PERFORMANCE ANALYSIS OF TEXT AND IMAGE STEGANOGRAPHY WITH RSA ALGORITHM IN CLOUD COMPUTING

Ismail Abdulkarim Adamu and Boukari Souley
Department of Mathematical Sciences, Abubakar Tafawa Balewa University Bauchi, Nigeria

ABSTRACT

Cloud computing provides a lot of shareable resources payable on demand to the users. The drawback with cloud computing is the security challenges since the data in the cloud are managed by third party. Steganography and cryptography are some of the security measures applied in the cloud to secure user data. The objective of steganography is to hide the existence of communication from the unintended users whereas cryptography does provide security to user data to be transferred in the cloud. Since users pay for the services utilize in the cloud, the need to evaluate the performance of the algorithms used in the cloud to secure user data in order to know the resource consumed by such algorithms such as storage memory, network bandwidth, computing power, encryption and decryption time becomes imperative. In this work, we implemented and evaluated the performance of Text steganography and RSA algorithm and Image steganography and RSA as Digital signature considering four test cases. The simulation results show that, image steganography with RSA as digital signature performs better than text steganography and RSA algorithm. The performance differences between the two algorithms are 10.76, 9.93, 10.53 and 10.53 seconds for encryption time, 60.68, 40.94, 40.9, and 41.85 seconds for decryption time, 8.1, 10.92, 15.2 and 5.17 mb for memory used when hiding data, 5.3, 1.95 and 17.18 mb for memory used when extracting data, 0.93, 1.04, 1.36 and 3.76 mb for bandwidth used, 75.75, 36.2, 36.9 and 37.45 kwh for processing power used when hiding and extracting data respectively. Except in test case2 where Text steganography and RSA algorithm perform better than Image Steganography and RSA as Digital Signature in terms of memory used when extracting data with performance difference of -5.09 mb because of the bit size of the image data when extracted. This research work recommend the use of image steganography and RSA as digital signature to cloud service providers and users since it can secure major data types such as text, image, audio and video used in the cloud and consume less system resources.

Keywords

Cloud Computing, Text Steganography, Image Steganography, RSA algorithm.

1. INTRODUCTION

Modern advancement in communication technologies has resulted in the widely and increase in use of the cloud resources by different users[14], [3], [1]. The various resources used in the cloud include software, servers, network, storage etc. payable on demand according to their usage [14]. The major drawback of cloud computing is the vulnerability of user data to malicious attack or intruders [13]. The most novel approach to arrest the security challenges in the cloud used by researchers is cryptography and steganography [2]. The both mentioned techniques are used to protect data but in different fashions [6]. Cryptography concerns itself with the masking of the content of a secret message whereas steganography deals with the concealment or hiding of a secret message from an unauthorized person [7]. Since, users pay for their services according to the resource consumed, the need to evaluate the performance of various security techniques used in the cloud against the resources they consumed becomes imperative. The major objective of this work is to do performance analysis of digital text and image steganography. RSA cryptosystem is

employed for secret information confidentiality and authentication. Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. The data types used for the analysis include text, image, audio and video whereas the system resources considered are encryption and decryption time, memory consumption, processing power usage and bandwidth utilization.

2. LITERATURE REVIEW

2.1. Text Steganography

This technique involves hiding the existence of communication within a text file. In text steganography, the text used for communication is formatted by altering the arrangement of the text without affecting its real content in order to achieve a secure communication. The method involves line shift coding, word shift coding and feature coding [5], [16].

2.1.1 Categories of Text steganography

Text steganography can be broadly classified into the following as stated by [4] and [10].

2.1.1.1 Format Based Methods

The format based method involves altering the format of the original text to be communicated with to the recipient of the text into a secret text that cannot be understood by unauthorized users. The format-based method has some major drawbacks such that if the secret text is open in a word processor it will contain so many misspelling and white spaces, the font size could also be changed which might arouse suspicion. Finally, if the original text becomes available, comparing the suspected stegano text would make the manipulated parts within the text visible.

2.1.1.2 Random and Statistical Generation

The random and statistical method conceals text information in a random looking sequence group of characters. Mostly stenographers do this in order to avoid the challenges of comparison with a known plain text by generating their own text cover. In addition, in other techniques the statistical properties of word length and letter frequencies are used to generate words that will appear to have the same statistical properties as the actual text word in the given language.

