XOR AND IP FILTER BASED STEGANOGRAPHY FOR SECURE DATA TRANSMISSION IN CLOUD ENVIRONMENT

Chandni[1] and Vikram Singh[2]

[1] M. Tech. CSE Scholar, Ch. Devi Lal University, Sirsa.
[1] Professor of Computer Science, Ch. Devi Lal University, Sirsa.

Abstract: Steganography is the technique of hiding information along with ordinary information at the source end. Steganography can be defined as an art. In the Stenography technique, the data, figures, etc. has been secured inside in the form of other data, figure, or files. The proposed work, XOR-based security has been merged with proposed model. It has been done to work in order to prevent brute force as well as to the timing attack. The IP filter programming is made by connecting java with the database. This database would store the authentic IP addresses. The user-defined port is to enhance security. The predefined protocol has been used in the proposed work. The ports from 0 to 1023 are reserved by existing protocols. The chances of timing attack in case of proposed XOR and steganography will be less than the traditional RSA technique. Threats of different attack are negligible with the use of proposed XOR and steganography. The proposed technique would be applicable to limit the unauthorized execution with the use of an IP filter. In the future, it will be beneficial to secure data transmission.

Key terms**:** Steganography, XOR encryption, decryption, IP filters, RSA.

1. INTRODUCTION

Visual cryptography has been known as a cryptographic technique. This technique enables the user to convert the visual data such as figures, text, etc. into visual image. Using this technique, data has been encrypted and decrypted data looks like a visual image. Visual cryptography has been introduced in 1994 by Moni Naor and Adi Shamir. This technique is best and well known techniques. Visual cryptography having the same theory has been used on graphical content. It can be said that the Visual cryptography may be anything. (Liu, 2011).

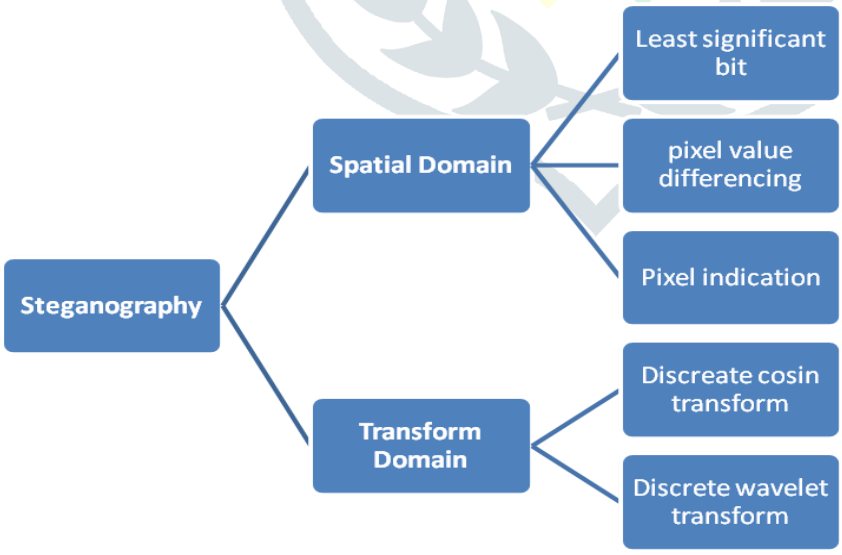

Figure 1. Steganography technique

Steganography's working process has been presented in this introduction part**.** In the present time, it has been analyzed that the steganography performs along with an enhancement in secret bits in files. It is not easy to break it in order to make it extra attractive. It is effective technique to send the very important personal parallel to business data. Here the social channels have been used.

