International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Enhancing the Security of Mobile Cloud Computing using Audio Steganography with Least Significant Bit Insertion

Seiba Alhassan
PHD Student KNUST

Mr. Lambert Bayor
PHD Student KNUST

***Abstract*:- Cloud Computing is an emerging and a popular technology that allows users to access and process Information from a remote location. These users use mobile applications to offload sensitive data over a network especially, the Internet to cloud. They are security and privacy issues that threaten data that is offloaded to cloud. One such problem is unauthorized access. Over the years, cloud administrators have put in place measures including encryption to prevent unauthorized access. However, there is no mechanism in place to prevent cloud administrator access to customer's data. This study therefore proposed Steganography which involves hiding the existence of information to enhance the data security of Mobile Cloud users. The study implemented the proposed system using audio Steganography with Least Significant Bits (LSB) Insertion. The implemented system was analysed in MATLAB. The results showed that the proposed system recorded a high Peak Signal to Noise Ratio (PSNR), low Mean Square Error (MSE) and high Embedding Capacity as compared to previous systems**

1. INTRODUCTION

Security of data is always important whenever communication is done and to achieve that purpose different techniques are used so that sensitive data will not be leaked to a third party (Saini et al,2017). In order to address this challenge, Steganography plays an important role (Bandyopadhay, Datta, B. and Ghoshay, 2010). According to Kumar and pooja (2010) Steganography is the art of hiding messages and an attempt to conceal the existence of embedded information. Steganography has a long history that dates back to the ancient Greek and Roman civilization (Warkentin and Schmidt, 2008). Also, according to Sharma et al (2014) Steganography can be traced back to ancient Greek when etching information in wooden tablets and casing them with polish was done. The increasing use of the Internet and the availability of digital data and its sharing have forced industry players and academia to pay particular attention to Information Security (Varsha and Chhillar, 2015). Modern Steganography involves concealing messages on a media file such as text, protocol, audio, images and video Morkel and Oliver, 2005). The use of images to conceal messages has the limitation of sending only few messages Reza and Sonawane, 2016). Due to the limitations of image Steganography stated above, this work is proposing audio Steganography to prevent cloud administrators access to customer's data in mobile cloud. The contribution of this work is that audio Steganography has the advantage of accommodating large data size send to Mobile Cloud as compared to image Steganography of the previous system. The proposed system ability to accommodate large size of client's data also means Mobile Cloud becomes more secure. The rest of the work is divided to five main sections namely the review of related literature, the methodology used, implementation, results and analysis and the conclusion.

2. REVIEW OF RELATED LITERATURE

2.1 Mobile Cloud Computing

The recent increased in the used of mobile devices to send data to cloud has also increased data security breaches and the leaking of sensitive customers data. The phenomenon however, has also help to improve the performance of mobile device increased battery life span and has made worker more productive. Due to the challenges and benefits that Mobile Cloud promise several research work has been done in the area.

Ibukum and Daramol (2015) conducted a study on Mobile Cloud Computing. The objective of their study was to identify area in Cloud Computing that are more researched and those that were less researched. Their study was successful since they were able to identify issues that were more researched and those that were less researched. Those issues that were less researched included security, privacy, trusts, and issues of architecture, context awareness and data management. Those issues that received much research included operations, end users, service and applications. However, this study was too theoretical and provided no practical solution to the several problems mentioned in this study. Also, Oskar (2012) conducted a study on mobile phone and Cloud Computing. His study aimed to investigate the effect on the performance of mobile device in terms of speed if those heavy applications were offloaded to cloud. To accomplish this, a proposed system was developed. The proposed system was tested by offloading heavy applications to cloud and recording the processing speed of the mobile device. Again, the proposed system was tested without offloading application and the time taken to process data was also recorded. The results showed that Cloud Computing was slower compared with using mobile phone itself. The strength of this work was that it provided a practical solution by developing a system. Apart from that, the system developed was in java and hence it was platform independent. Reza and Sonawane (2016) conducted a study to improve the security of Mobile Cloud Computing using Steganography. Their study basically looked at how Image Steganography can be used to enhance the security of mobile Cloud

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Computing. A proposed system was implemented in java using a simple case study. Their study was limited because the image Steganography used in their study could not send messages that were large in size. Another weakness of their study was that they failed to measure the performance of their proposed system. Their study however recommended the use of Video and Audio Steganography in the future.

2.3 Steganography

Reza Sonawane (2016) stated that cryptography has made it possible for people to send secret messages without any concern about their data being leaked or accessed by unauthorized persons. Their study identified that since unauthorized persons are prevented from having access to secret message; the major problem has to do with cloud administrators having access to customer data. They proposed Steganography as a technique for preventing cloud administrators from having access to customers‟ data. It is therefore clear from Reza and Sonawane (2016) argument that Cryptography and Steganography are methods for protecting data from cloud systems. Due to the increasing use of Mobile Cloud Computing it has become necessary for extensive research to be conducted on best methods to ensure secure data communication and storage. Steganography happens to be one of the methods of protecting data from hackers and attackers.