2.1.1.3 Linguistic Steganography

The linguistic steganography generally considers the linguistic characteristics of generated and edited text and in many situations, uses linguistic structure as the space in which the message is concealed. Context Free Grammar (CFG) creates tree structures which are used for hiding the bits such that the left branch represent ‘0’ and the right branch correspond to ‘1’. In some cases, a grammar in Greibnach Normal Form (GNF) is also used where the first choice in the production represents 0 and the second choice represents bits 1. Linguistic steganography has some limitation such as a small grammar will lead to the repetition of a lot of text. Moreover, even though it has good syntactical arrangement, it lacks semantic structures by having a result of string of sentences that has no relationship to one another.

2.2. IMAGE STEGANOGRAPHY

Image steganography is the process of hiding the existence of data to achieve a secure communication by using image cover. In this technique, the content to be transferred is hidden within an image folder in order to make the content not to look suspicious to intruders. There are different methods used for image steganography such as least significant bit insertion, Masking and filtering, redundant pattern encoding, encrypt and scatter, Algorithms and transformation techniques [15].

2.2.1 Categories of Image steganography

Image steganography technique as identified by [9] is categorized as listed below:

2.2.1.1 Spatial Domain Method

The spatial domain method involves changing some bits of the image pixel value to be used in concealing the secret message or data. There are various types of spatial domain method image steganography used such as Least Significant Bit (LSB), Pixel Value Differencing (PVD), Edges Based data Embedding method (EBE), Random Pixel Embedding method (RPE), mapping pixel to hiding data method, labelling or connective method, pixel intensity method, texture based method and histogram shifting method. Among all the mentioned different type of spatial domain methods, the most commonly used is least significant bit method because it can be used to hide secret message in LSB pixel value without exposing any perceptible distortion to human eyes. The change in the pixel values using LSB method is usually not perceptible to human eyes.

2.2.1.2 Transform Domain Techniques

In transform domain techniques, the secret message is embedded within the frequency domain of the cover image. It is one of the most complex image steganography technique because it involves the combination of different algorithms and transformation on the image within which the secret message is to hidden or the cover image. It is one of the strong image steganography technique used today because it hide message in an image in areas that are less exposed to cropping, compression and image processing. Some types of transform domain technique are Discrete Fourier Transformation Technique (DFT), Discrete Cosine Transformation Technique (DCT), Discrete Wavelet Transformation Technique (DWT), lossless or reversible method and embedding in coefficient bits.

2.2.1.3 Distortion Techniques

In distortion technique, a stegano object is created by applying some sequence of changes to the cover image to be used to convey the secret data. The sequence of modification created is used to match the secret message to be transmitted. The encoder adds the sequence of the modification created to the cover image. In this technique, information is stored by signal distortion. In order to extract the original message from the cover image, the decoder needs to have the knowledge of the original cover image and the distorted cover image in order to restore the secret data.

2.2.1.4 Masking and Filtering

This technique hide secret information in a more significant area by marking the image in the same way as to paper watermarking than just hiding it into the noise level. The advantage of this technique is that it is more robust than LSB technique but suffers the drawback of only being applicable to grey scale images and restricted to 24 bits images.

2.3. RSA ALGORITHM

RSA algorithm is a public key cryptography algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [17], [11]. The algorithm involves multiplying two large prime numbers to obtain a public and private keys that can be used for providing security on data. RSA algorithm involves three steps such as key generation, encryption and decryption [11], [12].

2.3.1 RSA Key Generation Phase

To secure data using RSA algorithm, the first step is to generate the Keys that will be used to protect the data using two large prime integers. The steps for generating RSA private and public keys are listed below:

Steps:
Step1: Choose two distinct prime numbers x and y. For security purposes, the integers x and y should be chosen at random and should be of similar bit length.
Step2: Compute n = p * q
Step3: Compute Euler's totient function, Ø (n) = (p-1) * (q-1).
Step4: Chose an integer e, such that 1 < e < Ø (n) and greatest common divisor of e, Ø (n) is 1. Now e is released as Public-Key exponent.
Step5: Now determine d as follows: d = e-1(mod Ø (n)) i.e., d is multiplicative inverse of e mod Ø (n).
Step6: d is kept as Private-Key component, so that d * e = 1 mod Ø (n).
Step7: The Public-Key consists of modulus n and the public exponent e i.e., (e, n).
Step8: The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e., (d, n).

