https://doi.org/10.48047/AFJBS.6.Si4.2024.2636-2645

African Journal of Biological Sciences

Comparative Analysis Of Steganographic Methods Versus Cryptographic Techniques In Information Security

Ms Vani Dave[1*], MsAnshika Shukla[2],Sakkaravarthi S[3], Kumaresan K[4], Dr. Kesavamoorthy R.[5], Thiruselvan P[6]

[1*]PSIT College of Higher Education, India –vani_dave@rediffmail.com
[2]Department of Artificial Intelligence and Machine Learning, CMR Institute of Technology, Bengaluru, India – anshikashukla4@gmail.com
[3]Assistant Professor, Department of IT, Ramco Institute of Technology, Rajapalayam, India – sakkaravarthi@ritrjpm.ac.in
[4]Chief Technical Officer, Marat Solutions, Coimbatore, India – kumaresh2020@gmail.com
[5]Department of Computer Science and Engineering, CMR Institute of Technology, Bengaluru, India – kesavamoorthycse@gmail.com
[6]Assistant Professor, Department of CSE, P.S.R. Engineering College, Sivakasi, India – thiruselvan@psr.edu.in

***Corresponding Author:** Ms Vani Dave
[*]PSIT College of Higher Education vani_dave@rediffmail.com

Article History
Volume 6, Issue Si4, 2024
Received: 20 May 2024
Accepted: 25 June 2024
Doi:
10.48047/AFJBS.6.Si4.2024.2636-2645

Abstract
Unauthorized access to an individual's data is becoming an increasing problem over the internet which leads to the development of insecure communication of important information between the parties in the field of information technology. System vulnerabilities or security breaches, such as system mis configuration, user misuse, or programme faults, can lead to undesired manipulations over a poorly secured network. Hence, in order to secure data from unauthorized means, steganography and cryptography are two most prominent techniques that have been used as an attempt to eliminate the threats and secure data. Steganography is related to hiding a message whereas the latter is responsible for encrypting the contents of the message shared between two parties. Both the aforementioned techniques have been proved to be efficient and resilient. This paper comprehensively mentions the techniques in detail along with its major applications. Furthermore, it also discusses in detail the major differences between the two techniques. Finally, keeping in mind the security of the data, attempts have been made to examine various methods for using the steganographic and cryptographic techniques in tandem to create a hybrid system called as Crypto- Steganography systems as there has been vigilance among individuals, groups, agencies, and government institution regarding the combined techniques that can be used to replace the conventional securitytechniques.

Keywords: Steganography, information security, encryption, data security, Cryptography, decryption

Introduction

The rapid emergence of the internet has definitely connected the world effortlessly but this has brought up a huge challenge of security of information and data being shared over the internet.

Sharing information and confidential data over an unsecure means that can be through emails or using the web browser are not at all safe mode of transmission due to the high probability of being intruded [1]. There has also been a significant increase in the active number of intruders over these years with the exposure to the internet [2]. To exemplify, during an online payment the entered details of the credit card information can be easily impeded and eventually be used by the intruders. Hence, the security of data has been a vital concern with the growth of numerous technologies and also as the exchange of information is significantly increasing on a regular basis[3].

There are mainly two types of attacks which can occur during the exchange of information and they are active attacks and passive attacks. If the data and information being shared between two communicating parties is modified then the attack is termed as an active attack. This attack hampers the integrity of the information being shared over a network. Conversely, the passive attack does not involve any kind of modification to the data being transmitted [4]. Thus, it can be easily deduced that the major reason behind the possibility of attackers being able to intrude the information being shared between two communicating parties is that the impeders are able to decode the information and then misuse or misinterpret it or maybe use it to plan a bigger scale attack[5].

Nevertheless, the challenges posed by the increasing communication over the internet pushed the researchers to perform studies that can be used to manage efficiently the security issues with the help of advanced technologies. Thus, the two important techniques which have the capability to point the potential attacks are Cryptography and Steganography which must be used in order to protect the useful data [1,3,6].

