing information into cloud with AES encryption technique. The projected system can solved and enhanced the cloud data privacy. Also, it provides high level cloud data security. Hence any user can access, share, stored the data from anywhere at any location without worry loss of information. Hence, this system is very much useful those who don't want to carry the data and make sure his data should available everywhere.

VI. CONCLUSIONS AND FUTURE WORK

Mostly the main focus of this paper is to solve and provide the robust security of cloud stored data in terms of sharing, securing and maintained data. In next step, this facilities are going to be obtainable via mobile Apps to save data, image, audio and video directly to cloud.

ACKNOWLEDGMENT

Our thanks to all the people who showered their kind support required for the whole analysis. The authors also want to thank the anonymous reviewers for their useful and constructive comments.

REFERENCES

i. *Seung Hyun Seo and Xiaoyu Ding "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transl. on Knowledge and Data Engineering, pp. 1041 - 4347, VOL. 26, No. 9, Sept 2014.*

ii. *Imran H. S. and Bhagyashree B.R., "Cloud Information Security Using Third Party Auditor and Cryptographic Concepts", International Journal of Application or Innovation in Engineering & Management (IJAIEM), pp. 2319 - 4847, VOL. 3, Issue 11, Nov 2014.*

iii. *Namita T., Dr. Madhu S. and Dr. Meenu C., "Spatial Domain Image Steganography based on Security and Randomization", International Journal of Advanced Computer Science and Applications (IJACSA), ISSN: 2345 - 4854, VOL. 5, No. 1, 2014.*

iv. *B. Poornima and Dr. T. Rajendran, "Improving Cloud Security by Enhanced Hasbe Using Hybrid Encryption Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 - 128, VOL. 4, Issue 4, and April 2014.*

v. *Rakhi and Suresh Gawande, "A Review on Steganography Methods", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), ISSN: 2278 – 8875, VOL. 2, Issue 10, and Oct 2013.*

vi. *Abhishek M., Ravi K. S. and Lalit K. A., "Robust Data Security for Cloud while using Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), ISSN: 2277 - 128, VOL. 2, Issue 2, Feb 2012.*

vii. *Sanjoli Singla and Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, VOL. 2, Issue 7, and July 2013.*

viii. *Hsiao-Ying Lin and Wen-Guey Tzeng, "Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE Transl. on Parallel and Distributed Systems, pp. 1045 - 9219, VOL. 23, NO. 6, 2012.*

ix. *Jean B., Thomas F. and Jatinder S., "Information Flow Control for Secure Cloud Computing", IEEE Transl. on Network and Service Management, pp. 1045-8294, VOL. 19, Sept. 2013.*

x. *Bhavani T., Vaibhav K. and Anuj Gupta, "Secure Data Storage and Retrieval in the Cloud", the University of Texas at Dallas, 800 W. Campbell Road, Richardson, TX 75080, 2010.*

xi. *[Book] Available: Luke Wroblewski, "Web Form Design: Filling in the Blanks", 2014, visited on 12/10/2015.*

xii. *L. Briand, Y. Labiche and Q. Lin, "Improving the coverage criteria of UML state machines using data flow analysis", J. Softw. Test., Verify, Rel., VOL. 20, no. 3, pp. 177–207, Sep. 2010.*

xiii. *[Book]. Available: Ron Patton, "Software Testing".*

xiv. *Parul Mukhi and Bhawna Chauhan, "Survey on triple system security in cloud computing", in proceeding of IJCSMC, VOL. 3, Issue. 4, April 2014.*

xv. *Parul Mukhi and Bhawna Chauhan, "Survey on triple system security in cloud computing", in proceeding of IJCSMC, VOL. 3, Issue. 4, April 2014.*

xvi. *Mohammed A. AlZain, Eric Pardede, Ben Soh, and James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", in 45th Hawaii International Conference on System Sciences, 2012.*

xvii. *A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-61, 2010.*

xviii. *Kritika S., "Hash Based Approach for Secure Image Steganography Using Canny Edge Detection Method", IJCSC, Vol.3, pp.155-157, June 2012.*

xix. *Cong Wang, Kui Ren, Wenjing Lou and Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, August 2010.*

xx. *C.Wang, "Ensuring Data Storage Security in Cloud Computing", In IJCA, pp. 1–9, July 2014 .*

xxi. *Dr.M.Umamaheswari, Prof. S.Sivasubramanian and S.Pandiarajan, "Analysis of Different Steganographic Algorithms for Secured Data Hiding", in IJCSNS International Journal of Computer Science and Network Security, VOL.10, No.8, August 2010.*

xxii. *Mrs.G.Prema and S.Natarajan, "Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application", IEEE, 2012.*

xxiii. *Fridrich, J. and Goljan, M, "Reliable Detection of LSB Steganography in Colour and Grayscale Images", in proceedings of ACM Workshop volume 02, Ottawa, October 5, 2001, pp.27-30.*

xxiv. *Shyamalendu K., Arnab M., "Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number", in International Journal of Computer Applications, VOL. 19– No.4, April 2011.*