2.3.2 RSA Encryption Phase

Once the public and private keys have been generated, the next thing is to encrypt the message that is needed to be secured using the RSA pubic Key.

Steps:
Step1: The Public- Key (n, e) is shared between the cloud service providers and the client or user.
Step2: The message to be communicated between the two parties is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
Step3: The message is encrypted and the resultant cipher text (data) C is: C = me (mod n).
Step4: The generated cipher text or encrypted message is now kept with the client.

2.2.3 RSA Decryption Phase

To have access to the encrypted message the client need to decrypt the message in order to be able to see the original message. To decrypt the message involve the following steps:

Step1: The client request for the message from the cloud service provider.
Step2: The cloud service provider now verifies the authenticity of the client and gives the encrypted data i.e., C.
Step3: The client then decrypts the data by computing, m = Cd (mod n).
Step4: Once m is obtained, the client can get back the original data by reversing the padding scheme.

2.4. METHODOLOGY

The major concern of this work is to evaluate the performance of the security model in cloud computing proposed by [4] using RSA as digital signature and Image Steganography to secure user data in the cloud with a developed security model in the cloud using Text Steganography and RSA algorithm

2.4.1 Working principle of RSA as digital signature and Image Steganography

The working principle of RSA as digital signature and Image steganography as proposed in [4] is shown in figure1 below.