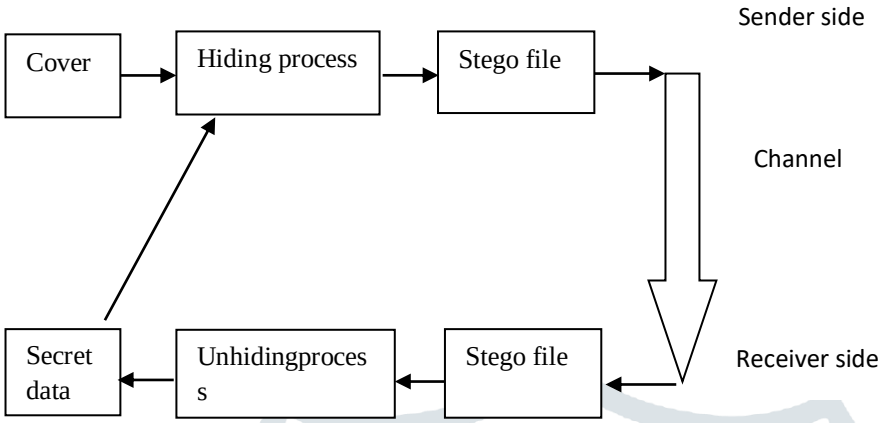

Figure 2. Working of Steganography

In the file header, the hidden message or data could be developed. This file header basically involves the data for example file type, resolution and graphics' with JPG graphics, color deepness. It has been evaluated that the Steganography is the initial technique used to secure the data. In the past time, it was used as a transformer of transmission. It has been assumed that the initial Greek used to cut the head hair of the message supplier. After that they locate the content of message on the head of messenger. After that, during the time taken by the messenger, his hair grew up. In this way the content situated on his hair becomes safe. After the progress of his hair, he passed the area of opponent without assuming. Not one can assume that precious data is located on the head of message. When the messenger reached near of data receiver, his head had been bald and got the message. (Liu, 2011).

1.1 XOR and IP Filtering

An XOR gate has been referred extended name that is the exclusive OR gate. It can be defined as a digital logic gate with two or more inputs and one output. These input and output perform exclusive disjunction. When exactly one of the inputs of the XOR gate is true, the output of an XOR gate will be true. IP filters are the rules define to the remove or allow to the packets (Velmurugan, 2018).

1.2 Steganography

Steganography is a technique used to hide the information and can be referred as an art.. In this technique, the data, figure, etc. are secured in different information, figure, or files. It has been done to secure the data. For this purpose, steganography has been used. This technique is able to hide the secret message using a cover-media. For this, a particular method has been followed. Using this technique, one cannot make expectation about the existence of secrete data. Simple in simple words, the steganography can be defined as a mean used to hide the data in another data for security. In Modern steganography, the opportunity has been used to secure the data into digital multimedia files. It has been done on network packet level also.
Using steganography, one can transfer the data securely and receiver gets the protected information without any treats. The sender and receiver have the knowledge about the actual data and they can make transmission securely. The data on which this technique has been applied looks like the normal objective (Liu, 2011).

1.3 Cloud Security

Cloud computing security stands for a set of policies, techniques, applications, and controls. These all have been used to secure the virtualized IP, data, applications, services, and the associated system related to cloud computing. It can be define as a sub-domain of computer security. It is also the sub part of network security

as well as of data security also. Cloud security system is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. Security management addresses these issues with security controls (Amalarethinam, 2017).

2. LITERATURE REVIEW

Liu (2011) investigated the thwarting audio steganography attacks which are made on cloud storage systems. The results of the research work has shown that the proposed work is capable to defeat the audio steganography Attacks which are made on cloud storage architecture.

Wojciech (2011) discussed the cloud computing steganography-proof. The research work has focused on data security feasibilities classification in Cloud environment. Particularly, the researcher provide the introduction of a classification of steganographic communication scenarios in cloud computing. The proposed work is dependent on the steganograms receiver location. Such scenarios with the threats that are possible to develop in steganographic technique. It can be received in account at the time of making design of services of secure cloud computing.

