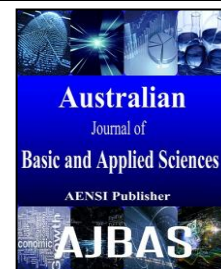




ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



Cloud Computing Data Security: AES Encryption Algorithm and PRT-PVD Steganography Technique

¹Suhad Shakir Jaber, ²Hilal Adnan Fadhil, ³Zahereel I. Abdul khalib, ⁴Rasim Azeez Kadhim

^{1,2,3,4}School of Computer and Communication Engineering, University Malaysia Perlis, Pauh Putra, Arau, Perlis 02600, Malaysia.

^{1,4}Ministry of Sciences and Technology, Baghdad, Iraq.

ARTICLE INFO

Article history:

Received 12 March 2015

Accepted 28 April 2015

Available online 2 May 2015

Keywords:

Cryptography, Steganography,
PRT_PVD, AES, Encryption,
Decryption

ABSTRACT

Cloud computing is a collection of virtually massive distributed large scale computers to handle tremendous enterprise computing, hardware, storage needs. Cryptography and Steganography are two popular techniques used to generate new security system. The main principle of cryptography is the ability to change the original information into an unreadable form, while steganography hides the existence of the information. In this paper a new cloud computing data security scheme that combines cryptography and steganography techniques is proposed to enhance the security of communication over an open channel. By means of cryptography, the secret image is encrypted using the Advanced Encryption Standard (AES) algorithm. Next, the Patch Reference Table Pixel Value Difference (PRT-PVD) steganography method is applied to hide the cipher image. The experimental result reveals that this method is easy to be implemented, achieve high image quality, and also highly robust to resist regular steganalysis such as the difference histogram.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Suhad Shakir Jaber, Hilal Adnan Fadhil, Zahereel I. Abdul khalib, Rasim Azeez Kadhim., Cloud Computing Data Security: AES Encryption Algorithm and PRT-PVD Steganography Technique. *Aust. J. Basic & Appl. Sci.*, 9(19): 85-93, 2015

INTRODUCTION

Cloud computing is a distributed computing systems architecture, which equips an elastic, on demand Computing capacity and virtually infinite database storage capacity. Regardless of geographical location of client, the data involved is transmitted through an insecure communication channel called Internet. Due to advancement of communication technologies, exponential growth on the numbers of users connecting to the cloud servers through light weight resource constrained devices like mobile phone, and tablets is evidence (Zadiraka and Kudin 2013). Hence, the need for secure communication over the cloud is a growing demand. Many researchers have analyzed security issues focusing on various areas of cloud security.

For instance, in 2013, Muakami *et al* have proposed an improvement of security in cloud systems based on steganography (Murakami, Hanyu *et al.* 2013). In 2013, Ramachandran *et al* discussed on security as a service using data steganography in cloud (Ramachandran, Paramjothi *et al.* 2013). In 2014, I.M.Khalil analyzed application of data steganography to cloud environment (Khalil, Khreishah *et al.* 2014). In 2014, Nimmy *et al* proposed a steganography based mutual

authentication protocol for cloud computing and claimed that their scheme resists major cryptographic attacks (Nimmy and Sethumadhavan 2014). They used new features like Out Of Band (OOB) secret sharing. They embed the data to be transferred into an image using Pixel Value Differencing technique (Chen and Jiang 2014). At server side the image is divided into two shares using (2, 2) secret image sharing scheme based on addition (Dong and Ku 2010). In 2014, Devi and Ganesan performed comprehensive analysis on security vulnerabilities, threats and attacks in cloud environment and proposed a classification among them. In addition, the study focused on various encryption techniques and proof of storage methods (Devi and San 2014).

In 2014, Mahyar Amini *et al* discussed the Small and medium enterprises (SMEs) due to cloud computing is a new phenomenon, which helps SMEs tackling many issues such as, cost and risk management to understand the potential of environmental factors for adoption of cloud computing (Amini, Sadat Safavi *et al.* 2014). The study also covered availability, privacy and integrity of client data to adoption of Cloud Computing for Small and Medium Enterprises. In this paper we will present a secure system that combined the two techniques aforementioned to achieve a higher level

Corresponding Author: Suhad Shakir Jaber, School of Computer and Communication Engineering, University Malaysia Perlis, Pauh Putra, Arau, Perlis 02600, Malaysia.
E-mail: shakir_suhad78@yahoo.com or hilaladnan@unimap.edu.my, Ph: +60143016114.

of robustness and provide a better image quality through hide data from unauthorized users or attack. As part of our contribution, we propose integration of AES encryption method (a cryptography technique) with the PRT_PVD scheme (a steganography technique) to enforce security of secret data. This approach gives a more robust security measure which are strongly secured and best suited for asymmetric cloud computing environment.