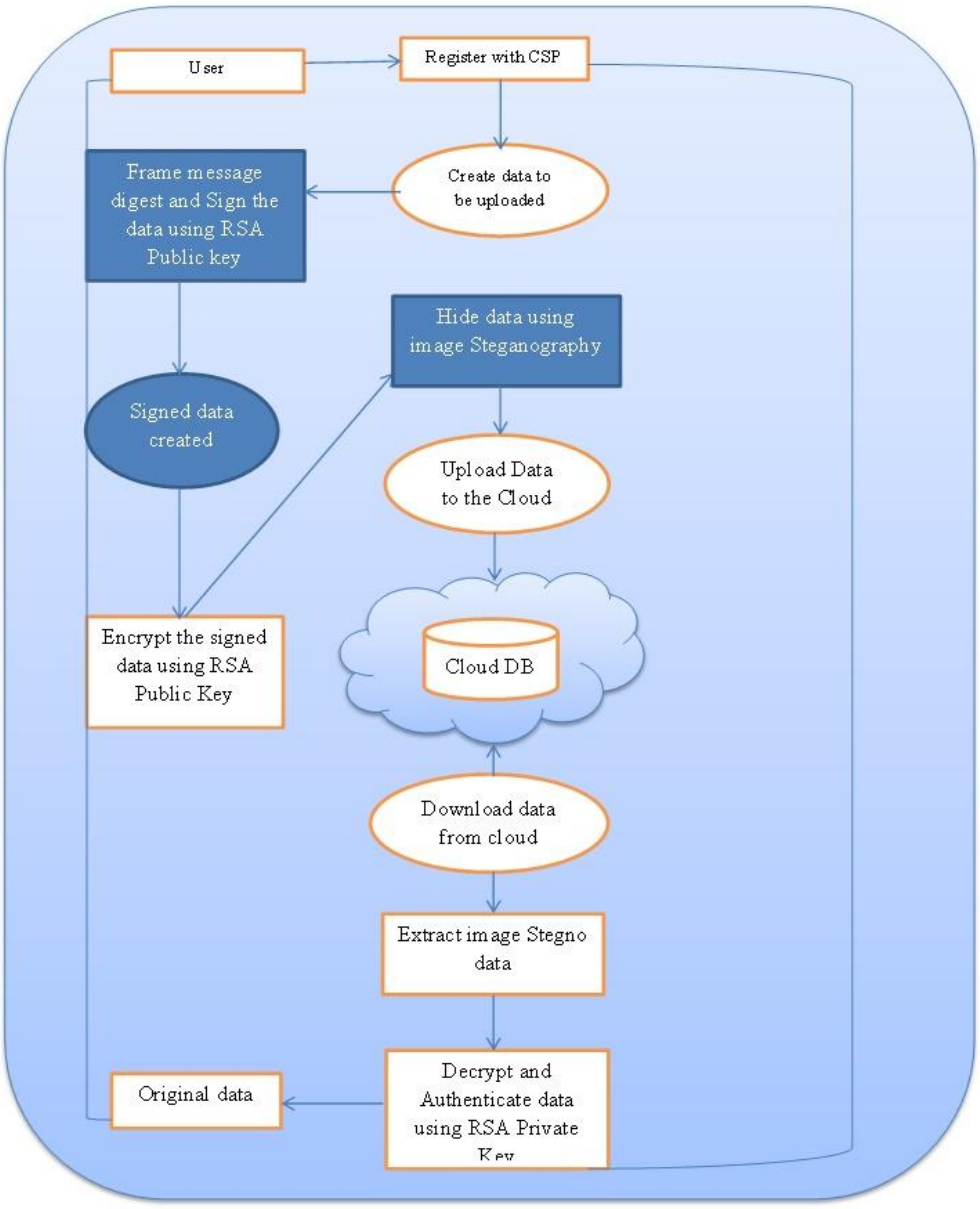

Figure1. Security model in the cloud proposed in [4]

2.4.2 Simulation Tool

The proposed model was implemented and evaluated using java NetBeans IDE 8.0.2 programing environment on HP laptop System Corei (TM) i5-4200U, 2.30GHz CPU, 8GB RAM and 1200 watt system processing power using different input data types and size such as 479 kb for text data, 532kb for Image data, 693kb for Audio data and 1926kb for Video data.

2.5. RESULT AND DISCUSSION

The security of data in the cloud is one of the major concerns of cloud users. In addition, developing a security technique that performs effectively and consumes less resources to the users in order to minimize cost by the users is very important since users pay for the resources utilized in the cloud according to the size of resource consumed. In this section, we discussed the resources consumed and the time it takes to encrypt and decrypt data by both Image steganography and RSA as digital signature and Text Steganography and RSA algorithm. After conducting four (4) test cases of simulation runs the following result were obtained as shown in table1 below.

Table1. Comparison of experimental results

Test cases	**Data types**	**Data Size (kb)**	**Resources consumed**	**Text Steganography and RSA Algorithm**	**Image Steganography and RSA as Digital Signature**	**Performance Difference between the two algorithms**
Case 1	Text1 / Text	479	Encryption time (s)	16.63	5.87	10.76
			Decryption time (s)	61.35	0.67	60.68
			Memory used when hiding data (mb)	16.36	8.26	8.1
			Memory used when extracting data (mb)	7.19	1.89	5.3
			Bandwidth Utilized (mb)	1.87	0.94	0.93
			Processing power usage (kwh)	83.60	7.85	75.75
Case 2	Text2 / Image	532	Encryption time (s)	15.60	5.67	9.93
			Decryption time (s)	41.40	0.46	40.94
			Memory used when hiding data (mb)	16.35	5.43	10.92
			Memory used when extracting data (mb)	1.44	6.53	-5.09
			Bandwidth Utilized (mb)	2.08	1.04	1.04

			Processing power usage (kwh)	43.56	7.36	36.2
Case 3	Text3 / Audio	693	Encryption time (s)	15.78	5.25	10.53
			Decryption time (s)	41.36	0.46	40.9
			Memory used when hiding data (mb)	20.39	5.19	15.2
			Memory used when extracting data (mb)	5.56	3.61	1.95
			Bandwidth Utilized (mb)	2.71	1.35	1.36
			Processing power usage (kwh)	43.75	6.85	36.9
Case 4	Text4 / Video	1926	Encryption time (s)	16.43	5.90	10.53
			Decryption time (s)	42.34	0.49	41.85
			Memory used when hiding data (mb)	12.18	7.01	5.17
			Memory used when extracting data (mb)	21.87	4.69	17.18
			Bandwidth Utilized (mb)	7.52	3.76	3.76
			Processing power usage (kwh)	45.12	7.67	37.45

2.5.1 Analysis of the experimental results

2.5.1.1 Resources Consumed in Test case1 using 479 kb of Text data types

Figure2 below shows the graphical representation of the resources consumed when hiding and extracting data for both Text Steganography and RSA algorithm and Image steganography and RSA as digital signature using 479 kb of text data types for both the algorithms.