Cryptography has been accepted widely due to its capacity to ensure communication confidentiality by encrypting the message. Cryptography encrypt or encode the information by altering its meaning and modifying its appearance. This technique simply ciphers the information using mathematical techniques and algorithms such as private key or symmetric, public key cryptography and asymmetric algorithm to protect highly sensitive information [7]. However, encrypting only the message is not enough and there persists numerous possibilities of attack and the information can be easily decoded. Hence, the knowledge of the information should also be restricted and the art of doing so is termed as Steganography. This technique protects the secret information in inconspicuous cover in order to prevent it from the unauthorized access. In some instances, sending encrypted information may draw attention, whereas invisible information may not. Thus, considering the limitations of each technique, the best approach to prevent the data and information from unauthorized access is to develop a hybrid system called Crypto-Steganography systems which can be advantageous in comparison to utilizing a single technique for data prevention[8,9,23].

In this manuscript, the details about Cryptography and Steganography techniques, its advantages and limitations have been discussed in detail. The research also presents in detail the major differences in terms of objective, definition, key, output obtained and method employed between the two techniques. Additionally, an overarching review of utilizing these techniques together as mentioned above in the form of hybrid systems and its advantages have also been presented. Finally, a few noteworthy conclusions have been presented by the author.

Background

The information systems are currently essential for the survival of all the individuals or organizations. Considering a wider aspect, as the organization's dependency on its information

system grows, proportionally the probability of the intruders as well as competitor organisations to have access to other organisations' information systems increases tremendously [10]. Hence, in today's world, with increasing threat to the sharing of data, the two distinct techniques as mentioned before that help in maintaining the integrity of the data between two communicating parties are steganography and cryptography. The two techniques differ from each other significantly in terms of the methodologies used to secure the data and information being shared. The major agenda behind the usage of the former technique is that it helps in hiding the information by making its existence unknown [11]. On the other hand, the latter is responsible for providing protection by modifying the meaning of the information. The steganography technique utilizes mostly images to camouflage the information and communicate securely while cryptography is actually a mathematical study which obscures the integrity of data by utilizing multiple algorithms. If the key or the encoding system is cracked or known by the intruders, it becomes very easy to misinterpret the information whereas cryptography completely alters the definition and meaning of the information which is known only by the sender and receiver. Nevertheless, a detailed investigation regarding the usage of these techniques and their amalgamation is required [1,3].

There is also a classification which has to be taken into consideration while considering the various methods of steganography and Cryptography. The numerous methods available for providing security of the data employ the cryptographic techniques that is encryption before the steganographic methods and the termed coined for such method is called a Class-A. In contrary, if the steganographic methods are executed before cryptographic methods then it is termed as Class-B. The flowcharts of the Class-A and Class- B methods are shown in Figure 1 and Figure 2 respectively[3].

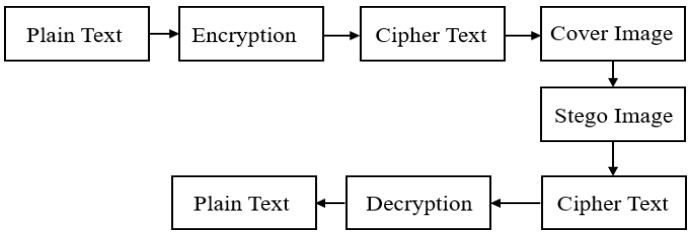

Figure 1 Flowchart of Class A. Adapted from Almuhammadi et al., (2017) [3]

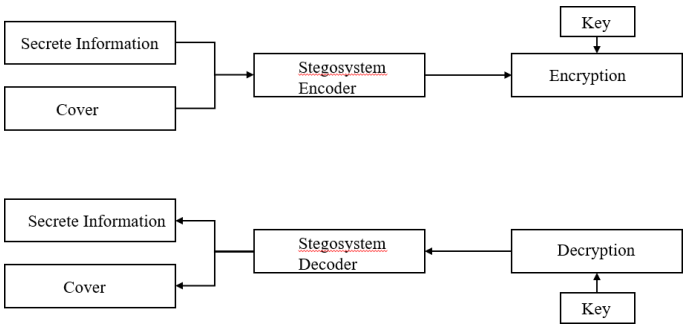

Figure 2 Flowchart of Class B. Adapted from Almuhammadi et al., (2017) [3]