I. Overview of General Models of Image Steganography System and Cryptography Technique:

It is necessary to keep all information related to work in a safe and secret way. Today, steganography and cryptography methods are widely used to

manipulate information in order to cipher or hide their existence. In cryptography, the message is transformed into an unreadable format that is protected by an encryption key. In this case, no one can know and get the message except the sender and receiver. In steganography, the secret message is hidden in a cover image. Thus, no intermediate person can see that secret message. Meanwhile, the secret message in cryptography can always be display clearly (Shukla, Chadha *et al.*). The sender can send the encryption message to the recipient by using a secret key, and the recipient can extract the secret message with the help of the same secret key available by the sender. A Model of the cryptography and steganography is displayed in Figure 1 and Figure 2 respectively.

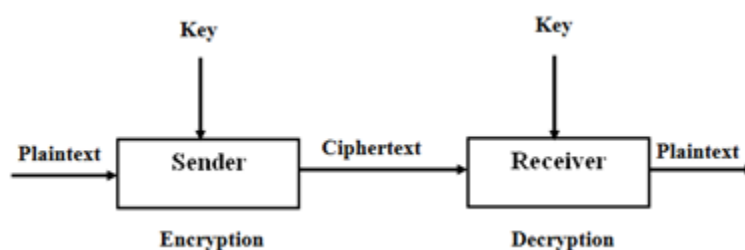


Fig. 1: General Model of Cryptography Technique.

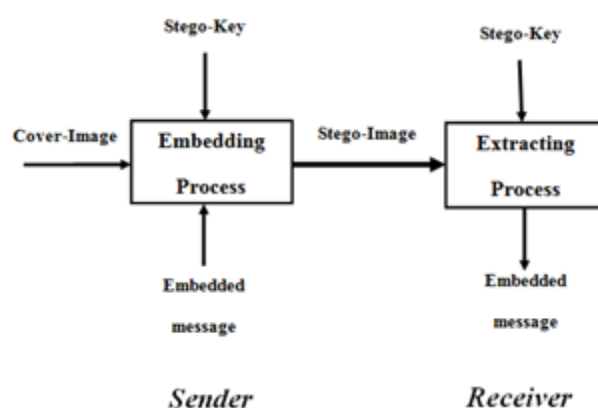


Fig. 2: General Model of Image Steganography System.

A. Cryptography:

Cryptography is the art of cipher and decipheres the secret message which scrambles a message into an understood form. There are three kinds of cryptography algorithm. The first type is symmetric known as (secret key) encryption using a single key for both encryption and decryption. The second one is asymmetric known as (public key) encryption using two keys (i.e., one for encryption and another for decryption) (Aung and Naing). The last type of cryptography algorithm is a hash function based on a mathematical formula to generate a small size of digits that is generated from a large sized file, and it does not have a key (Raphael and Sundaram 2011).

B. Steganography:

Steganography is a technique for hiding and retrieving the secret message without raising suspicions. The secret message is transmitted from a sender to a receiver during an open channel depending on the digital medium such as audio, video, text, and image. The steganography approaches can be classified into three types: pure steganography, secret key steganography, and public key steganography. Different methods are proposed for steganography as follows:

- 1- Least significant bit (LSB).
- 2- Pixel value difference (PVD).
- 3- Modulus pixel value difference.

- 4- Patch reference table pixel value difference (PRT-PVD).
- 5- Transform domain.
- 6- Spread spectrum.

The present work aims to achieve a higher level of robustness and provide a better image quality due to a combination of cryptography and steganography to enhance the security of the embedded data [(Abikoye Oluwakemi, Adewole Kayode *et al.* 2012), (Song, Zhang *et al.* 2011)]. In this paper, The AES algorithm is used for cryptography; whereas PRT-PVD method is used for steganography to transmit a small size secret image carried by a big size image. This paper is divided into six sections. Section 1 presents the introduction, section 2 provides a detail description of AES encryption algorithm. The principles of PRT-PVD technique is described in section 3. Section 4 presents the proposed method. Section 5 discusses the experimental results. Finally, the conclusion is drawn in section 6.