Similarly, Ramalingam (2011) contends that Steganography is the science of transforming secret information in a manner that prevents unauthorized persons from having access to such information. Again, (Xu, Ping, Zhang, 2006) opined that Steganography is a contemporary approach of convert communication whose primary objective is to hide data from unauthorized persons. Also, Patidar and Patidar (2015) argued that Steganography must necessarily prevent the reading of the content of an embedded message by a third party. For Steganography to provide the needed security and concealment from attackers, it must be based on appropriate techniques Distortion techniques, Spread Spectrum techniques, Transform Domain techniques, Substitution and Insertion are some of the Steganography techniques used to modify the covert media (Mathe, Atukuri and Devireddy, 2012). The components of Steganography are shown in the diagram below

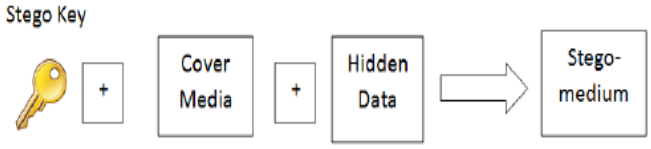

Figure 2.7: components of Steganography
Source: Odeh and Elleithy 2012

2.4 Types of Steganography

Several researchers have proposed various types of Steganography. The types of Steganography are classified based on the cover object used (Wajgade and Kumar, 2013). Morkel and Oliver (2005) mentioned text, images, audio, video and protocol as major media used for Steganography. Also, according to Rana, Sangwan and Jangir (2012) there are four types of Steganography depending on the cover media as text, image/audio, video and protocol. The argument made by Rana, Sangwan and Jangir (2012) is almost the same as that of (Morkel and Oliver, 2005). The protocol that appears in the works of Wajgade and Kumar (2013) and Morkel and Oliver (2005) was because TCP/IP packets were recognized as capable of hiding information. Even though the protocol Steganography exist, the most popular ones are text, audio, images and video. Khot and Patil (2015) supported the argument that the four media types are the most used when they opined that the four types of cover objects that are mainly in use are text, image, audio and video. Khot and Patil (2015) however failed to acknowledge TCP/IP ability to hide secret message. Amina and Fareeha (2014) proposed five types of Steganography which they listed as text, image, audio, and video and network protocol. From the views of the researchers above, Steganography has to do with hiding information from people who are not authorized to access such information using cover media such as text, images, audio, video and protocol.

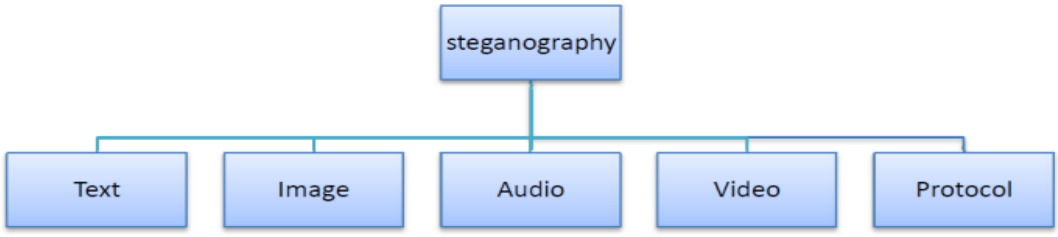

Figure 2.8: Types of Steganography
Source: Amina and Fareeha 2014

2.4.1 Audio Steganography

Audio Steganography is a technique used to send secret information by modifying audio signals in an imperceptible manner Doshi, Jain and Gupta (2012). According to Jayaram, Ramganath and Anuapanma 2011) the basic model of audio

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Steganography is made up of a cover media which is the original audio file .The original file serves as a medium for embedding data or secret messages. The second part of the model is the key that serves as a password and prevents unauthorized people from having access to the secret message. The third part is the message that is to be embedded into the audio file. The cover audio, the key and the message together is known as a stego audio. The figure 2. 9 shows the basic model of audio Steganography. An audio file is first selected as a medium to hold the secret message. The secret message and the key is then added to form a stego audio, using an embedding module