Murakami (2013) discussed updated security in cloud environment. In the proposed work, they used the steganography (855 Kb). Recently, several cloud computing architecture are provided over the world.

Nimmy (2014) proposed the novel mutual authentication protocol. This protocol has been used in cloud computing. For this purpose, they used the secret sharing as well as the steganography. It has been analyzed that the proposed protocol offers the mutual authentication in users and cloud server. Also, the users are achieved the flexibility for changing the password. Therefore, the efficient security characteristics provide the protocol well suited. It has been used cloud system.

Mandai (2015) make the consideration of the hiding data sharing. It has been done in cloud system. For this objective, steganography as well as the encryption with GA has been used. steganography with an innovative cryptography has been utilized. The steganographic method has embedded secret data with the use of pixel mapping method. It has been determined that it has been done in a chaotic sequence. This sequence has been created by technique of chaotic map.

Prakash (2015) proposed three-step data security model. The proposed model performs in cloud computing environment. The proposed model is dependent on RSA as well as on steganography. This research work has described a pattern to secure data and information in a cloud system. It is necessary to secure the data during data sharing and storing of data. For this in proposed work, they have used a pattern in which cryptography with steganography method has been involved.

Bansal (2016) discussed the low error rate related secure sharing. This considered sharing is of personal health record within cloud environment. For this, DWT steganography has been used. In the research work, the researcher has focused on enhancement of security related to the PHR. It has been by the implementation of DWT related to the Steganography. It has been analyzed that the Steganography can be defining as a process used to secure the information in the form of the graphical content. Steganography involves to the insert the huge size data in the graph form.

Maitri (2016) provide the discussion of protected file storage within cloud computing. For this hybrid cryptography algorithm has been used. Cryptography and steganography has been known as well populated technique used to secure the data. The research has attempted to highlight the challenge faced during the formulation of a model to secure the data using image steganography. The proposed technique is an updated LSB image steganographic method. Here the password has been utilized to secure the data in an image.

Abduljabbar (2016) researched on robust scheme. This proposed scheme is applicable to secure the authentication code related to the message over cloud environment. Several content authentications with integrity system is conducted. It has been done to categorize any updating in the replacement related to the documents. It has been made by two entities suppliar of data and receiver of data in a cloud system.

Mittal (2016) provide the research on data security. For this, they discussed the RSA encryption technique along with image steganography. In the research work, RSA algorithm has been used to encrypt the data. Here image steganography has been applied to data hide with the use of LSB technique.

Ranjan (2016) offered the research work on advanced techniques. This discussed technique has been used to share and secure the data on cloud. For this, multilayer steganography with cryptography has been used. The aim considered in the proposed work is to prevent the data access by unauthorized users.

Amalarethinam (2017) provide the research work on data security increment in public cloud storage. For this, data obfuscation as well as the steganography has been used. Security of Data storage can be

defined as issue faced during cloud storage. The results have proved that defined technique is more capacity with best quality of stego images.

3. ANXOR AND IP FILTER BASEDSTEGANOGRAPHYTECHNIQUE

Steganography has been considered as a procedure which is used to hide the sensitive information in organizations every one communication with each other and secure the data. Steganography can be defined as a technology used to secure data and provide the communications securely. Scopes with use of the internet are growing day by day in the commercial field as well as in the educational sector. Internet is providing a platform for eCommerce and activities related to social. Flipkart, Homeshop18, E-Bay have been provided and discussed as the E Commerce related sites. Facebook and twitter can be discussed as the social network sites. Structure of steganography with its security challenges are discussed here. The traditional Steganography security technique has been reviewed in order to classify the loopholes of traditional security methods. To enhance the security of steganography technique the integration model of IP filter and Steganography would be developed. The encoding and decoding technique design would be more secure as compared to traditional design.

To enhance the steganography security IP filter is used. It has been integrated in order to do the rejection of unauthenticated dealing with packets from the server to client.