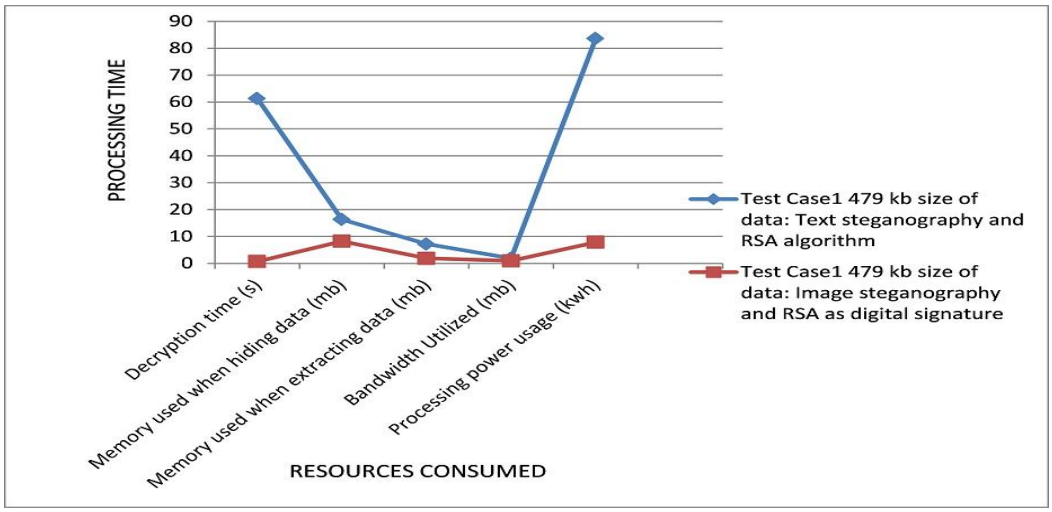

Figure2. Resources Consumed by both algorithms in Test Case1

2.5.1.2 Resources Consumed in Test case2 using 532 kb of Text and Image data types

Figure3 below shows the graphical representation of the resources consumed when hiding and extracting data for both Text Steganography and RSA algorithm and Image steganography and RSA as digital signature using 532 kb of Text and Image data types for both the algorithms.

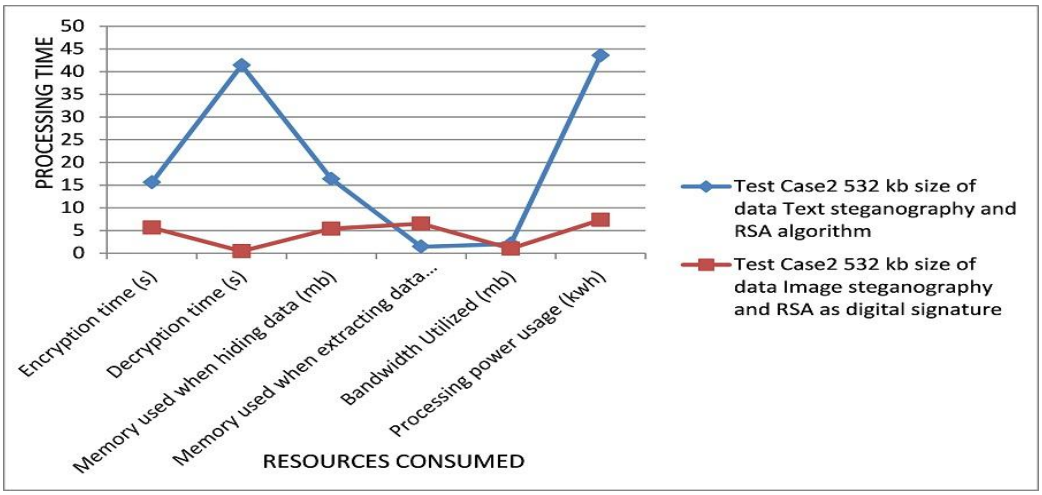

Figure3. Resources Consumed by both algorithms in Test Case2

2.5.1.3 Resources consumed in Test case3 using 693 kb of Text and Audio data types

Figure4 below shows the graphical representation of the resources consumed when hiding and extracting data for both Text Steganography and RSA algorithm and Image steganography and RSA as digital signature using 693 kb of Text and Audio data types for both the algorithms.