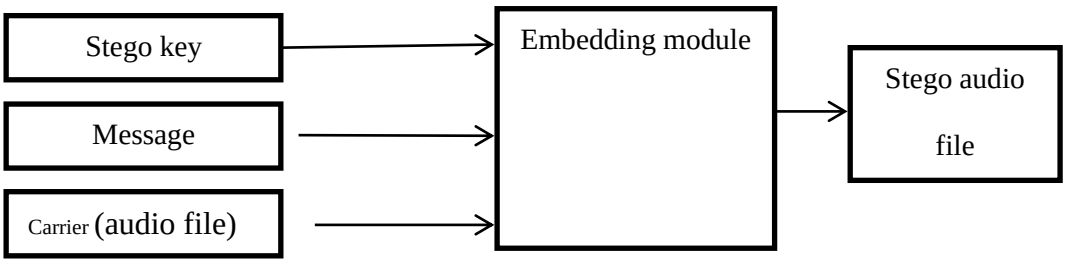

Figure 2.9: Basic Audio Stenographic Model
Source: Doshi , Jain and Gupta 2012

2.5 Least Significant Bits (LSB)

The simplest approach to hiding data within an image file is called Least Significant Bit (LSB) insertion Habibi, Karimi and Nosralnti (2013). Replacing the Least Significant Bits in Steganography does not result in much difference between the cover audio and the stego audio (Reza and Sonawane, 2016). This is so because the change in maximum displacement of the signals from their original position is small (Amin et al, 2003). According to Kamred (2014) LSB coding technique makes use of less computer resource such as memory and time of execution because of its low computational complexity. Also, according to Deshpande et al (2015) LSB, as a Steganography technique replaces the Least Significant Bits in the cover audio with the bits from the secret message. It is extremely difficult for the human eye to discriminate between a 21bit color and 24 bit colour (Juneja and Sandhu 2009).

METHODOLOGY

3.1 Proposed Model

The proposed model shown in Figure 3.1 is a detail description of how customers of Mobile Cloud would have their data protected from unauthorized access. The components of this model include a key and data or secret information. Any user with a mobile device such as a Laptop or a smart phone having the stego application (SA), that act as an interface between the sender of the secret data and the receiver. The components also include an embedded audio and a cloud system. This model make use audio as a cover media for hiding the secret data. The data that is embedded into the model becomes an input file which is then send over a communication channel to a receiver. To be able to retrieve the data, the intended recipient must have the right software and privilege to be able to access the secret data. This means that even if an attacker gets access to the audio file he still need the right software and the privilege to retrieve the secret data and hence making the proposed system very secure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

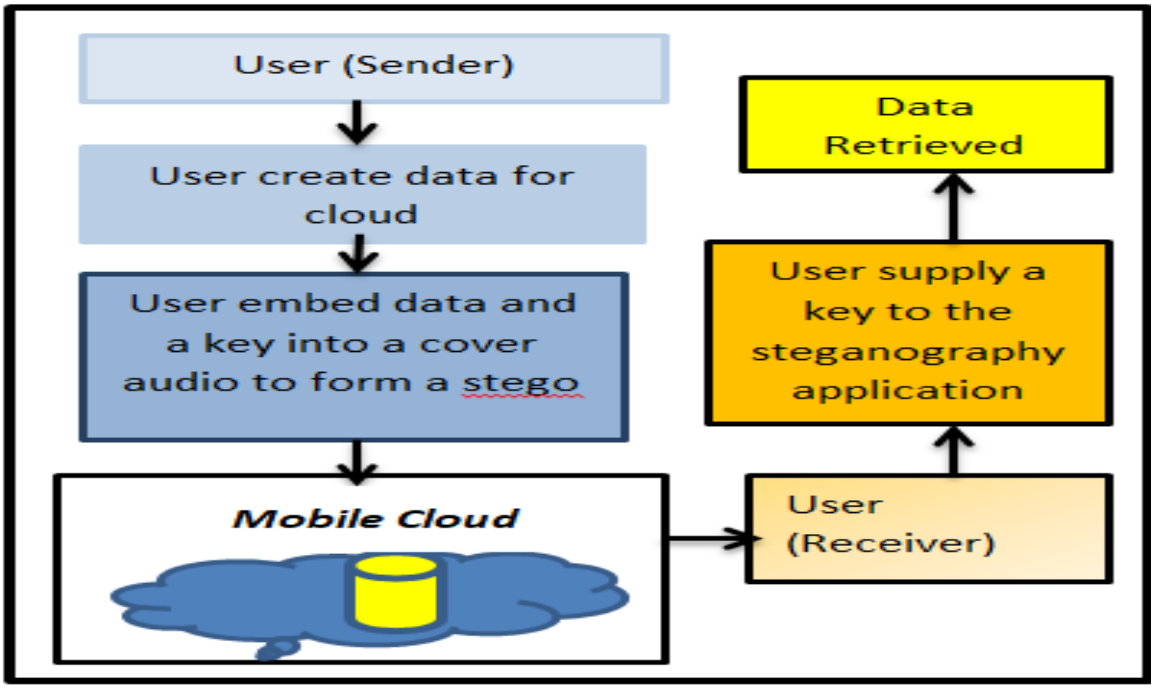

Figure 3.1: The proposed system

3.2 Algorithm for embedding data

The Least Significant Bit (LSB) is the algorithm that is used to embed data into the cover audio

The algorithm below shows how the proposed system works.

1. A key is added to cover audio and the secret data
2. The key, cover audio and secret data is converted to a binary format and the LSB determined.
3. The LSB of the cover audio are replaced with bits from the secret data.

