ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 8, pp. 19596-19601, August, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

ENHANCE DATA SECURITY IN CLOUD USING STEGANOGRAPHY

Vaibhav Singhal[1] and Rachna Jain[2]

[1]Completed Bachelors of Technology (B.Tech) from Bharati Vidyapeeth's College of Engineering, IPU, India
[2]Computer Science & Engineering Department Bharati Vidyapeeth's College Of Engineering, IPU, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0808.0727

ARTICLE INFO

Article History:

Received 20th May, 2017
Received in revised form 25th June, 2017
Accepted 23rd July, 2017
Published online 28th August, 2017

Key Words:

Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud platform, Grid Computing, Steganography.

ABSTRACT

Cloud Computing is same as having a computer but without a computer. It delivers computer services- Servers, Storages, database, networking, software, and analytics- over the internet. We don't have to buy extra hardware for extra storage, server, etc. we get all that by virtually and it is pay-per-use. In cloud computing, data storage is a big issue because the entire data reside over a set of interconnected resource pools that enables the data to be accessed through virtual machines. These resource pools are situated over different parts of the world, therefore, security and management of the data may not be fully trustworthy. The objective of this paper is to prevent unauthorized access of data in cloud computing environment. In this paper, we introduce a model for storage of data, by hiding data inside images, using an algorithm based on LSB steganography technique.

INTRODUCTION

CLOUD Computing rather than a product, is the conveyance of computing as a service, done by sharing resources, software, and information, which are provided to computers and other devices as an expediency like the electric grid over a network or internet by the cloud service providers. Clouds can be classified as public, private or hybrid. Cloud computing, which is also called as shorthand just "the cloud", focuses on magnifying the forcefulness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computing facility that provides series to Indian users during Indian business hours with a specific application (e.g., accounting) may reallocate the same resources to serve Canadian users during Canadian business hours with a different application (e.g., email). With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

Cloud Service Providers (CSP) works similar as Internet Service Providers (ISP), ISP offers costumers high-speed broadband to access the internet, whereas CSP offers cloud platform for their customers to create and use their web services. In general, CSP offers Services like Infrastructure as a service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS) and lastly Framework as a service (Faas), which is another type of service that falls somewhere between SaaS and PaaS.

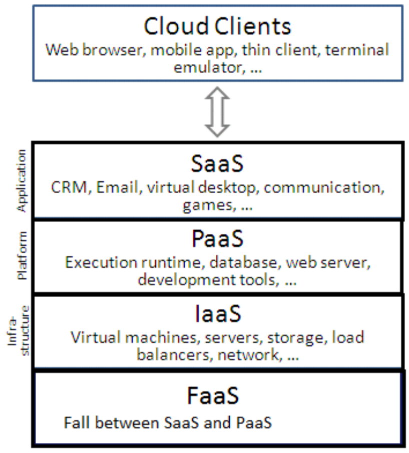
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...
FaaS
Fall between SaaS and PaaS

Figure 1 Service Models

Cloud computing has a unique property called data abstraction, which allows users to use these services without worrying

Corresponding author:* **Vaibhav Singhal
Completed Bachelors of Technology (B.Tech) from Bharati Vidyapeeth's College of Engineering, IPU, India

about any technical stuff, he will be provided with the user-friendly Graphical User Interface (GUI) on which he will access all the data. Cloud computing providers deliver common online business applications, which are accessed, from servers through web browser [1].

Cloud computing is just required to pay for the resources on the consumption basis. In addition, the cloud-computing organization can easily meet the requirements of the rapidly changing needs of markets to make sure that they are always on the leading edge for their consumers [2]. It appeared as a business necessity, by the idea of just using the infrastructure without managing it or buying it for the extra requirement. Microsoft is a leading global provider of cloud computing services for businesses of all sizes; recently companies like Google, Yahoo, Amazon, etc transposed in it. Benefits like cost, speed, Global scale, Productivity, Performance, Reliability make possible to create new ideas and convert them into reality without worrying about budget and space because it is greatly optimized. Cloud users can buy/rent computing power or storage space virtually according to the needs of their business. A user can run high demanding applications on fixed and portable devices Like PCs, PDAs, Laptops and mobile phones.

Steganography

Steganography is the study of encapsulating and hiding messages in a medium called a cover text. Steganography is just about as old as cryptography and related to it as well; used by the Ancient Greeks to hide information about troop movements by tattooing the information on someone's head and then hiding the tattoo by letting the person grow out their hair. Simply put, steganography is as old as dirt [3].