Steganography

The technique of concealing the information into a cover message in a particular way that the intruders remain unaware about its existence is called Steganography. It is one of the techniques of information security which is responsible for the hiding the information which provides aids in preventing any kind of modification, disruption and disclosure of the highly sensitive information. The message can be converted into a normal text, image and amongst others, that can be

represented as a bit. If an intruder figures out the existence of the cover in which the information is being shared, it almost impossible for him to know the hidden data present under the cover [1,7]. This technique helps in protecting the information in a cover as mentioned earlier and is called a stego-object and in order to hamper the piece of information, sometimes, a key or pass code is required (Stego-key) to decode it and has to be known beforehand. In this technique, the stego-system encoder follows a specific algorithm to inject the secret information into the cover media. Generally, anything that can be represented as a bit string, including plaintext, images, and cipher text, can be used as a secret message. By selecting an appropriate channel, the stego objectdetails can be transferred to a receiver, where the secret data is extracted using a decoder system and the same stego technique. The security can be further improved by using the Kerckhoff principle. Employing this technique, even if an intruder understands the design and implementation of the steganographic system, he must have the secret key to launch a successful attack on it. Hence, the stego-object contains concealed data that can only be accessed by the intended recipient who understands the decoding technique [8].

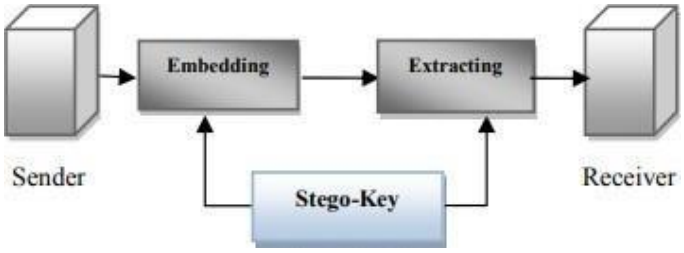

Figure 3: Steganography. Adapted from Sainiet al., (2013) [8]

The different types of steganography presented by Kumar et al. (2014) are text steganography, image steganography, audio steganography and video steganography. The method of hiding the data inside a text can be termed as text stego. The positive aspect for this type of steganography is that requires low memory space that facilitates fast transfer between the two parties. Image steganography is the technique in which the information is secured using the pixels. Least Significant Bit (LSB) is the most widely adopted image steganography method. In the similar manner, if audio media or video frames are utilized for securing the information then it's termed as audio steganography or video steganography [3,8]. Furthermore, Petitcolas et al., (1999) commented that watermarking and fingerprinting are also techniques which are related to steganography. There is a significant difference between these techniques as suggested by the authors owing to the fact that they majorly ensureprivacyofintellectualpropertywhichimpactsthe levelofsecurity[12].

The research conducted by Conklins et al., (2009) presented that the use of Steganography with other methods is most advantageous in order to provide layered levels of security to information. The methodology behind this is that the intruder cannot access the encrypted information by decoding one layer only. The intruder has to decode all the layers to successfully be able to use the information for his benefit [13]. Moreover, the very crucial information relating to the governments, banking information and military can really be protected in the aforementioned security mechanism. But there are a few major limitations offered by this technique despite of its extensive use and robust nature. The techniques can also be used by various terrorist groups and they can also communicate information between themselves secretly which is difficult to decode by the law enforcement agencies [1].