II. The AES algorithm for cryptography

The AES algorithm is composed of a series of fixed steps that should be followed to encrypt and decrypt the original message by the sender and the receiver respectively. The original message is called a plaintext, and the encrypted form is a cipher text (Nechvatal, Barker *et al.* 2000). The cipher text contains all of the original information of the plaintext. However, in an unreadable form, only the desired receiver can extract it by using a suitable secret key for decryption. The input of the AES algorithm consists of 128 bits (16 bytes) sequence

that is converted into 4×4 arrays, which is sometimes named a 'state'. Three sequences 128, 192, and 256 bits of cipher key can be used for the AES algorithm. The advantages of the AES algorithm are simple design, low cost, resistance against adversary, and provide high security level [(Daemen and Rijmen 1999), (Mohan and Reddy 2011)].

The AES algorithm has fixed steps inside a loop repeated for N_r times. Where N_r is the number of rounds take values of 10, 12 or 14 that depends on the length of a cipher key. The general block diagram of encryption and decryption of the AES algorithm is shown in Figure 3. The input data (plain text) will go through the steps illustrated in Figure 3 in order to get the cipher text at the sender's side whereas the same procedure but in a reverse direction is used at the receiver side to get back the plaintext back from the cipher text. The main steps of the AES algorithm are as follows:-

- **SubBytes:** is a nonlinear transformation for byte-by-byte substitution by using a special designed table that operates on each of the state bytes independently.
- **ShiftRows:** a process of cyclically shifting the last three rows of the state by different offsets.
- **MixColumns:** a transformation in the cipher that takes all of the columns of the state and mixes their data (independently of one another) to produce new columns.
- **AddRoundKey:** a Round Key is added to the state by a simple bitwise XOR operation

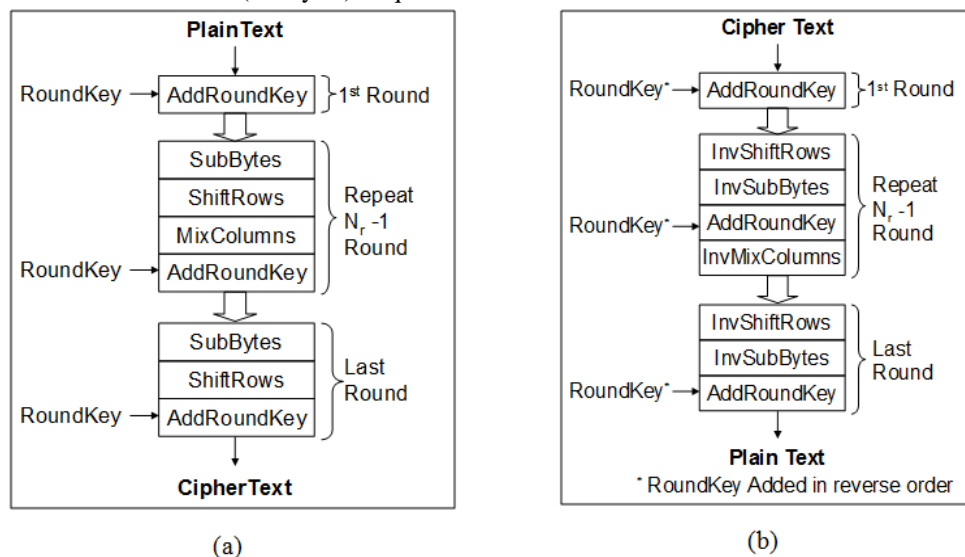


Fig. 3: The Diagram of AES Algorithm: (a) Encryption, (b) Decryption.

III. PRT-PVD technique for image steganography:

The recent image steganography technique can be classified into two main branches. One is spatial domain, and the other is transform domain. Spatial domain schemes are more popular in all applications of steganography than transform domain. In fact,

spatial domain schemes are simple, fast and have a low distortion. PRT-PVD is one of the spatial domain methods that uses medium such as texts, audios, videos, and images to embed the secret message guided by a reference table (Hong 2013). The main feature of this technique is the robustness

against intruders. Also, it's provides a high quality of image by using a special patch that exploited to construct the reference tables.