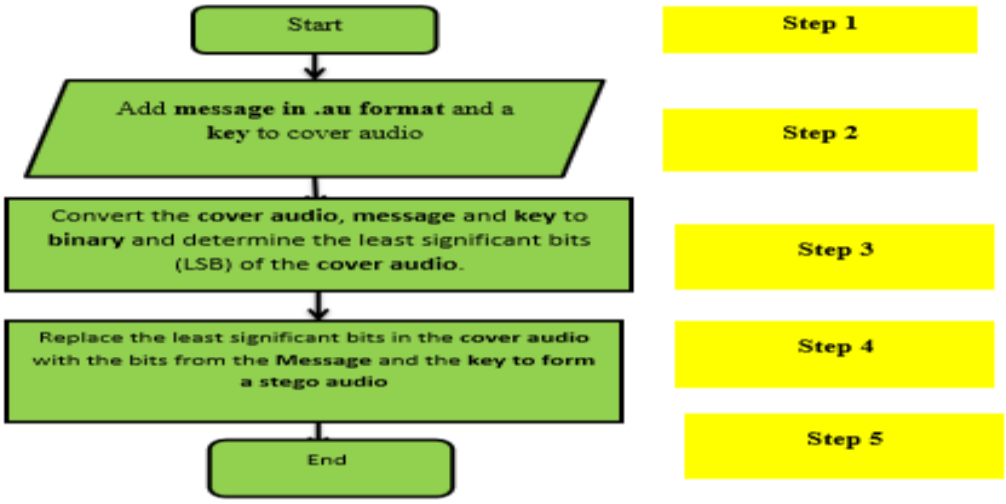

Figure 3.2: Flow chart representing embedding algorithm of LSB

3.3 Algorithm for extracting data

The extraction process is represented in a pseudo code as shown below

1. A cover audio is selected for extracting secret data
2. A key is entered
3. Extraction become successful if the keys matches but unsuccessful if the keys do not match.

The diagrammatic representation of the extraction process is shown below.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

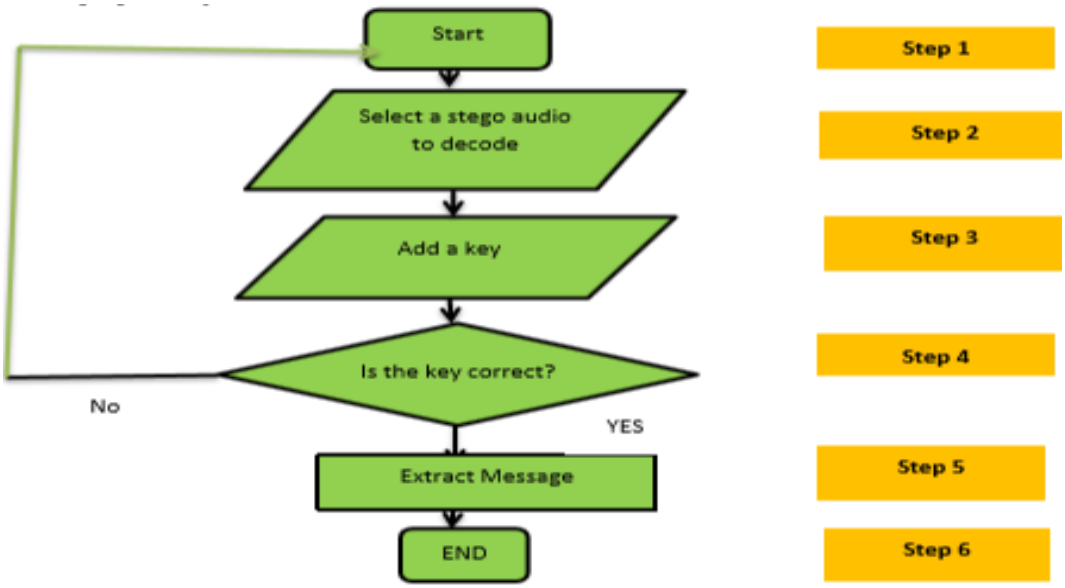

Figure 3.3: Flow chart showing extraction algorithm of LSB

3.4 Research Strategy and procedure

The Experiment Research method is used to implement the proposed system. Normally Experimental Research has the objective of critically evaluating and testing new and existing to provide answers to research questions. The benefits of Experimental Research in Computer Science and Information Technology is that, it lead to improvement of existing systems as well as providing solutions to existing problems in society. Java JDK (Java Development Tool Kit), Netbeans IDE 8.0.2 was used for the development of test suite at the Computer Laboratory.

3.5 Performance Evaluation and Analysis

Figure 3.4: Criteria for Performance Evaluation

Evaluation of any steganography system is based on three main metrics namely Security, Robustness, and Embedding Capacity. The proposed system which is an audio steganography is also evaluated based on these same parameters.