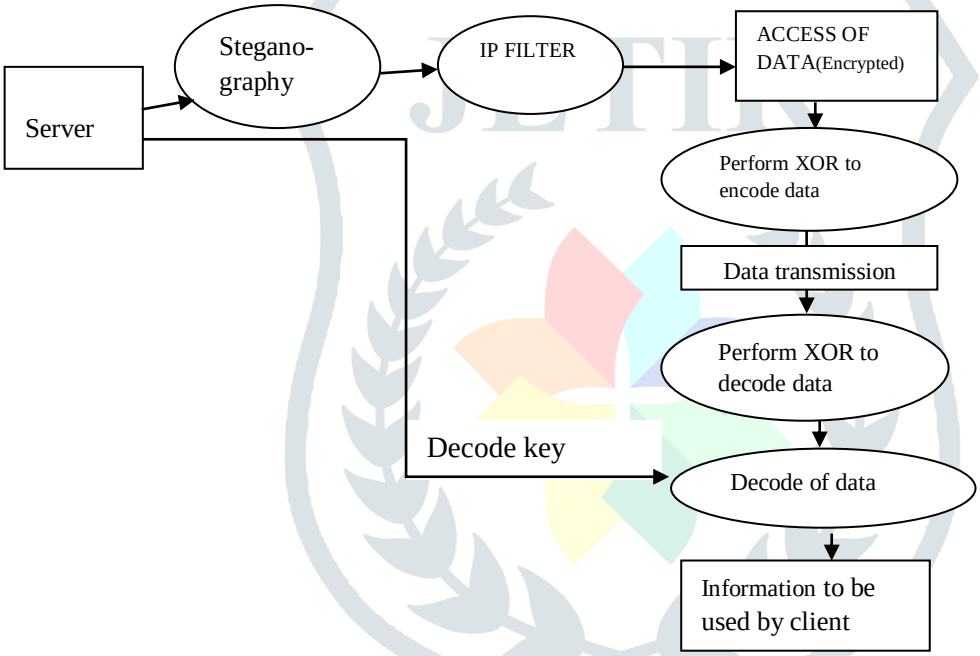

Figure 3. Proposed model

Here network security is enhanced to customize the traditional Steganography technique with the use of XOR operation. Motive of the research is to study the limitation of traditional protection technique andpropose an enhanced protection mechanism using steganography. The investigator shall write her own socket server and corresponding client. It has been done to avoid illegal interference at the time of data dealing. Further, the user interface would be created in order to create the client-server transmission.

3.1 XOR Encryption Process

Encryption: The encryption procedure applying XOR has been outlined:

1:- Have data named D for encryption
2:- Use X that is XOR key for encoding of data
3:- Determine the counter count is equal to one
4:- C is equal to D XOR X
5:- If count greater than nine, after that follow step 8 otherwise
6:- Achieve the cipher data with the use of C=C XOR X
7:- Determine count equal to count+1 perform step 8
8:- Achieve C as cipher text after that makes transmission on network

The input value is equal to 8. XOR is equal to 4
Assume for XOR encryption, the input value is equal to 8
Execute 8 XOR 4
1000 XOR 0100 is equal to1100
Now, the encrypted data is 1100 which is equal to 12

3.2 XOR Decryption Process

Decryption: The decryption procedure applying XOR is:

1:- Take the data C to decrypt
2:- Have XOR key X for decoding of data
3:- Determine counter count is equal to 1
4:- D equal to C XOR X
5:- IF count is greater than 9. After that, perform step 8 in the opposite condition
6:- Achieve the cipher data with the use of D=D XOR X
7:- Determine count=count+1 perform step 5
8:- Achieve D as normal text.