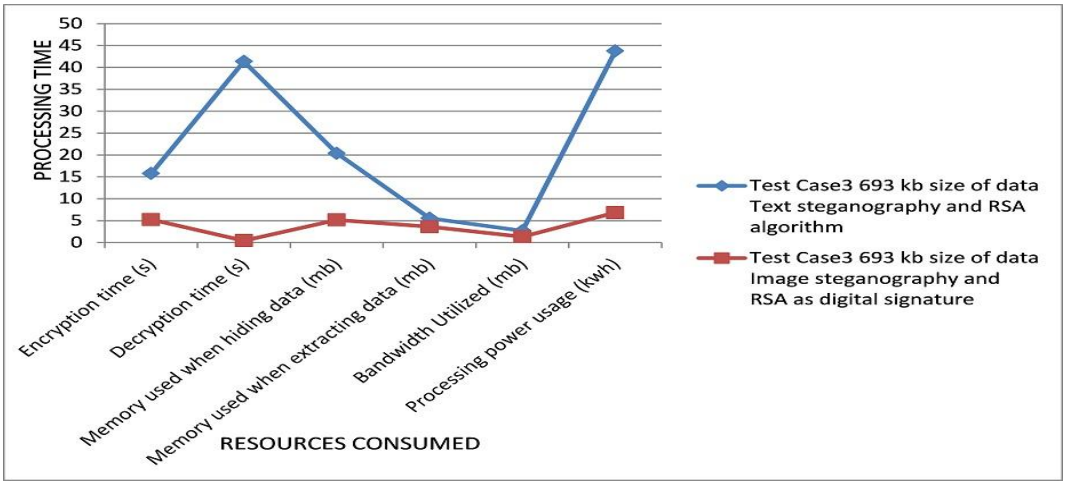

Figure4. Resources Consumed by both algorithms in Test Case3

2.5.1.4 Resources consumed in Test case4 using 1926 kb of Text and Audio data types

Figure5 below shows the graphical representation of the resources consumed when hiding and extracting data for both Text Steganography and RSA algorithm and Image steganography and RSA as digital signature using 1926 kb of Text and Video data types for both the algorithms.

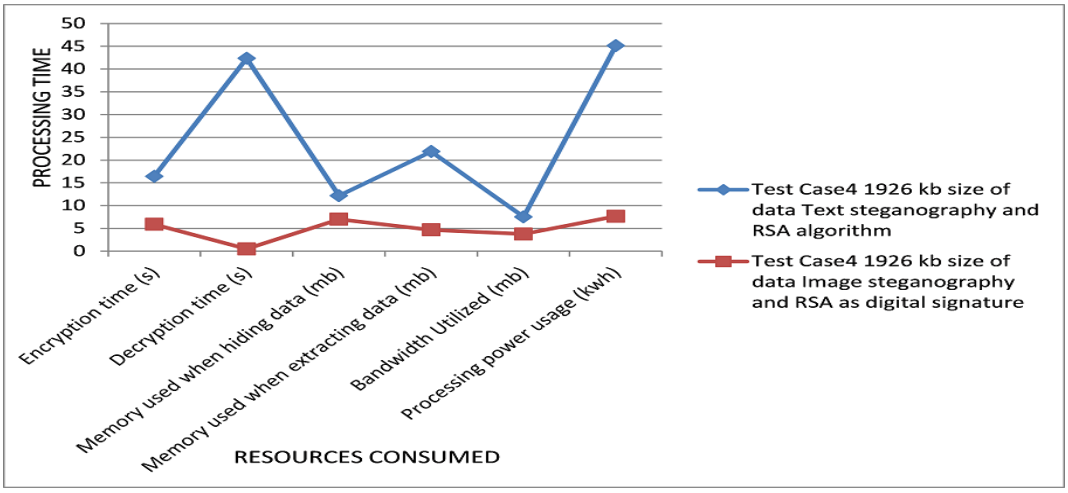

Figure5. Resources Consumed by both algorithms in Test Case4

2.5.2 Discussion of Result

2.5.2.1 Encryption time when hiding

As shown on the comparison of experimental result Table in table1 above, Text Steganography with RSA algorithm consumes more time than Image steganography with RSA as digital signature when hiding data. In the first, second, third and fourth cases the text steganography and RSA algorithm took 16.63, 15.60, 15.78 and 16.43 seconds to encrypt data while image steganography and RSA as digital signature took just 5.87, 5.67, 5.25 and 5.90 seconds to encrypt the same size of data. This is because text steganography and RSA algorithm contain a lot of libraries to search through in order to come out with corresponding secret text to be communicated with in disguise as the original text.