3.5.1 Robustness

When a steganography system is able to withstand manipulation and attack then such system is said to be Robust. The proposed system can be said to be robust provided the sound the sound quality before embedding the secret data into it and after embedding the secret data is the same. A robust steganography system makes it difficult for attackers to change secret data but a less robust system is prone to attacks and manipulations. Two main parameters are always used to demonstrate the robustness of an audio steganography. These two parameters are Peak Signal to Noise Ratio (PSNR) that represents the peak error the unit of measurement of PSNR is decibels (dBs) and Mean Square Error (MSE) that represents the Accumulative Error between the original audio file and the embedded audio file. PSNR is calculated as follows

PSNR = 10.log10 [MAX2/MSE]

= 20.log10 [MAX2/√MSE]

=20.log10 [MAX] -10.log10 [MSE] (Equation 1)

Where MAX is the maximum possible value of the audio signal If the audio is represented using 8bit sample, Max = 28-1 = 255

PSNR = 20.log10 [255] – 10.log10 [MSE]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

MSE is also calculated as follows

$$MSE = \sum_{x\,y} [x\,(M*N) - y\,(M*N)]^2 \quad \text{(Equation 2)}$$

Where x is the original signal, y is the stego signal and M and N represent the row and column of the input signal.

3.5.2 Capacity

Capacity refers to the amount of secret data that is embedded into a cover media (audio) without significantly affecting the quality of it statistically, and that secret data embedded can also be retrieved successfully. Capacity or payload is normally expressed in bits or bytes per signal. However, maximum hiding capacity or payload is expressed in percentage. It is calculated by evaluating the ratio of the amount of secret message to that of the cover audio object.

$$\text{Capacity} = \frac{Number\ of\ bits\ used\ to\ hide\ data}{Total\ number\ of\ bits\ in\ audio\ signal} * 100\% \quad \text{(Equation 3)}$$

3.5.3 Imperceptibility or security

Security of audio Steganography means the ability to prevent detection of the presence of secret data embedded on an audio file. Security of a steganography system also means that an attacker cannot extract embedded secret data even if the attacker is aware of the presence of secret data embedded in it. The algorithm for embedding the secret data on the proposed system ensures that attackers are not able to discover the presence of the secret data. Again, cloud service providers provide end to end encryption service during transit, hence, another layer of security is provided. Java as a programming language used for building the proposed system stores a password which is known as the key in an encrypted format. So only authorized persons will be authenticated and hence provides for imperceptibility

4.0 IMPLEMENTATION OF THE PROPOSED SYSTEM

The proposed system is implemented in java using Java development Kit (JDK. Java Standard Edition is the version of java used for this development. Java as a development tool provides several advantages but the most important one is portability which allows the proposed system to work across all platforms. A part from that, java as an Object Oriented programming (OOP) language allows for re-use of existing code and this feature helped the researcher to rapidly develop the proposed system. Also, Java as an OOP has several library resources that simplify applications development. This study made use of Abstract Windowing Toolkit (AWT) and Swing for the development of the user interface. The Swing preserves the look and feel on each platform. This ensures that the proposed system buttons and icons look the same in window platform, Mac or apple machine.

4.1. Home page of the proposed system

The home page shows the first screen that appears when the user runs the proposed system. It contains the menu bar that consists of two menus, thus, the file menu and the help menu. The file menu also contains three submenus namely: the encoding or embedding, the decoding or extraction and the exit.

Figure 4.1: Home page of the proposed System

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

4.2 Results and Analysis

Every stenographic application is normally evaluated based on the Embedding capacity, Robustness and Imperceptibility. Imperceptibility or security is the inability of intruders to detect and extract message from a stego object. In order to measure the imperceptibility or security of Steganography, two quantitative metrics are used. The first one is Mean Square Error (MSE) which measures the distortion between the original audio and the stego audio. The second metric is Peak Signal to Noise Radio (PSNR) which measures the similarities between the original audio and the stego audio. The properties of the stego audio were generated using MATLABR2017b. The analysis of this experimental study starts by measuring the embedding capacity of the proposed system. Five audio files labeled as Test 1, Test 2, Test 3, Test 4 and Test 5 with specific sizes were embedded with secret messages using the proposed system and their corresponding Embedding capacities recorded as shown in Table 4.1

Table 4.1: Embedding Capacity of the proposed System

Audio file	Audio Size	Message Size	Embedding Capacity
Test 1	66256	12045	18.17%
Test 2	27042	5122	19.90%
Test 3	66942	12590	18.80%
Test 4	58011	10899	18.79%
Test 5	61199	11517	18.81%
Average embedding capacity			**18.89%**

The embedding capacity determines how much data the cover audio will accept without affecting the normal quality of the sound. The results from Table 4.1 show that the proposed system has an average embedding capacity of 18.89% compared with 12.75% of the previous system by Pinardi, Garzia and Cusani (2013) and 18.64% of the previous system by (Bhalshankar , 2015). The results imply that the proposed system is more secure than the previous system because it is difficult to detect the existence of secret information due to the high embedding capacity. Again, the results also imply that more data can be sent by Mobile Cloud Client using the proposed system.