Cryptography

Cryptography is an alternative that provides aids in hiding and encrypting the confidential information that is being shared between the two parties. It involves the process of secret writing by encoding the message at the sender's end and then decoding at the receiver's end [8]. In other words, there exists an encryption framework which include a typical algorithm responsible for altering of the message being communicated into indecipherable configurations for the unauthorised people and also a decryption framework which are used for the decoding process by the person who has possess the rights [1,3]. Numerous sectors which including non-repudiation, sensitive information exchange, and authentication, have a huge dependence on cryptography. The primary purpose of encryption in cryptography is to prevent unauthorised changes to sensitive data. In order to guarantee a complete secure transmission, it entails the encryption of both the information and the stored data. Because an encrypted communication cannot potentially be deciphered by an authorised person, even if an eavesdropper is successful in intercepting it, the attacker will be not be able to do anything [14,15].

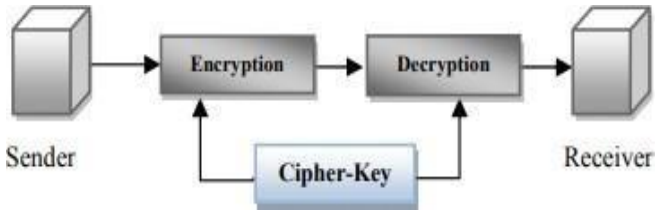

Figure 4: Cryptography. Adapted from Saini et al., (2013) [8]

The three types of methods that can be used in order to encode the data and information using cryptography are "public-key cryptography", "secret key cryptography", and "hash functions". The encryption algorithms decide the type and key of the aforementioned methods of cryptography [1,3]. If the exchange of information within the two parties occurs with the help of the same key for encryption and decryption then the technique is termed as symmetric-key encryption. AES and DES algorithms are the typical examples of symmetric- key encryption. On the contrary, for enhanced security, if the keys are different for encryption and decryption, then the technique is known as Asymmetric-Key Cryptography. RSA is a typical example of Asymmetric-Key Cryptography (AES). Finally, the functions which use no keys are called as the hash functions. Infact, for each object in the data a unique has value is assigned. Typically, hash functions are employed in order to create digital fingerprints of data, ensuring their integrity. However, there are limitations linked to the techniques mentioned above. Symmetric-key encryption (SEA) lacks in terms of distribution of keys. The information can be accessed if the key is stolen as both the sender and receiver uses the same key leading to the compromise of security and adding a dimension of un safety to this method [1,16]. The research conducted by Gisin et al., (2002), have reported that the problem of SEA can be solved by using different keys in AES but it involves mathematical functions which the researchers have still being facing issues to obtain results after solving it [17]. In a nutshell, the issues with the cryptography techniques are associated with key sharing problems, cryptanalysis, government restrictions, mathematical flaws with asymmetric encryption and amongothers.

Steganography vs Cryptography

The transfer of data and information across an unsecured network can be accomplished by using cryptography and steganography to protect the data from unauthorisedaccess. A comparative study was important to be performed as it helped in developing understanding about the technique implementation in various applications.

The difference in terms of definition of the techniques is that the cryptography encrypts the data, but steganography embeds it in an image to secure it. The main objective behind the steganography technique is that it aids in secret communication whereas cryptography is mainly responsible for data protection by maintaining the details of the message confidential. The difference in terms of the key used for encryption is that it is not a mandatory thing for steganography methods whereas most of the algorithms of the cryptography have a secret key to be used for encoding and decoding the message. In contrast to cryptography, which encrypts data before sending it over a network, steganography has the benefit of not raising any suspicions in the eyes of the attacker that the file hasn't been altered or that any data may be concealed. Moreover, the former alters the completer structure of the piece of information being shared over the two communicating parties whereas the latter does not modify. The final output obtained for the cryptography and steganography techniques is cipher text and stegio media respectively. If the unauthorised people discover that there is an exchange of information it is difficult to decode in the cryptography technique while very easy to decode in steganographic methods. The problems encountered by the techniques in terms of technology are also to be taken into consideration. Hence, the study of mathematical functions known as cryptanalysis, which aims to undermine the security of cryptographic processes, can exploit any of the security services provided by cryptography. Cryptanalysis has previously been used to break several hash functions and encryption methods. But another security method may be provided by the stego object; yet, in recent decades,as steganalysis has advanced, steganography has also become more susceptible. The security services such as authentication, confidentiality and identification are offered by both the techniques with the possibility of data integrity and non repudiation being provided only by the cryptographic algorithms, giving it an upper hand [3,7].