2.5.2.2 Decryption time when extracting data

In the first, second, third and fourth cases text steganography and RSA algorithm took 61.35, 41.40, 41.36 and 42.34 seconds to decrypt data while image steganography and RSA as digital signature took just 0.67, 0.46, 0.46 and 0.49 seconds to decrypt the same size of data. The analysis shows that, Text steganography and RSA algorithm takes longer time to get back the original data because it has to go through the same librabries used to concealed the text than Image steganography and RSA as digita signature; in order to restore back the original text from the corresponding text which consumes minut time to extract or get back the original data from the cover image.

2.5.2.3 Memory used when hiding data

The result of the analysis for memory consumption when hiding data shows that in the first, second, third and fourth cases text steganography and RSA algorithm consumed 16.36, 16.35, 20.39 and 12.18 Megabyte space to hide data. While Image steganography and RSA as digital signature consumed just 8.26, 5.43, 5.19 and 4.6 megabyte space to hide the same size of data. This indicates that, Text steganography with RSA algorithm consumes more memory space when hiding data. Because when concealing text data, a single line of text can be converted into ten (10) or more line of text drawn from different libraries in order to divert the attention of the user from identifying that the secret message is trying to convey an information or communication. The process of converting a single text into multiple texts causes the text steganography with RSA algorithm to consume more memory space compared to the image steganography with RSA as digital signature.

2.5.2.4 Memory used when extracting data

The result of the analysis for memory consumed when extracting data shows that text steganography with RSA algorithm consumes more space when extracting the concealed data compared to Image steganography with RSA as digital signature. This is because, in first, second, third and fourth cases text steganography with RSA algorithm consumed 7.19, 1.44, 5.56 and 21.87 megabyte space to extract the data while Image steganography with RSA as digital signature consumed just 1.89, 6.53, 3.61 and 4.69 megabyte space to extract the same size of data. Except in the second test case where Text Steganography and RSA algorithm perform better.

2.5.2.5 Bandwidth consumed when hiding and extracting data

The analysis shows that Text steganography with RSA algorithm utilized more bandwidth than Image Steganography with RSA as digital signature. The result in the first, second, third and fourth cases shows that Text steganography with RSA algorithm utilizes 1.87, 2.08, 2.71 and 7.52 mb to hide and extract data while Image Steganography with RSA as digital signature utilizes just 0.94, 1.04, 1.35 and 3.76 mb to hide and extract the same size of data. This is because the processing time it takes for the Text steganography with RSA algorithm to search through the libraries and convert the original text into corresponding text and back to the original text takes longer time compared to Image Steganography and RSA as digital signature, which makes it, consumes more bandwidth.

2.5.2.6 Computing power drop rate when hiding and extracting data

The result for computing power drop rate when hiding and extracting data shows that In the first, second, third and fourth cases text steganography and RSA algorithm processing power usage was 83.60, 43.56, 43.75 and 45.12 kwh when hiding and extracting data while Image

steganography and RSA as digital signature processing power usage was just 7.85, 7.36, 6.85, 7.67 kWh when hiding, and extracting the same size of data. The result indicates that with smaller data size, Text steganography and RSA algorithm consumes more battery power than Image steganography and RSA as digital signature. However, as the data keep increasing to larger size; Text Steganography with RSA began to improve in it processing power usage. This is because the more the size of the text to hide with Text steganography and RSA algorithm the less time it takes the Text steganography and RSA algorithm to browse through its libraries and convert the original text into a secret text and vice versa.