A. Design of the reference tables:

The reference table is filled with a non-repeated random number of values in the range of $(0, \dots, 2^{2k}-1)$, where $(k=1, 2, 3, \text{ or } 4)$ is the number of bits that will be embedded in each pixel. Generally, each pixel in a color or grayscale image represent by 8 bits where its decimal ranges from 0 to 255. So that, the size of a reference table must be 256×256 to include the pixel value range. The reference table is constructed by using a specially designed patch to

reduce the embedding impact on image quality. The base of numbers used in construction the reference table is 2 to avoid the conversion between bases and eliminate the consumed time in conversion process. As displayed in Figure 4, a four search regions can be used to construct four different reference tables with different payloads (Hong 2013). Based on a specific search region, a reference table is filled through patching the same search regions horizontally and vertically. In this work, a single threshold is chose to divide the range 0-255 into two sub-ranges. Consequently, two reference tables are used to embed 1bbp and 2bbp namely reference table 1 and reference table 2, respectively.

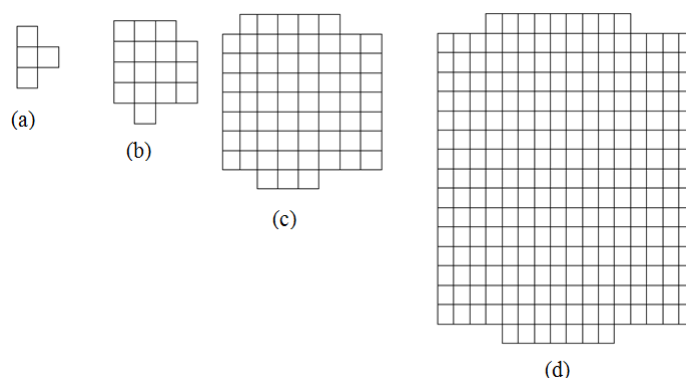


Fig. 4: The Search Regions of Reference Tables for Embedding. (a) 2-bits, (b) 4-bits, (c) 6-bits, (d) 8-bits per Pixel Pair.

B. Embedding and De-embedding algorithm:

The construction of embedding sequence can start after the required reference tables. First, a binary matrix with the same size of cover image is initialized with zero values. Then, raster scan is used to visit every location in the binary matrix. The first pixel location of pixel pairs is selected sequentially but the second pixel location is selected randomly from positions to the right, bottom right, bottom, and left bottom of the current location. At the receiver's side, the recipient must have the same seed that serves as a key to construct the same embedding sequence from the cover image. After the construction of required reference tables and embedding sequence, the embedding and de-embedding process can be started.

The cover image is scanned based on the embedding sequence to collect the pixel pairs' values. Then, the absolute difference between these two pixels is calculated and compared with threshold levels (threshold is used to divide the interval $[0,255]$ into sub-intervals) to know the number of bits that will be embedded in this pair and thus, which reference table must be used. After that, the desired secret message bits are converted into a decimal value. A selected pixel pair is located at a position in the reference table. Search around this position in the table to find a location that satisfies these two

conditions: (1) the position must contain the same value of secret bits, and (2) the difference between the horizontal and vertical values of the location must be in the same interval of the original pixel pair. Finally, the original pixel pair is substituted by the horizontal and vertical values of that location. This routine is repeated until the secret message is completely hidden. The flowchart of the embedding process is shown in Figure 5. For de-embedding at the receiver's side, the opposite process must be done. The recipient constructs the required reference tables and the embedding sequence similar to the one that is already constructed by the sender based on the same seeds. The retrieve process is simpler than the embedding process. A chosen pair of pixel values based on the embedding sequence is located on the reference table after the absolute difference between these two pixels is calculated and compare with the threshold levels. After that, the content of the selected location in the reference table is collected and converted into a binary form. The process is repeated depending on the length of the secret message and stopped when all secret bits are collected. The Peak Signal to Noise Ratio (PSNR) depends on the value of threshold. The highest value of PSNR is recorded when a threshold value increases. On the contrary, the payload decreases. As a result, a better image quality is achieved.