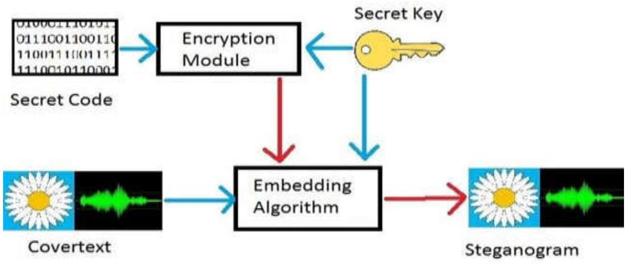

Figure 2 Image Illustrating Steganography

However, unlike Cryptography; scrambles messages so they cannot be understood, Steganography, hide the message so there is no evidence of the existence of the message in the first place. In some cases, sending the encrypted might attract some unauthorized to hack into the message, while an "invisible" message will not create such attention to do so. Both sciences combined to produce better protection of the message. It provides double layer protection, even if, the steganography fails to hide the message and detected by some unauthorized user, it is still protected by the encryption, which is done by cryptography technique and it is of no use. [3]

As any other message passing technique, steganography also contains two types of materials in it: message and carrier. A message is the secret data that should be hidden and a carrier is the material that takes the message in it [4].

The different types of file formats that can be applicable for steganography techniques are given in the in figure below [5].

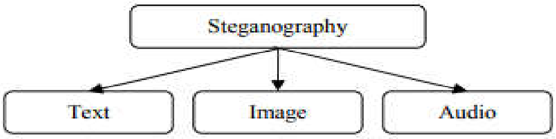

Figure 3 Steganography Type

Text Steganography- This technique can be achieved by altering certain characteristics of textual elements (e.g., characters) or just by changing the text style and formatting, or. The main objective in coding method is to think of alterations that are reliably decode-able; even in the presence of noise, yet largely indiscernible to the reader.

Audio Steganography- The main/secret message is encapsulated into a digitized audio signal, which ends up resulting only a slight changes of the binary sequence of the corresponding audio file. There are several methods, which are available for audio steganography. We are going to have a brief introduction on some of them.

Image Steganography- An image with a secret message hidden inside can easily be spread over the World Wide Web or in newsgroups. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. There are many techniques by which these alterations can be achievable, like the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

Symmetric Key Encryption

An encryption is a ritual in which the sender and receiver share the same key (or, negatively commonly, in which their keys are divergent, but allied in an easily computable way). Symmetric key ciphers are machined as each of two block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as averse to individual characters, the guidance form used by a stream cipher.

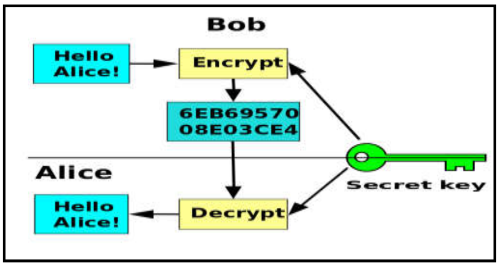

Figure 4 Symmetric Key Encryption

The Data Encryption Standard (DES) including the Advanced Encryption Standard (AES) are block cipher conceptions which have been designated cryptography standards by the US government. Stream ciphers, in foil to the 'block' type, forges an arbitrarily far-away stream of key material, which is pooled with the plaintext bit-by-bit as a choice character-by-character.

AES Encryption- The Advanced Encryption Standard (AES), conjointly termed in the act of Rijndael (its original name), is a stipulation for the encryption of electronic data well-established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Working- AES span onto three block ciphers, AES-128, AES-192, and AES-256. Respective cipher inscribes and decrypts data in blocks of 128 bits with the help of cryptographic keys of 128-, 192- and 256-bits, fitly. (Rijndael was designed to crank additional block sizes and key lengths, though the functionality was not seized in AES.) Symmetric or secret-key ciphers make use of the same key for encrypting and decrypting, so the pair the sender and the receiver devoir know and make use of the same secret key. Gross key lengths are deemed sufficient to foster classified network up to the "Secret" level with "Top Secret" lore requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- domical consists of several processing traces that entails substitution, transposition, and mixing of the steer plain text and transfigure it into the final output of the cipher-text.

