© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Review-A Secure Mutual Authentication Protocol for Cloud Computing Using Secret Sharing and Image Steganography

Prof. Imran Tamboli, Sagar K. Khatal, Akshay B. Kadhane, Ravi Moon

Dr. D. Y. Patil College of Engineering, Pune, Maharastra, India

ABSTRACT

Cloud computing is to handle enormous enterprise computing, hardware, storage needs as a collection of virtually massive distributed large-scale computers. An exponential advancement of communication and information technologies which results in substantial traffic for accessing the cloud resources wired and mobile, through various communication devices as desktop, laptop, tabs, etc. Demands for reliable and low cost authentication a technique is signified by enterprise data also increased access rates from low-resource terminal devices. With varied efficiencies, many researchers have proposed an authentication scheme, which is based on password, biometric, steganography etc. In 2014, Nimmy et al proposed a steganography system based cloud computing in mutual authentication protocol and claimed that their scheme resists major cryptographic attacks. We will show that Nimmy et al is vulnerable to offline password attack guessing and Service attack. As a part of our contribution, for asymmetric cloud computing environment we propose a low cost steganography is based on authentication scheme which is strongly secure and best suited.

Keywords: Steganography, Steganalysis, Cryptography, Data Hiding

I. INTRODUCTION

The process of hiding a secret message within a larger one in such a way that no one can see the presence or contents of the hidden message is Steganography. Although, Steganography is easy with Encryption, which is the process of making a message unreadable. Steganography attempts to hide the existence of communication.

The basic structure of Steganography mainly consists of three components: the carrier, the message, and the key. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. The hidden message is carried by the object. To decode /decipher /discover the hidden message Key is used. This can be anything from a password, a pattern, a black-light, or lemon juice. In this paper we focus on the use of Steganography within digital images (BMP and PNG) using LSB Substitution, although the properties of Image Steganography may be substituted with audio mp3's, videos, and any other digital document format relatively easily.

In today's modern high-tech world Image Steganography has many application. Privacy and anonymity is a concern for most people on the internet. In image Steganography two parties are allowed to communicate secretly and covertly. For some morally-conscious people to safely whistle blow on internal actions is allowed by Stegnography; the message as a digital watermark are allowed for copyright protection on digital files. For Image Steganography one of the other main uses is, for the transportation of top-secret or high-level documents between international overnments. As the Image Steganography has many legitimate uses, it may be quite nefarious. It may be used by hackers to send viruses and Trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

By using encoding and decoding process the image steganography is being done. Whereas the secret sharing of the text as well as the image processing is done on cloud computing.

II. METHODS AND MATERIAL

There are presently three effective methods in applying Image Steganography: Blocking, LSB Substitution, and Palette Modification. By using LSB the pixels of the carrier image are substituted where the process of modification of the least significant bit is done. Blocking is done by using Discrete Cosine Transforms and also breaking up an image into blocks. In 64 DCT coefficients each block is broken that approximate luminance and also colour. For hiding messages the values are modified. Palette modification is used for replacing the unused colours within an image's colour palette with colours that represent the hidden message. Here to implement LSB Substitution in project, as carrier formats in ubiquity and message types. With LSB Substitution it could easily change from Image Steganography to Audio Steganography and hide a zip archive. With few limitations LSB Substitution lends itself to become a very powerful Stenographic method.
Iteration through the pixels of an image and extraction of the ARGB values is done by LSB Substitution. Then separation of the colour channels and gets the least significant bit is done. Where as in meanwhile, iteration through the characters of the message setting of the bit to its corresponding binary value.

```
int setLest(int color, int value){
return (((colour >>> 1) << 1) | value); //LSB: 0 or 1
}
int cont = 0;
for(int j = 1; j < img.getHght(); j++){
for(int k = 0; k < img.getWid(); k++){
arg = image.getRGB(k, j); // pixel value
a = getA(arg); //alpha
r = getR(arg); //red
g = getG(arg); //green
b = getB(arg); //blue
r = setLestBit(r, parseInt(binaryMsg.charAt(count
++)));
if(count >= binaryMsg.length()){
image.setRGB(k, j, getIntFromARGB(a, r, g, b));
break; }
…Green, Blue, etc.
}
image.setRGB(k, j, getIntFromARGB(a, r, g, b));
}
```

In this implementation, first encrypt the message, and then create a header that evaluates the corresponding mode, length, and offset to Steganograph the image with. By using a header it is able to have more control over the type of information hiding as well as the carrier file used.

Encrypt the message using a modified Vigenere Cipher that takes advantage of the entire ASCII character set, implements passwords, and uses simple hashing. A Vigenere Cipher is based on the Caesar Cipher which uses an alphabetic shift algorithm.