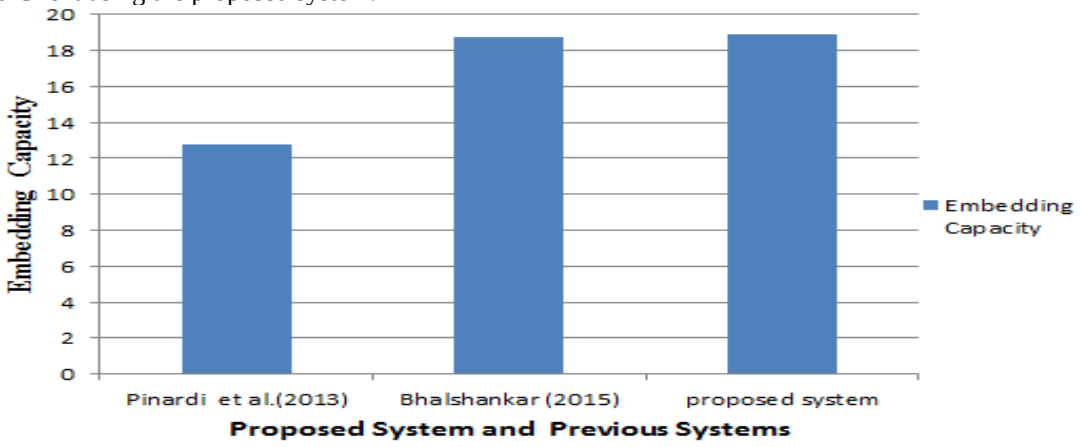

Figure 4.2: Proposed system and previous system vr embedding capacity

Figure 4.2 shows clearly that the proposed system performed better than the previous system in terms of embedding capacity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Table 4.2: MSE and PSNR of previous and proposed work

Audio File Name	MSE and PSNR of previous System		MSE and PSNR of proposed System	
	MSE	PSNR	MSE	PSNR
Test1	0.0019	46.2726	0.0021	50.000
Test2	0.0040	65.9811	0.0040	66.1565
Test3	0.0083	62.7916	0.0084	63.8425
Test4	0.1102	69.0890	0.1112	69.9100
Test5	0.2316	48.6383	0.2254	49.9826
Test6	0.3994	46.2726	0.04038	46.7833

.Table 4.2 represents the results of the Mean Square Errors (MSE) and Peak Signal to noise Ratios (PSNR) of a previous system by Chowdhury et al (2016) and the proposed system. From Table 4.2, the proposed system recorded a better average PSNR of 57.78dB as compared with the previous system of 56.09dB by (Chowdhury et al, 2016). Similarly, Kaur and Singh (2015) recorded PSNR of 52dB. The high PSNR of the proposed system means that the original cover audio and the embedded audio have the same sound quality; hence, it makes it difficult for eavesdroppers to detect the presence of secret messages.
Table 4.3 shows the results of PSNR of the proposed system by maintaining a constant cover audio file size of 187KB and varying the message embedded.

Table 4.3: message size vr varied PSNR

Audio file	Message size(KB)	PSNR
Q1.au 187KB	32.30	69.91
	37.50	67.58
	40.80	66.22
	43.30	65.65
	52.30	63.80
	54.00	61.85

From figure 4.3, the PSNR decreases as the file size increases. This shows that as the file size increases the PSNR decreases and hence, the security of the audio file is compromised. The results also imply that the Mean Square Error (MSE) increases as the file size increases. The increasing MSE and decreasing PSNR have the potential for making it easy for attackers to detect the presence of secret messages in an audio file. However, the superior PSNR and MSE recorded by the proposed system makes it difficult for eavesdroppers and attackers as well as Mobile Cloud Administrators to detect the presence of a message on an audio file.
The outcome of the analyses of the proposed system has led to the realization that when a message is embedded in a cover audio, the properties of the original audio and the stego audio are the same. The bit rate, the number of columns and the data type of the original audio remain the same. These properties are achieved by employing Least Significant Bits (LSB) Insertion Algorithm. The LSB insertion algorithm stores data in existing bits of the cover audio. This simply means that no additional bits are introduced to the cover audio; hence, the size remains the same. These revelations go to prove the fact that the proposed system has been effective and efficient