As a cipher, AES has attested reliable. The only successful attack facing it have been side-channel onsets on weaknesses raised in the implementation or key management of cocksure AES-based encryption products. (Side-channel blitz don't use brute force or theoretical weaknesses to break a cipher, but rather exploit warts in the way it has been implemented.) The BEAST browser maneuver against the TLS v1.0 protocol is a good paragon; TLS can use AES to encrypt data, but due to the data that TLS exposes, pushers managed to predict the initialization vector block worn at the start of the encryption process.

Sundry researchers have published attacks adjacent reduced-round versions of the Advanced Encryption Standard, and a research paper published in 2011 manifested a technique christened a biclique barrage could salvage AES keys nimble than a brute-force attack by an aspect of between three and five, reckoning on the cipher version. Steadily this attack, though, does not threaten the practical custom of AES due to its steep computational complexity.

Related Work

R. Chandramouli *et al* [7] in October 2001, he derived a closed form expression of the probability of detection and false alarm in terms of the number of bits that are hidden.

Atallah M. Al-Shatnawi *et al* [8] in March 2012, he proposed method hide the secret message based on searching about the identical bits between the image pixels values and secret messages.

Abdul Wahid Khan *et al* [9] in May-June 2012, he defined various data protection models and techniques and their contribution. Also illustrated problem of data privacy in cloud.
Parsi Kalpana *et al* [10] in September, 2012, she used RSA encryption algorithm for provision of security, to obtain the goal of secure storage and management of data.

Ramadhan Mstafa *et al* [11] in March 2013,Authors have reviewed some techniques of steganography and digital watermarking in both spatial and frequency domains.

Cherukuri Balakrishna *et al* [12] in January 2014, They proposed a novel single digit sum (SDS) based image steganography scheme. The purpose of proposed technique is to control the amount of change in a pixel. A lossy compressed version of the cover image has been used to determine the upper limit of change in each pixel value.

Praveen Nagar *et al* [13] in June 2014, discussed the implementation and analysis of image steganographic process is carried out to secure the data on cloud.

Wojciech Mazurczyk *et al* [14], focused on characterisation of information hiding possibilities in cloud computing environment. In particular this paper introduced classification of steganographic communication scenarios in cloud computing which is based on location of the steganograms receiver.

Proposed Idea

For altering the image by hiding the secret message in it without any detection I will be using LSB method with some custom modification to make it more effective and more pragmatic.

Least-Significant Bits- It is the simplest steganography technique, which encapsulates the bits of the message directly into LSB plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small [6]. A proper cover image is needed to hide an undisclosed message inside an image. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise, the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When ‘A’ character, which is equal to 10000001 in the binary value, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

In this case, only three bits were needed to be switched in order to interject the character successfully. On an average, one half of the bits in an image might be needed to be modified to tuck away a concealed message using the maximal cover stature. The changes that are shaped to the least significant bits are withal small to be recognized aside from the human visual system (HVS), so the message is effectively veiled [3].

Done in two phases

1. It explains the encoding process used in the project, i.e. it deals with information regarding hiding data inside the image.
2. It explains the decoding process used in the project i.e. it deals with information regarding extracting data from the image.

Encoding

The file, which is selected by the user, will undergo in AES 256 bit encryption. The encrypted file then, converted to a byte array, and calculate the number of images required to hide the file. For each RGB component of a pixel, calculate the number of bits that can be stored, based on the position of the first set bit and replace those bit from file to be hidden. As the data is hidden, add random data to remaining pixel positions. Store image name and all the relevant information in the database.

Decoding

Retrieve the images required to containing data of the file to be extracted. For each RGB component of image's pixel do the following.

1. Check the position of the first set bit in the component.
2. On the basis of the first set bit, extract the number of bits from the image.
3. Add the bits to form a byte, when the byte is completed add to the byte array.

Once all the data is retrieved, decrypt the data using AES 256 bit encryption. Send the decrypted file to the user.

Proposed Algorithm

In classical LSB method, the data was embedded in last bit of the RGB components of every pixel. Thus every pixel can only store 3 bits of data. This amount of data is very small if we storing large files in an image. Hence, we have modified this concept and decide the number of bits to store in the RGB component based on the first set bit of RGB component of a current pixel.
Let the RGB components of the pixels (Pi) are:

Screenshots

RED (Pi) = $(134)_{10} = (10000110)_2$
BLUE (Pi) = $(14)_{10} = (00001110)_2$
GREEN (Pi) = $(108)_{10} = (01101100)_2$

For the pixel Pi's red component, first set bit is at position 8. If 15 is added to this pixel it would not change image significantly. The minimum 8-bit number is 128 if we add 15 to this number the number becomes 143. In color, this pixel is not much significant to human eyes. Here is the preview of the red pixel:

Figure 5 with RED (pi) = 128

Figure 6 with RED (pi) = 143

Table 1 the basis for selection of number of bits to replace

Bit number(first set bit)	Replace number of the bits
7-8	4
5-6	3
3-4	2
2-1	1

For example:

Data: "m" has ASCII value 109.
$(109)_{10} = (01101101)_2$

If Data is embedded in the above pixel then the resultant pixels are as follows:

RED (Pi) = $(134)_{10} = (10000110)_2$
BLUE (Pi) = $(14)_{10} = (00001111)_2$
GREEN (Pi) = $(108)_{10} = (01100100)_2$
highlighted bits represent the embedded data. If the data bits are less than bits that can be replaced then we add random data following that bit in the remaining pixels of the image.

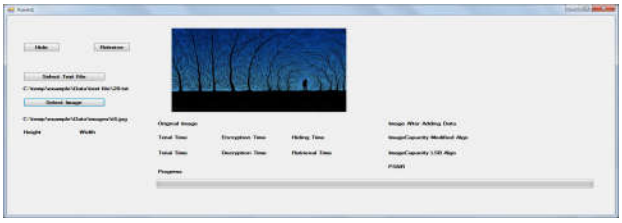

Image 7 Carrier image and file to be hidden are selected.

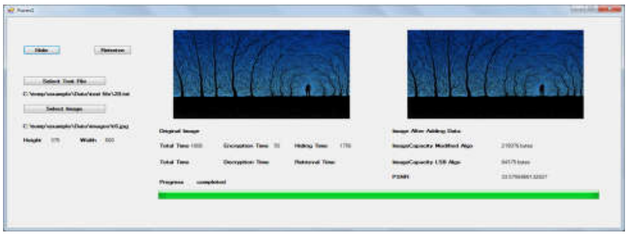

Image 8 Comparison of original image and image with data

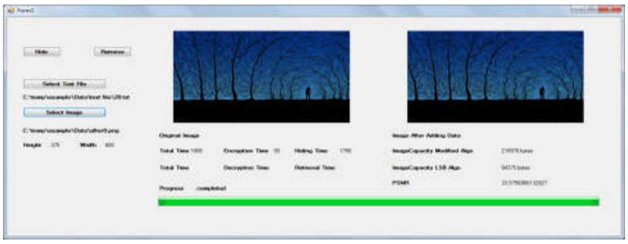

Image 9 Image with data selected

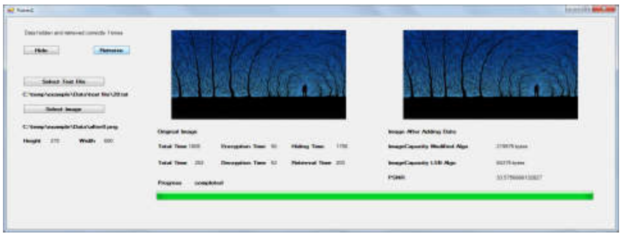

Image 10 Hidden file retrieved from image.

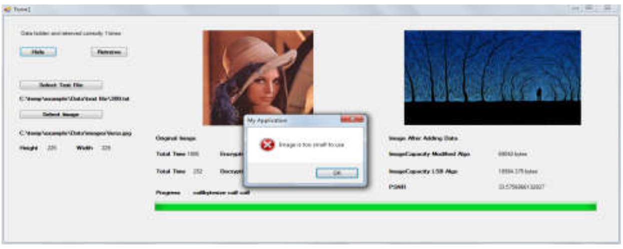

Image 11 Image data hiding capacity less than size of file to be hidden.

RESULTS

Data Hiding Capacity

The graph above shows the amount of data which can be stored in an image using LSB technique and the proposed algorithm. The data stored in an image using the proposed algorithm is much more as compared to the data which can be stored using LSB technique.

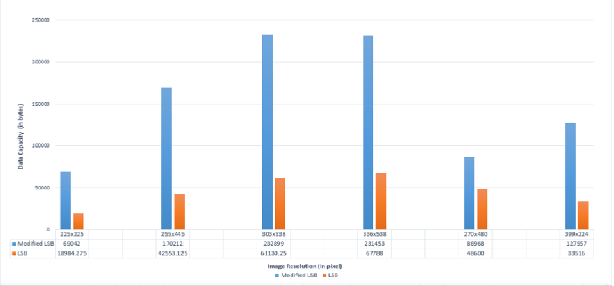

Image 12 Data hiding capacity in modified LSB and LSB method

Image 13 Image resolution 394x224 pixels before embedding data

Image 14 Image resolution 394x224 pixels after embedding data

Visual of Images before and After Encoding

We show some images before and after embedding data within the image. We have embedded data of size 158KB inside the image of different resolution.