Input for XOR decryption
For XOR decryption, Input is **1100**
1100 is again performed XOR along with 100
1100 XOR 0100 equal to 1000 (8)

8 is the output for XOR decryption

4. SIMULATION EXPERIMENT

In the simulation, the data has been encrypted using RSA based implementation in traditional work. The traditional mechanism of encryption was RSA that has been made. In order to reduce the limitation of the traditional RSA model, the XOR-based security system has been proposed. In order to implement This XOR-based system, the file sender and receiver modules have been built in net beans environment. The sender would send the content and receiver would receive the contents. The function XOR written in java would encrypt the contents more quickly as compared to the traditional RSA algorithm. In this section, the transmission in sender and receiver has been simulated using server and client program. The transmission has been made using socket programming in java.

4.1 Process followed to execute the application

1: To execute the server-side application, the compilation of code has been made with the use of
```
javac MyServer.java
```
2: After that one execute the server-side application with the use of below given command
```
javaMyServer
```
3: To execute the client-side application one make compilation of the client code initial
```
javac MyClient.java
```
4: To execute application make typing of below given command
```
javaMyClient
```

5. RESULTS AND DISCUSSION

The results have shown the difference between the time taken in case of traditional RSA based security system and proposed XOR-based system.

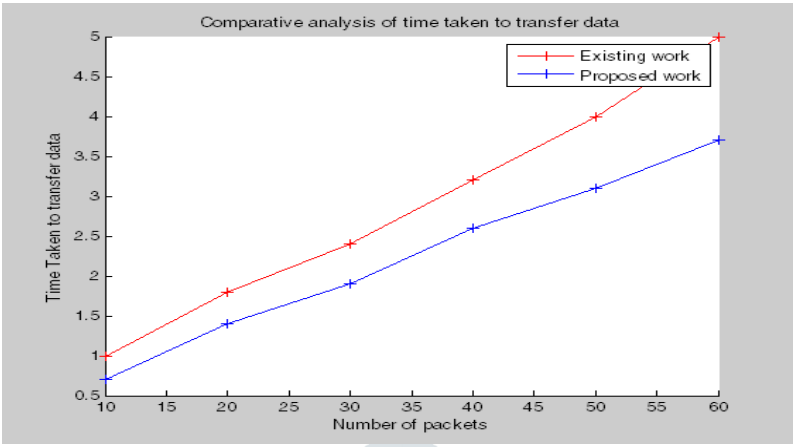

Figure 4. Time was taken during transmission

Figure 5 below shows the comparison of error rates in RSA and XOR-based security systems.

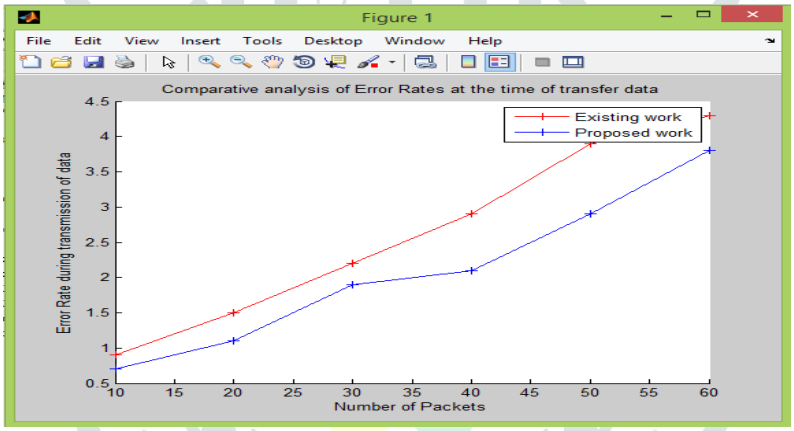

Figure 5. Error rates during data transmission

In proposed work, due to the reduction in the size of data the packet size get reduced. Figure 6 shows the comparison of packet size in RSA andXOR-based works.