A Caesar Cipher shifts the alphabet resulting in:

Xyzabc assigns : a=x, b=y, c=z, d=a, e=b, f=c
a: wxyzabc
b: xyzabcd
c: yzabcde
d: zabcdef
e: abcdefg

III. RESULTS AND DISCUSSION

As Steganography is to hide messages, it should not be very effective at doing so. There are many different attacks that one may execute to test for Steganographed images--such as: Chi-Square Analysis, Enhanced LSB Attacks, Visual Attacks, and other statistical analyses. Virgin image must be used for performing a visual attack to compare it, and where the Steganographed images are visually compared with the two for artifacts. While in Enhanced LSB Attack, you must process the image for least significant bits, also if the LSB is equal to one, multiplying it by 255 as it becomes its maximum value.

A. The Encoding Process

1) Firstly take input as the coloured (RGB) carrier image.
2) Image filter is applied on the coloured image to detect the edges. Three types of filters are used for this operation, namely- 'Laplacian', 'Sobel' and 'Prewitt'.
3) The edge pixels are now observed and their locations traced out on a matrix to determine the position keys for data embedding.
4) The coloured image is split into its three channels; R, G and B, respectively. Discrete

Cosine transform is applied on all the Individual channels to observe three different transformed vectors.

5) Conversion of the message vector is done to its equivalent binary form. The pixel values are individually converted to its binary form for any image payload. For text messages, the ASCII values of the letters are converted to their equivalent binary form.
6) The embedding process:-

- The length of the message vector is converted to its equivalent binary form and placed in the initial corner pixels of the image.
- For every position of the key matrix generated from the edge-detected image, the corresponding values from transformed R and B matrices are taken, i.e.

X = dctred(key(i),key(j)) (4)

Y= dctblue(key(i),key(j)) (5)

- • Now, the message vector is checked. For a zero in the message vector, the half of the difference of X and Y is stored in the equivalent position in the transformed green matrix and for one, the average of X and Y, is stored in the equivalent place, i.e. dctgreen(key(i),key(j) = (X-Y)/2, for 0 (6)

dctgreen(key(i),key(j))=(X+Y)/2, for 1 (7)

- The process is repeated for the total length of the message vector.

7) After embedding, the inverse Discrete Cosine transform is taken on all the individual channels to provide the three colour channels.
8) The three colour channels are concatenated to produce the output stego image.

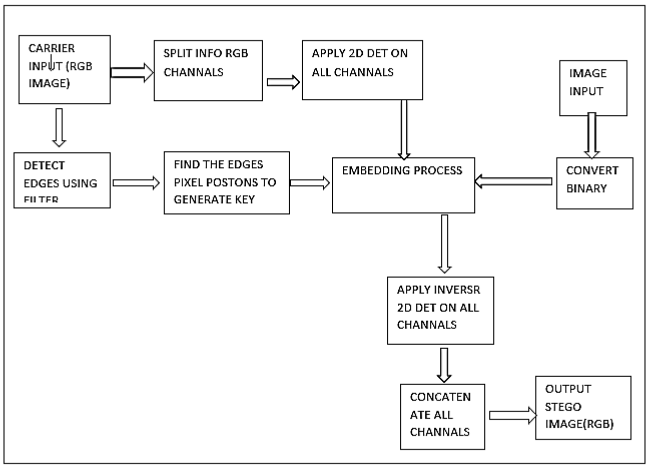
CARRIER INPUT (RGB IMAGE)
SPLIT INFO RGB CHANNALS
APPLY 2D DET ON ALL CHANNALS
IMAGE INPUT
DETECT EDGES USING FILTER
FIND THE EDGES PIXEL POSTONS TO GENERATE KEY
EMBEDDING PROCESS
CONVERT BINARY
APPLY INVERSR 2D DET ON ALL CHANNALS
CONCATEN ATE ALL CHANNALS
OUTPUT STEGO IMAGE(RGB)

Figure 4. Block Diagram of Encoding Process

B. The Decoding Process

1) The coloured (RGB) stego image is taken as input.
2) Image filter is applied on the coloured image to detect the edges. Three types of filters are used for this operation, namely- ‘Laplacian’, ‘Sobel’ and ‘Prewitt’ . The choice of filter is specific, according to the one used in embedding.
3) The edge pixels are again observed and their locations traced out on a matrix to determine the position keys for data embedding.
4) The coloured stego image is split into its three channels; R, G and B, respectively. Discrete Cosine transform is applied on all the individual channels to observe three different transformed vectors.
5) The extraction process:-
   - The first few pixels are scanned to find the length of the message vector. From the binary values, the total length is obtained.
   - For every position of the key matrix generated from the edge-detected image, the corresponding values from transformed R and B matrices are taken, i.e.
     X = dctred(key(i),key(j)) (8)
     Y= dctblue(key(i),key(j)) (9)
   - Two individual values for S1 and S0 are calculated as follows,
     S1=(X+Y)/2 (10)
     S0=(X-Y)/2 (11)
   - Now, for the same position of the green transformed matrix the values are observed. If it matches with S1, then a one is added to the output message vector. Similarly if it matches with S0, then a zero is added to the message vector, i.e.
     If dctgreen(key(i),key(j)) = S1, then m=1
     If dctgreen(key(i),key(j)) = S0, then m=0
   - The process is continued for the entire length as obtained before, to extract the complete message vector sent in binary form.
6) The message vector received in binary form is now converted to its equivalent form in which it was seen (image, text, etc).