PSNR Ratio

We used Peak Signal to Noise Ratio (PSNR) as a measure of quality. PSNR is a measure of the peak error. PSNR ratio is mathematically defined as

$$PSNR = 20 \times \log_{10} (255 \div \sqrt{MSE})$$

Where MSE is the mean signal error of new image. A lower value for MSE means lesser error, leading to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher.

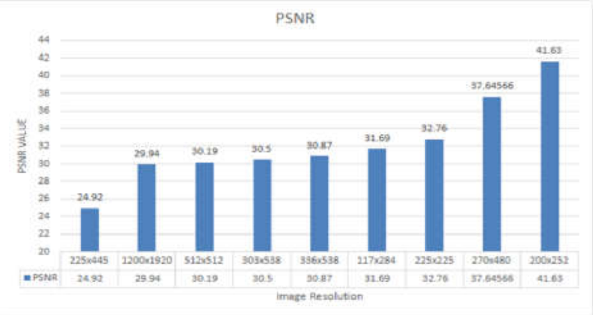

Image 15 PSNR values for different image resolutions.

During our tests we found PSNR values to fall in range 30-40, due to adding of random data in the image it becomes hard to find end of data in the image, without having prior knowledge about it. During our tests we also analyses that value of PSNR is independent of the Image resolution. The value of PSNR depends on color combination that is it is better for dark color images in comparison to light color images.

CONCLUSION

Our model thus successfully provides security to sensitive data, by encrypting sensitive data and hiding it behind images, thus obfuscating presence of data to any unauthorized user; using an algorithm based on LSB steganography technique. Modifying LSB and making it better for practical usage. Random data inside the image add another layer of security by hiding end of data. which makes this technique even more effective and more suitable for current needs.

References

1. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", *International Journal of Digital Content Technology and its Applications*, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
2. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008.
3. Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf
4. Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.
5. Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, Data Hiding Through Multi Level Steganography and SSCE, *Journal of Global Research in Computer Scienc Journal Science*, ISSN: 2229-371x, Volume 2, No. 2, February 2011, pp. 38-47.
6. Atallah M. Al-Shatnawi "A New Method in Image Steganography with Improved Image Quality". "Applied Mathematical Sciences, Vol. 6, 2012," March, 2012
7. R. Chandramouli, Nasir Memon "Analysis of LSB based image steganography techniques". "Image Processing, 2001. Proceedings. 2001 International Conference, IEEE" October 2001
8. Atallah M. Al-Shatnawi "A New Method in Image Steganography with Improved Image Quality". "Applied Mathematical Sciences, Vol. 6, 2012," March, 2012
9. Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem, "A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing", *IOSR Journal of Computer Engineering (IOSRJCE),* ISSN: 2278-0661 Volume 1, Issue 3 (May-June 2012)
10. Parsi Kalpana and Sudha Singaraja, "Data Security in Cloud Computing using RSA Algorithm", *International Journal of Research in Computer and Communication technology, IJRCCT,* ISSN 2278-5841, Volume 1, Issue 4, September 2012

11. Ramadhan Mstafa, Christian Bach, “Information Hiding in Images Using Steganography Techniques”. 2013 American society for engineering education (ASEE) Northeast Section Conference, March 2013
12. Cherukuri Balakrishna, Valluru NaveenChandra, Rajarshi Pal “Image Steganography Using Single Digit Sum with Varying Base”. “Electronics, Computing and Communication Technologies (IEEE CONECCT), 2014 IEEE International Conference” January 2014
13. Praveen Nagar, Noor Mohamned, Navdeep Kumar, Neha Sharma “A Secure Implementation and Analysis of Image Steganographic Method for Data Security in Clouds”. “*International Journal of Advanced Research in Computer Science and Software Engineering*” June 2014.
14. Wojciech Mazurczyk, Krzysztof Szczypiorski “Is Cloud Computing Steganography proof?”

How to cite this article:

Vaibhav Singhal and Rachna Jain.2017, Enhance Data Security In Cloud Using Steganography. *Int J Recent Sci Res.* 8(8), pp. 19596-19601. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0808.0727

****