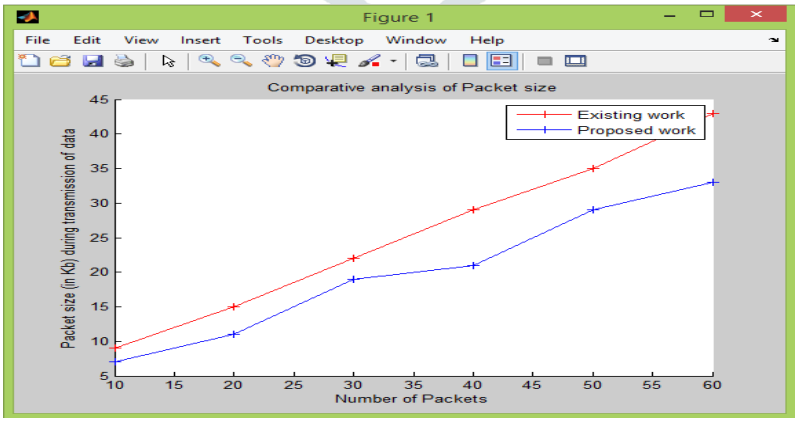

Figure 6. Packet size

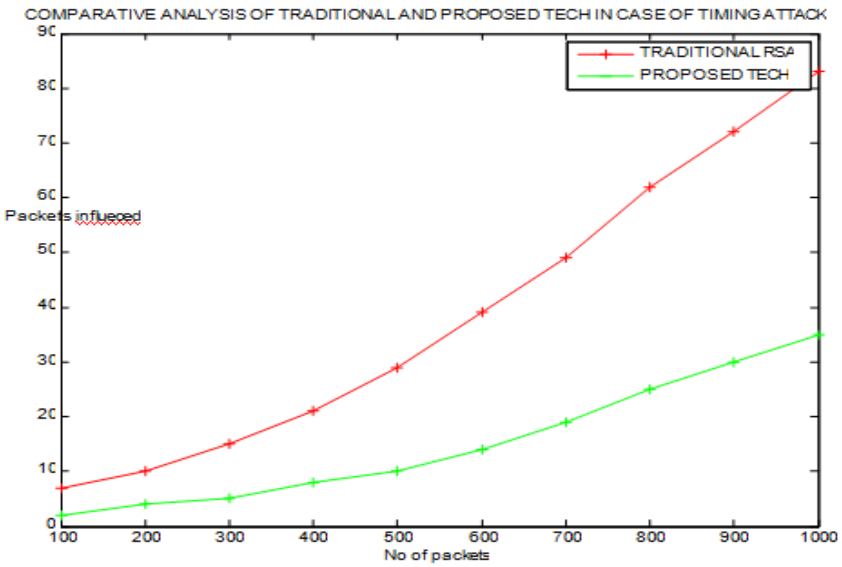

Figure 7. RSA and XOR based techniques(brute force attack)

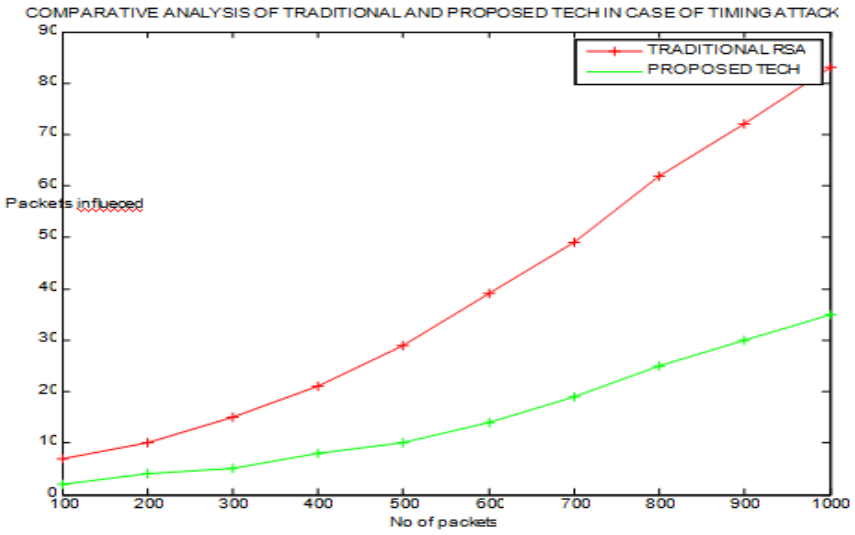

Figure 8. RSA and XOR techniques (timing attack)