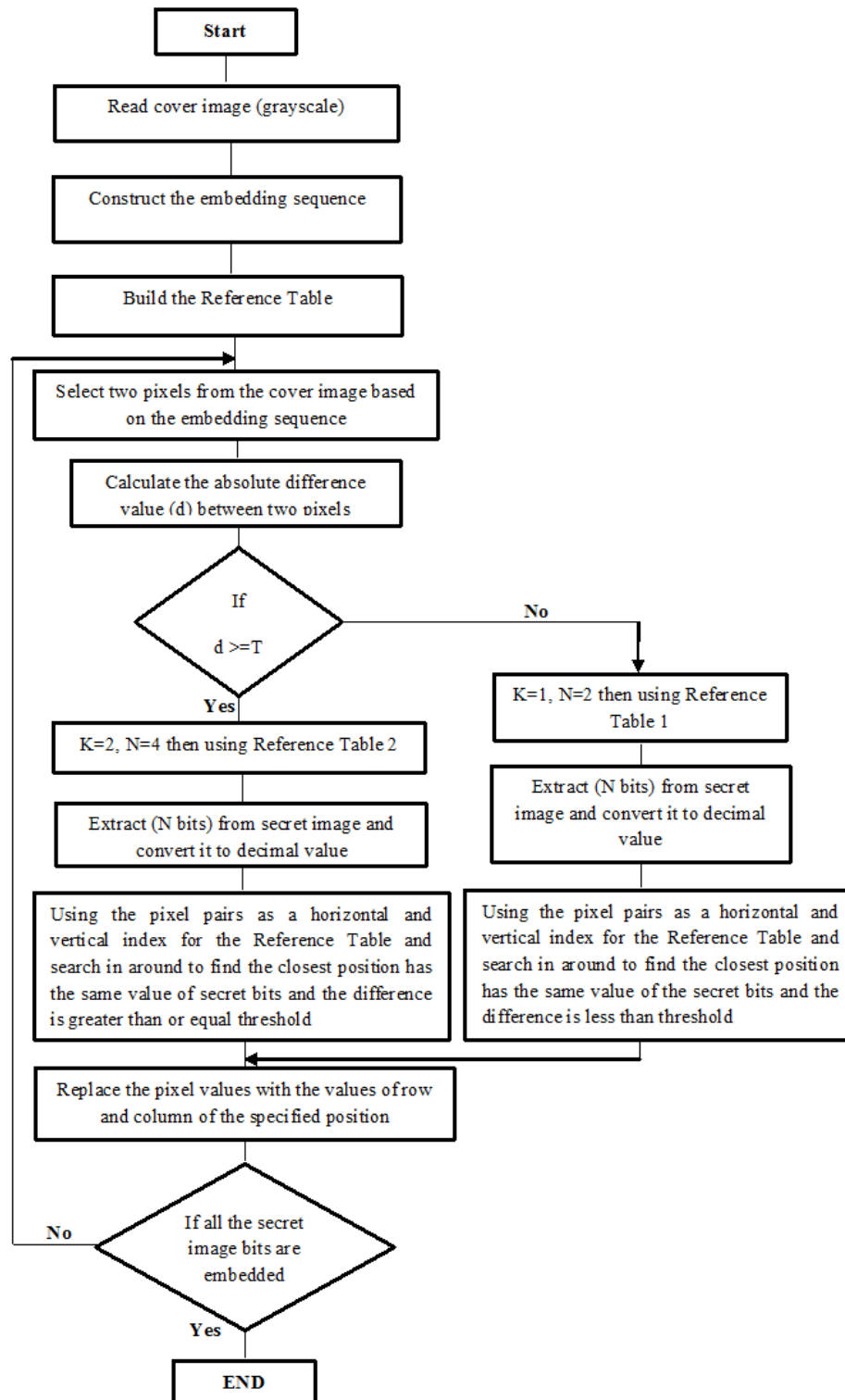


Fig. 5: Flowchart of Embedding Algorithm of PRT-PVD.

IV. Proposed Approach:

Certainly, using a combination of the cryptography and steganography techniques together is an effective way to increase the security, robustness and capacity of transmitted secret data through an open channel (Kumar and Sharma 2013). In this work, the AES encryption technique is used in

the first stage for ciphering the secret image. In the second stage the PRT-PVD steganography method is used to embed the cipher image into the cover image and obtain the stego-image (Hong 2013). Figure 6 and Figure 7 illustrate the flow chart of the proposed method at the sender and the receiver respectively.

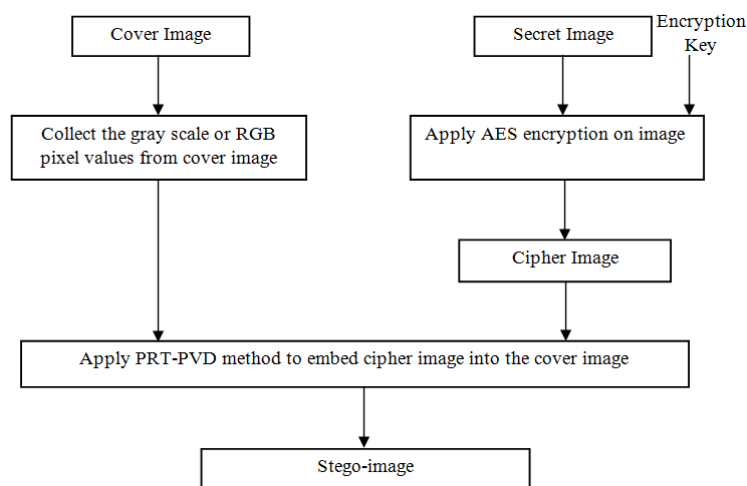


Fig. 6: The Process of Encrypting and Embedding the Secret Image into the Cover Image.