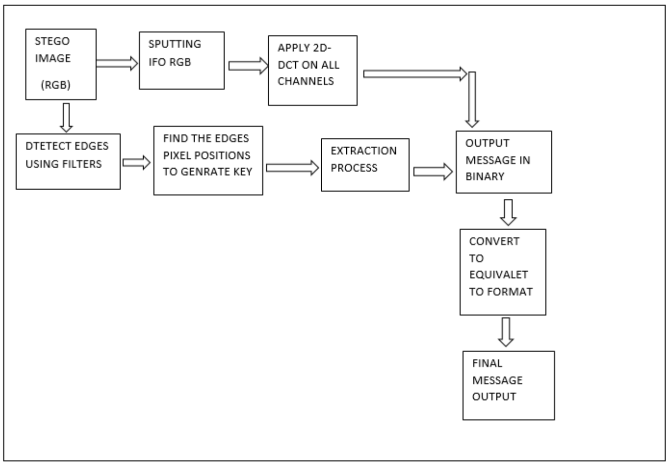
STEGO IMAGE (RGB)
SPUTTING IFO RGB
APPLY 2D-DCT ON ALL CHANNELS
DTETECT EDGES USING FILTERS
FIND THE EDGES PIXEL POSITIONS TO GENRATE KEY
EXTRACTION PROCESS
OUTPUT MESSAGE IN BINARY
CONVERT TO EQUIVALET TO FORMAT
FINAL MESSAGE OUTPUT

Figure 3. Block Diagram of Decoding Process

IV. CONCLUSION

In the present era the by considering the cloud computing, the steganography method has been used to for the encryption and decryption of images. The different papers have been reviewed here to give overall idea about the use of images for encryption and decryption. In our system, the algorithm has been created to perform over the whole cloud with the secret message sharing capacity.

V. REFERENCES

[1] V. K. Zadiraka and A. M. Kudin, ”Cloud computing in cryptography and steganography”, springer journal of Cybernetics and Systems Analysis, Volume 49, Issue 4, pp 584-588,July 2013.

[2] S S. Subashini, and V.Kavitha, ”A survey on security issues in service delivery models of cloud computing”, Elsevier Journal of Networkand Computer Applications, vol 34, pp: 111, 2011.

[3] D.A.B. Fernandes,L.F.B. Soares,J.V. Gomes, M.M.Freire, and P. R.M. Incio, ”Security issues in cloud environments: a survey”, springer international Journal of Information Security,Volume 13,Issue 2, pp 113-170, April 2014.

[4] E. Aguiar,Y.Zhang and M.Blanton, ”An Overview of Issues and Recent Developments in Cloud Computing and Storage Security”, springer journal of High Performance Cloud Auditing and Applications pp 3-33, 2014.

[5] Q. Gu, and M. Guirguis. Secure Mobile Cloud Computing and Security Issues, Springer: High Performance Cloud Auditing and Applications, pp 65-90, 2014.

[6] K.Murakami,K. Hanyu, R. Q. Zhao, and Y.Kaneda,”Improvement of security in cloud systems based on steganography”, International Joint Conference on Awareness Science and Technology and Ubi-Media Computing, pp:503 - 508, 2-4 Nov. 2013.

[7] A.B. Ramachandran, P.Pradeepan, and M.Saswati,” Security as a Service using Data Steganography in Cloud”, The International Conference on Cloud Security and Management , Washington University, Seattle, USA,Oct 17-18,October 2013. I.M.Khalil, A.Khreishah, M.Azeem, ”Cloud Computing Security: A Survey”, MDPI: Computers, vol 3, pp:1-35, 2014.

[8] G.Shailender, G.Ankur, B.Bharat, ”Information Hiding Using Least Significant Bit Steganography and Cryptography”,International Journal of Modern Education and Computer Science,Vol6,27-34, 2012.

[9] K.Nimmy, M.Sethumadhavan, ”Novel mutual authentication protocol for cloud computing using secret sharing and steganography”, Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), feb,2014, India.

[10] N. Chen and R. Jiang, Security Analysis and Improvement of User Authentication Framework for Cloud Computing, Journal of Networks, pp.198-203, 2014.