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

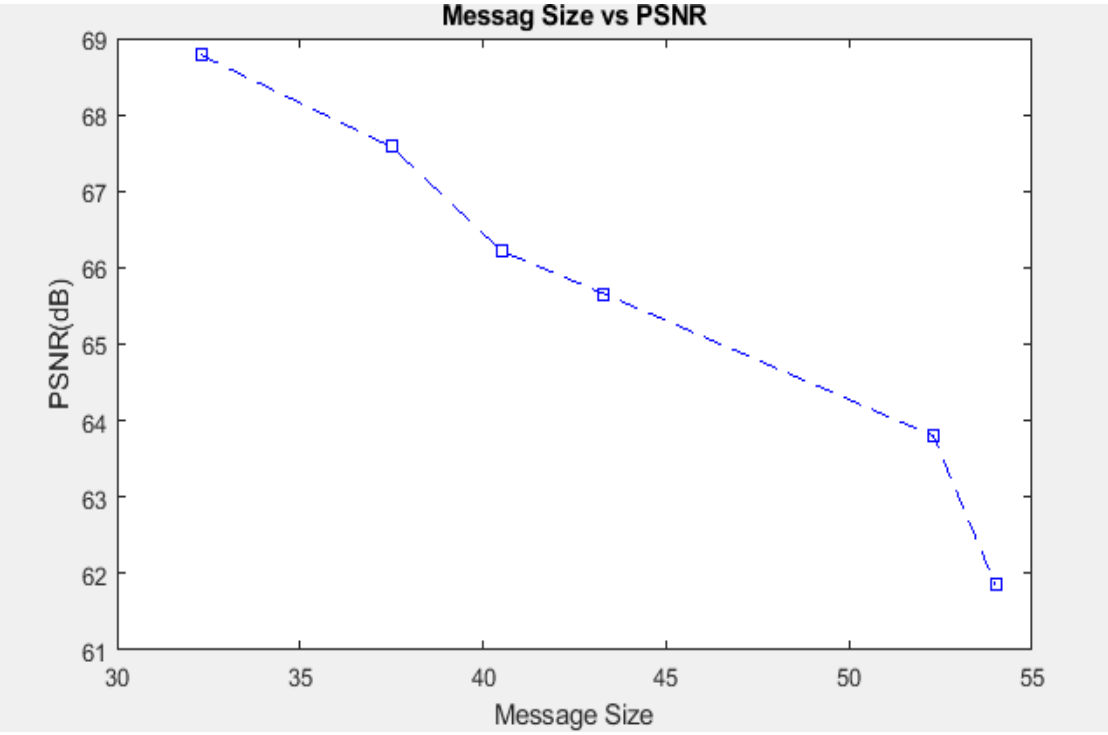

Figure 4.3: Message Size vr PSNR

Table 4.4: Comparison of the original audio file and a stego audio file.

Audio File	Number of Characters in a message	Cover Audio Size	Stego Audio Size
Test1	2104706	1.09MB	1.09MB
Test2	1359360	0.722MB	0.722MB
Test3	713090	0.379MB	0.379MB
Test4	1661185	0.883MB	0.883MB
Test5	1191169	0.633MB	0.633MB
Test6	914689	0.486MB	0.486MB

The table 4.4 shows the resulting sizes of six audio files before embedding a secret message (cover audio size) and after embedding a secret message (Stego Audio Size) on the proposed system.
The results from table 4.4 show that the cover audio has the same size as the embedded audio or stego audio. The cover audio and the stego audio are the same because the Least Significant Bit algorithm only replaces existing LSB bits from the cover audio with bits from the secret message.

4.3 Performance Evaluation of the proposed System

The performance of every Steganography system is evaluated based on three main parameters that are security, capacity and robustness. The proposed system has made some improvement in each of these parameters. Firstly, the proposed system has an average embedding capacity of 18.89 % compared with the previous system average embedding capacity of 18.64% representing an increase in embedding capacity of 0.25%. This increase means that more data can be embedded into a cover audio without reduction in the quality of the audio file. Secondly, security is improved because the Least Significant Bits (LSB) insertion algorithm implemented allows large data size to be embedded without detection of the presence of secret messages on the stego audio when played. The high Peak Signal to Noise Ratio and low Mean Square Error (MSE) of the proposed system make the proposed system very robust. The high average PSNR value of 57.65 makes it difficult to differentiate between a stego

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

audio and the cover audio. This means that the original audio has the same quality as the embedded audio and finally since java is used in the development of the proposed system it makes it platform independent.

5.1 CONCLUSION

The Internet and Cloud Computing has brought serious security challenges to individuals, companies, organizations and Government agencies. Steganography involves hiding data on a cover object such as images, videos, audio and text. This research brings to light how to effectively use Steganography to prevent Mobile Cloud Administrators from getting access to customer data. Mobile Cloud Computing which involves storing, processing and accessing data from a cloud system is made more secure in this study with the use of Steganography. From the results of the study, it can be concluded that Steganography which made use of Least Significant Bit (LSB) insertion has provided security by concealing secret messages from hackers, eavesdroppers and cloud administrators. This security is achieved through the high Peak Signal to Noise Ratio (PSNR) and low Mean Square Error (MSE) obtained in this study.

High PSNR and low MSE imply the quality of the original audio is almost the same as the embedded audio. The average high Embedding Capacity of 18.89% for an audio Steganography in this study also makes it possible for Mobile Cloud users to offload and access more data from a cloud.