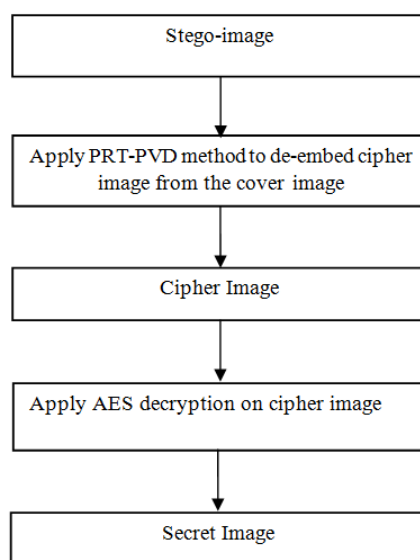


Fig. 7: The Process of Retrieving the Secret Image from the Stego-Image.

V. Experimental results:

The proposed approach has been successfully implemented using MATLAB. Figure 8 and Figure 9 display the secret image and the cover images respectively. The cover images are “Baboon”, “Lena”, “Scene”, “Gold hill”, “Jet”, and “Couple” with size 512×512, and the secret image is Monaliza with different sizes 200×200, 140×140, 92×92. By using AES encryption algorithm the secret image pixels were encrypted and converted to cipher image.

Then, the cipher image was hidden in the cover image by using PRT-PVD method. Peak signal –to–noise ratio (PSNR) represents the measurement of image quality that measures the average distortion between the original cover and stego-images. The output of each stage of the secret image (Monaliza) before and after encryption, as well as the cover image (Baboon) before and after embedding is indicated in Figure 10.

Table 1: The Values of PSNRs for Six Tests Cover Images of Size 512 ×512 with Three Sizes for Secret Image.

Cover images	Encrypted secret image size 200 x 200 PSNR	Encrypted secret image size 140 x 140 PSNR	Encrypted secret image size 92 x 92 PSNR
Baboon	48.2363	49.7898	51.6289
Lena	48.3211	49.8668	51.7151
Scene	48.2661	49.8441	51.6926
Gold hill	48.2343	49.8204	51.8027
Jet	48.4733	50.0535	51.8440
Couple	48.2394	49.8337	51.6916



Fig. 8: Secret Image.

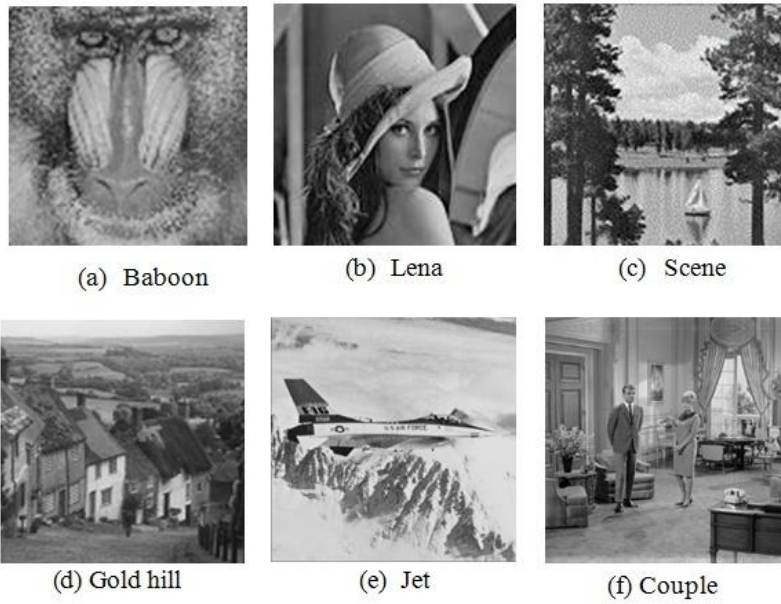


Fig. 9: Six Grayscale Cover Images of Size 512×512.