3. CONCLUSION

The increased demand and use of cloud resources by various users such as institution, organization and individuals has drawn so much attention of cloud service providers to provide strong security mechanism to secure and protect user's data from attacks or unauthorized access by malicious users and intruders. The used of hybrid security techniques such as steganography and cryptography provide strong security techniques to guarantee safety of user data in the cloud. The major advantage of combining cryptography and Steganography to secure user data in the cloud is to make the data difficult to access, modify by unauthorized users, and guarantee secure communication of the data over the cloud without drawing the attention of intruders. The analysis of the two adopted techniques Image steganography and RSA as digital signature and Text steganography and RSA algorithm in this research work shows that, image steganography and RSA as digital signature consumes less resource, executes data faster and provide more robust security compare to text steganography with RSA algorithm. Image steganography and RSA as digital signature can handle and hide both text, audio, video and image data types as compared to text steganography with RSA algorithm that can only handle and hide text data. Finally, the concept discussed in this research will help to build a strong architecture for security in the field of cloud computing. This kind of structure of security will also be able to improve customer satisfaction to a great extent and will attract more investor in this cloud computation concept for industrial as well as future research farms. In the future, we intend to carry out more simulations on the system in order to evaluate it performance with order different image steganography techniques proposed by other researchers.

REFERENCES

[1] B. M. Shereek, Z. Muda, and S. Yasin, "Improve Cloud Computing Security Using RSA Encryption WithFermat's Little Theorem," International organization of Scientific Research, vol. 4, no. 2, pp. 2278-8719, February 2014.

[2] D. Prasannan and R. Thomas, "Hybrid Technique for Hiding Data Inside Video Using Combined Cryptography and Steganography," International Journal of Innovative Research in Science, Engineering and Technology, vol. 6, no. 5, pp. 7775-7779, May 2017.

[3] G. Garikapati, D. Yakobu, G. Nitta, and J. Amudhavel, "An Analysis of Cloud Data Security Issues and Mechanisms," International Journal of Pure and Applied Mathematics, Vol. 116, no. 6, pp.141-147, 2017

[4] I. A. Adamu and S. Boukari, "An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography," International Journal of Scientific & Engineering Research, Vol 8, no. 7, pp. 1512-1517, July 2017.

[5] K. A. Kumar, S. Pabboju and S. N. Desai, "Advance Text Steganography Algorithms: An Overview," International Journal of Research and Applications, vol. 1, no. 1, pp. 31-35, March 2014.

[6] K. F. Rafat, and M. Sher, "StegRithm: Steganographic Algorithm for Digital ASCII," International Journal of Engineering and Technology, vol. 4, no. 6, pp. 765-769, December 2012.

[7] Manisha and D. Munjal, "A Review Paper of Dual Steganography Technique Using Status LSB and DWT Algorithms," International Journal of Computer Science & Engineering Technology, vol. 7, no. 5, pp. 233-237, May 2016 .

[8] M. Agarwal, "Text Steganography Approaches: A comparison," International journal of network Securities & Its Application, Vol. 5, no. 1, pp. 1-16, 2013

[9] M. Hussain and H. Mureed, "A Survey of Image Steganography Techniques," International Journal of Advanced Science and Technology, vol. 54, pp. 1-12, 2013

[10] M. N. Rao and L. Pamulaparty, "Text Steganography: REVIEW". International Journal of Computer Science and Information Technology & Security, vol. 6, no. 4, pp. 80-83, August 2016.

[11] N. Padmaja and P. Koduru, "Providing data security in cloud computing using public key cryptography," International Journal of Engineering Science Reserch, vol. 4, no. 1, pp. 1059-1063, 2013.

[12] N. Soumya and R. Prabha, "Cloud Computing: Data Security Using RSA," Internatonal Journal of Latest Research in Engineering, Management &Appled Science, vol. 4, no. 10, pp. 57-59, 2015.

[13] O. M. Ahmed and W. M. Abduallah, " A Review on Recent Steganography Techniques in Cloud Computing," Academic Journal of Nawroz University, Vol.6, no.3, pp.106-111, August 2017

[14] S. Kalra, K. Atal and R. Jain, "Security Issues in Cloud Computing," International Journal of Computer Applications, vol. 164, no. 2, pp. 37-41, June 2017.

[15] S. Pal and S. K. Bandyopadhyay,"Image Steganography using Block Level Entropy Thresholding Technique" Journal for Research, vol. 2, no. 4, pp. 9-11, June 2016.

[16] S. S. Iyer and K. Lakhtaria, "Clustering Algorithm for Text Steganography," International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no.3, pp. 74-77, Novemer 2016.

[17] S. Singhal, and N. Singhal, "A Comparative Analysis of AES and RSA Algorithms," International Journal of Scientific & Engineering Research, vol. 7, no. 5, pp. 149-151, 2016.