6. CONCLUSION

Finally, it is clear that proposed work is more capable than the existing RSA work. The proposed model is very efficient and reliable to defeat the brute force attack and timing attack. It has been proved that XOR-based security system is required to improve the efficiency of encryption and decryption. The Design including the proposed steganography technique, IP filter with the visual steganography is used in order to increase the security of data. After observing the research evaluation, it can be said that the chances of different attacks is less using proposed XOR and visual Steganography. According to the increment in number of packet, there is the enhancement in the chances of timing attack. Using the proposed technique, the probability of unauthentic data access applying timing attack is less as compare to existing technique. In addition, IP verification has been used as security technique to restrict the hackers.

Real Image has been loaded to encrypt it. Then the key image has been loaded in order to execute the XOR operation. The threat of different attack will be negligible with the use of proposed XOR and Steganography. The research model would be applicable to limit the unauthorized execution with the use of an IP filter. In future, it will be beneficial to secure the data transmission

REFERENCES

Liu, B. et al., "Thwarting Audio Steganography Attacks in Cloud Storage Systems," pp. 259–265, 2011.

Murakami, K., Hanyu, R., Zhao, Q. and Kaneda, Y., "Improvement of Security in Cloud Systems Based on Steganography," pp. 503–508, 2013.

Nimmy, K., "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography," pp. 101–106, 2014.

Mandai, S., "Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA," pp. 1469–1474, 2015.

Prakash, J. and Cse,M.T., "Three-Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques," pp. 490–494. 2015.

Bansal, P., Sharma, B.and Saxena, M., "Low Error Rate Based Secure Sharing of Personal Health Record in Cloud Computing using DWT Steganography," 2016.

Maitri, P. V., "Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm," pp. 1635–1638, 2016.

Abduljabbar, Z.A., "Robust scheme to protect the authentication code of message/image documents in cloud computing" 2016.

Mittal,S., Arora, S. and Jain, R., "Data Security using RSA Encryption Combined with Image Steganography," 2016.

Ranjan, A., "Advanced techniques to shared & protect cloud data using Multilayer Steganography and Cryptography," pp. 35–41, 2016.

Amalarethinam, D.I.G., "Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography," 2016.

Pradesh, U., Singh, R., Pradesh, U.and Pradesh, U.,"Enhancement of Steganography Using K Strange Point Clustering" 2017.

El-latif, A.A.A., Abd-el-atty, B., Hossain, M.S., Elmougy, S. and Ghoniem, A., "Secure quantum steganography protocol for fog cloud Internet of Things," vol. 3536, no. c, pp. 1–8, 2018.

Singla, S. and Bala, A., "A Review: Cryptography and Steganography Algorithm for Cloud Computing," 2018 Second Int. Conf. Inven. Commun. Comput. Technol., no. Icicct, pp. 953–957, 2018.

Ahmad, Z., "Optimized Data Hiding in Complemented or Non- Complemented Form in Video Steganography," 2018 Cyber Resil. Conf., pp. 1–4, 2018.

Alkhamese, A.Y. and Hanafy, I.M., "Steganography: A Review," 2019 Int. Conf. Innov. Trends Comput. Eng., no. February, pp. 549–558, 2019.

Velmurugan, N. and Winster, G., "Implementation of Enhanced AES for Secure and Efficient Data Storage in Cloud Environment", Volume 119, No. 16, pp. 3511-3517, 2018.