REFERENCES

[1] Saini, A., Joshi, K., Sharma, K., Nandal, R. (2017). Of LSB techniques in video Steganography Using PSNR and MSE. *International Journal of Advanced Research in Computer Science, 8*(5). 2405-2410
[2] Bandyopadhay, S., Datta, B. & Ghoshay, N. (2010). New Methods for embedding data with Images. *Journal of Global Research in Computer Science*, 6(3), 1-10
[3] Kumar, A. & pooja, K. (2010) Steganography- Data Hiding Techniques. International Journal of Advanced Computer Applications, 9(7), 19-23
[4] Warkentin, M., & Schmidt, M. B. (2008). *Steganography : Forensic, Security, and Legal Issues*. *January*. https://doi.org/10.15394/jdfsl.2008.1039
[5] Sarma, M., Sunkari, V., Yoseph, A. & Sreenivas, N. (2014). A proposed Solution to Secure MCC Uprising Issue and Challenges in the Domain of Cyber Security Open Journal Of Mobile Computing and Cloud Computing, 10(11), pages: 16-25.
[6] Singh Chhillar, R. (2015). Data Hiding Using Steganography and Cryptography. *International Journal of Computer Science and Mobile Computing, 44*(4), 802–805.http://ijcsmc.com/docs/papers/April2015/V4I4201599a38.pdf
[7] Morkel, J. & Oliver, M. (2005). An Overview of image Steganography. *In Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA).*
[8] Reza, H. & Sonawane, M. (2016). Enhancing Mobile Clou Computing Security Using Steganography *Journal of computer science and Communication, 7(4), 245-259.*
[9] Ibukum, E. & Daramola, O. (2015). A Systematic Literature Review of Mobile Cloud Computing. *International Journal of Multimedia and Ubiquitous Engineering, 10(*12*),* 135-15
[10] Oskar, H. (2012).Mobile Phones and Cloud and Computing (*Master's thesis, University of UMEA)*
[11] Ramalingam, M. (2011). Stego Machine- Video Modified LSB Algorithm. *World Academy of And Technology, 5(2), 170-173 Engineering*
[12] Xu, C Ping, X., Zhang, T. (2006). Steganography in Compressed video stream. In Innovative 13 ComputingInformation and Control. First IEEE International Conference (vol.1, pp.269-272)
[13] Patidar, R. & Patidar K. (2015). Steganography Method Hiding data in video. *International Journal of Computer Science and Information Technology (IJCSIT), 6(1), 237-239.)*
[14] Mathe, R., Atukuri, V. & Devireddy (2012).Securing Information: Cryptography and Steganography. *International Journal of Computer Science and* Information *Technology, 3(3),*
[15] Odeh, A. & Elleithy, K. (2012). Steganography in Arabic Text Using Zero Width and Kashidha Letters. *International Journal of Computer Science & Information Technology (IJCSIT), 4(3), 1 -11.*
[16] Wajgade, V. M., & Kumar, D. S. (2013).Enhancing Data Security Using Video Steganography. *International Journal* of *Emerging Technology and Advanced Engineering, 3(4), 549-552*
[17] Rana, M., Sangwan, B. & Jangir, J. (2012). Art of Hiding: An Introduction to Steganography. *International Journal of Engineering and Computer Science 1(1) 11-22*
[18] Khot, R. & Patil, A.S. (2015). Review Paper on Different Types of Steganography. *International Journal of* Research in Electronics and Computer Engineering (IJRECE), 3(2), 122-124
[19] Amina, D. & Fareeha, A. (2014). Image Steganography for hiding Audio Messages within GrayScale Messages Using LSB, DCT and AES Algorithm *Master's thesis, International Islamic(University of Islamabad).*
[20] Doshi, R., Jain, P. & Gupta, L. (2012). Steganography and It Applications in Security. International Journal of Modern Engineering Research (IJMER), 2(6), 4634-4638
[21] Jayaram P., Ramganatha, H. & Anuapanma (2011). Information Hiding Using Audio Steganography. *International Journal of Multimedia and its Application (IJMA),* 3(3),Pages: 86-96,
[22] Habibi, M., Karimi,R. & Nosralnti, M.(2013) Using SFLA for Text Message Steganography in 24-Bit RGB Color Images. International Journal of 7-14
[23] Amin, M., Ibrahim, S., Salleh, M., Katmin, M. (2003). Information Hiding Using Steganography. *NCTT 2003 Proceedings 4th conference on Telecommunication Technology,* pp: 21-25
[24] Kamred, U. (2014). A survey on Audio Steganography Approaches. *International Journal of Computer Science Applications*, 95(14)
[25] Deshpande N., Fusate R., Malviya, P. & Dhyavartiwar, S. (2015). Implementation of AudioSteganography Using RSA Algorithm. *International Journal of Technology Enhancement and Emerging Engineering Research, 3*(4), 81-84
[26] Juneja,M. & Sandhu, P. (2009). Designing of Robust Image Steganography Techniques Based On LSB insertion and Encryption. *Proceedings of* International *Conference on Advanced in Recent Technologies in Communication and Computing, 302-305*
[27] Pinardi, R., Garzia, F. & Cusani, R (2013). Peak- Shaped–Based Technique for MP3 Audio.*Journal of Information Security 4(1).12-18.*
[28] Bhalshankar, S. (2015). Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes. International Journal of Advanced Computer Research, 5(20), 233-248 29Chowdhury, R.,Debnath, B., Bandyopadhyay, S. & Kim,T. (2016).
[29] A view on LSB base audioSteganography. *International Journal of Security and applications 10(*2) 51- 62.
[30] Kaur, R. & Singh, T. (2015). Hiding Data in Video Using LSB with Elliptic Curve.Cryptography International *Journal of Computer Applications, 117(18). 36-40*