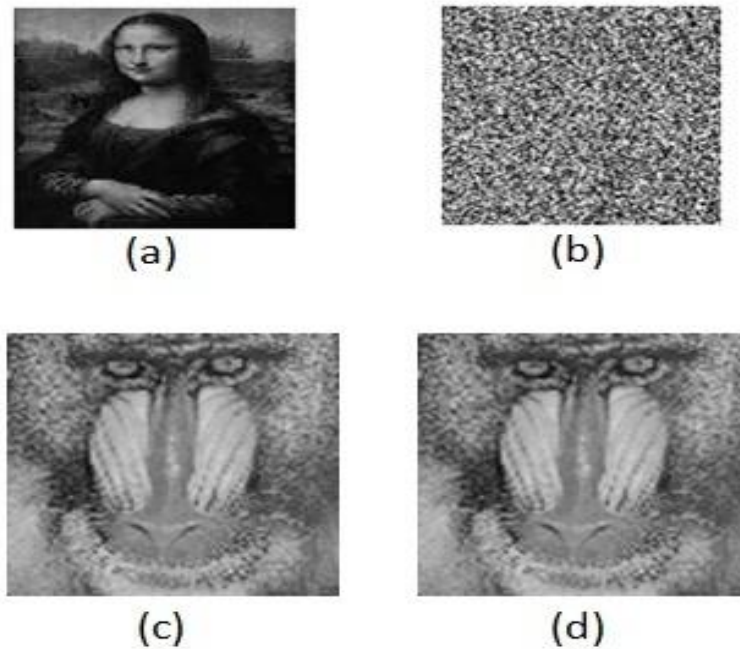


Fig. 10: Sample of a Cover and Secret Image at Different Stages: (a) Secret Image, (b) Encrypted image, (c) Cover Image, (d) Stego-Image.

Table 1 shows the PSNR of six different cover images were embedded by different secret image sizes based on PRT_PVD method. Similarly, the same thresholds $T=5$ is used. The experimental result reveals that the average PSNRs values depend on the size of the secret image. With this technique, it is observed that high PSNR and better image quality is achieved when the size of the secret image is small.

In addition, the difference histograms of Baboon cover image and the stego-image after embedding the secret image with three sizes is shown in Figure 11. Clearly, the difference histogram of the cover is similar to the stego-image that makes the proposed approach is more robust against the steganalysis tools such as difference histogram analysis.

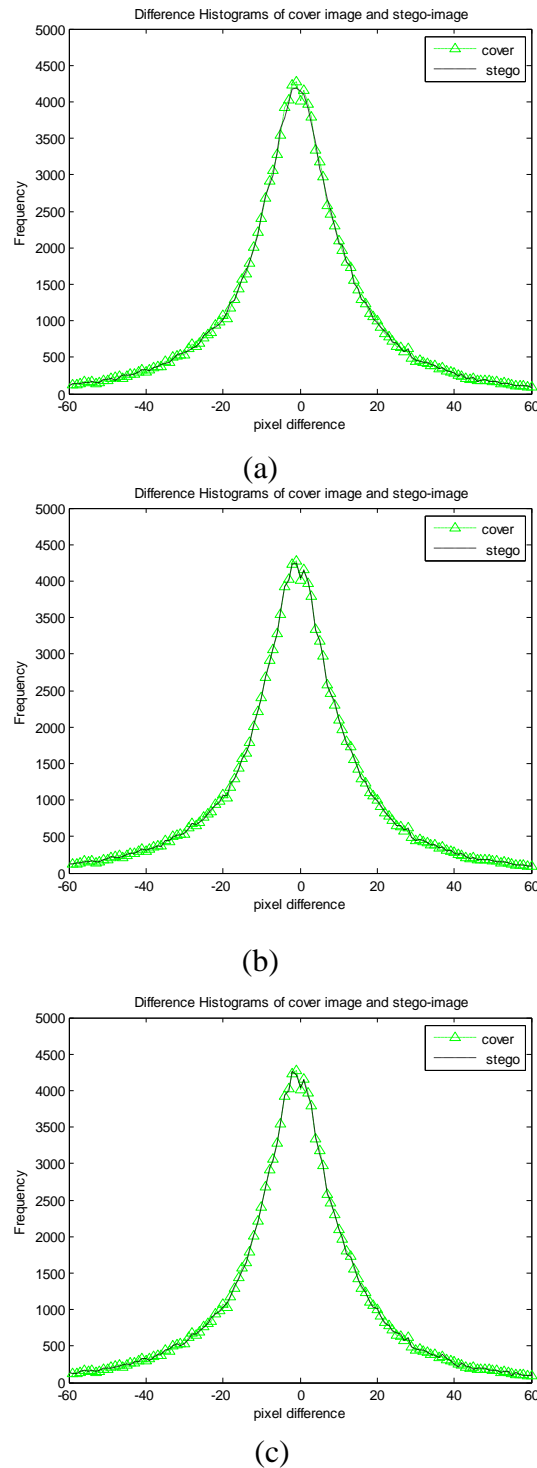


Fig. 11: Difference Histograms of the Grayscale Test Image Baboon Size 512 x 512 with Three Different Secret Image Sizes: (a) 200×200, (b) 140×140, and (c) 92×92.

VI. Conclusion:

Security of data communicated through the cloud is an important issue. Cryptography techniques were used in cloud computing to assure integrity of private data. But there are a numerous number of chances to break the cryptography techniques by the attackers. In this work, a data security scheme that combines cryptography and steganography techniques to provide multi-layers of security is presented. The AES encryption method is used to encrypt the secret image and the PRT_PVD scheme is used to hide the encrypted secret image inside the cover image file. The simulation results shows that the proposed approach provides a high image quality in term of PSNR. Moreover, it reduces the suspicion over the existence of hidden data in the image where the difference histogram of a stego-image is very close to the cover image.

REFERENCES

- Abikoye Oluwakemi, C., *et al.*, 2012. "Efficient Data Hiding System using Cryptography and Steganography". International Journal of Applied Information Systems, 4(11).
- Amini, M., *et al.*, 2014. "Development of an Instrument for Assessing the Impact of Environmental Context on Adoption of Cloud Computing for Small and Medium Enterprises". Australian Journal of Basic and Applied Sciences (AJBAS) 8(10): 129-135.
- Aung, P.P. and T.M. Naing. "AN ovel Secure Combination Technique of Steganography and Cryptography".
- Chen, N. and R. Jiang, 2014. "Security Analysis and Improvement of User Authentication Framework for Cloud Computing." Journal of Networks, 9(1): 198-203.
- Daemen, J. and V. Rijmen, 1999. "AES Proposal: Rijndael, AES algorithm submission". September 3, 1999 URL <http://www.nist.gov/CryptoToolKit>.
- Devi, T. and R.G. San, 2014. "Data security frameworks in cloud". Science Engineering and Management Research (ICSEMR), 2014 International Conference on, IEEE.
- Dong, L. and M. Ku, 2010. "Novel (n, n) secret image sharing scheme based on addition". Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE Computer Society.
- Hong, W., 2013. "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique." Information Sciences, 221: 473-489.
- Khalil, I.M., *et al.*, 2014. "Cloud computing security: a survey". Computers, 3(1): 1-35.
- Kumar, A. and R. Sharma, 2013. "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique". International Journal of Advanced Research in Computer Science and Software Engineering 3(7).
- Mohan, H. and A.R. Reddy, 2011. "Performance analysis of AES and MARS encryption algorithms". JCSI International Journal of Computer Science Issues, 8(4): 1694-0814.
- Murakami, K., *et al.*, 2013. "Improvement of security in cloud systems based on steganography". Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), 2013 International Joint Conference on, IEEE.
- Nechvatal, J., *et al.*, 2000. Report on the development of the Advanced Encryption Standard (AES), DTIC Document.
- Nimmy, K. and M. Sethumadhavan, 2014. "Novel mutual authentication protocol for cloud computing using secret sharing and steganography". Applications of Digital Information and Web Technologies (ICADIWT), 2014 Fifth International Conference on the, IEEE.
- Ramachandran, A.B., *et al.*, 2013. "Security as a Service using Data Steganography in Cloud". Proceedings of the International Conference on Cloud Security Management: ICCSM 2013, Academic Conferences Limited.
- Raphael, A.J. and V. Sundaram, 2011. "Cryptography and Steganography- A Survey". International Journal of Computer Technology and Applications, 2(3).
- Shukla, C.P., *et al.*, "Enhance Security in Steganography with cryptography".
- Song, S., *et al.*, 2011. "A novel secure communication protocol combining steganography and cryptography." Procedia Engineering, 15: 2767-2772.
- Zadiraka, V. and A. Kudin, 2013. "Cloud computing in cryptography and steganography". Cybernetics and Systems Analysis, 49(4): 584-588.