Hybrid Model: Steganography and Cryptography

The steganography and cryptography techniques offer certain limitations as mentioned in the previous section and hence, are known to be insufficient for data security if used separately. However, combining these technologies together will result in a more dependable and potent method. The combination of the two techniques also results in the enhanced security of the information being shared between the two parties. When integrated, they will meet all the requirements, including memory capacity, security, and robustness, for the transmission of critical data over an unsecured network. Additionally, it will include a robust system that allows individuals to communicate without coming into notice that there is a means of communication occurring in the first place [1].

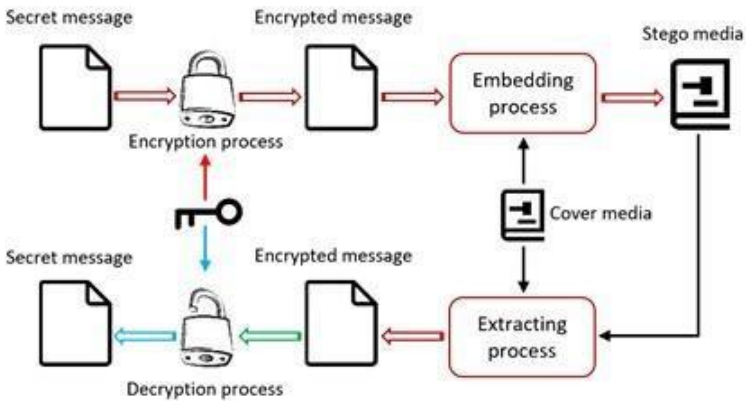

Figure 5: Hybrid Model–Steganography and Cryptography. Adapted from Taha et al., (2003) [1]

Integrating the two techniques develops a mechanism which has the capability to outshine the limitations of each other and this point was proved by researchers in their study. For instance, the study conducted by Dhamija, A et al, (2015) proved that the using SCMACS, an efficient data encryption cryptographic method that makes use of the one's complement approach and it employs a symmetric key technique, wherein the encryption as well as decryption keys are shared between the sender and the recipient of the message. They suggested using the widely used LSB approach for the steganographic component [18]. Then, the research conducted by Vijaya kumar et al., (2016)suggested that using the hyper elliptic curve cryptography in conjunction with DNA sequence which is a steganography technique can be an optimum combination in terms of enhanced safety of the information [19]. It has also been suggested that this hybrid model makes it almost impossible for the attackers to breach the information and unravel the secret information. The encryption in the suggested system was performed using the recently created Two Fish algorithm, while the steganography was performed using the Adaptive B45 steganography approach [1]. Jaspal et al., (2013), conducted a study on a using hybrid approach for image security by providing encryption, followed by hiding the encrypted image within a cover picture. The authors implemented a newer version of AES called MAES for the encryption of the image which provided better performance in comparison to the conventional AES. It divided the actual image into blocks then the cipher image is fabricated. Finally, the encrypted picture is concealed to enable covert communication, making it impossible for anybody to interpret the exchange except for the persons involved [8]. The simulation results of their research proved after examination that the hybrid method that has been suggested is successful against different types ofassaults.

Furthermore, the study conducted by Karthikeyan et al., (2016) concluded that using the hybrid model in which a very strong encryption technique is adapted along with the steganographic technique results in an enhanced safety transmission channel. The authors for securing the confidential information suggested the usage of encrypting technique, AES-18, before embedding it into a QR code. To make sure it can be processed further, the encrypted message in UTF-8 format is then translated to base 64 format and then the scrambling of the encoded image is performed so as to add even more levels of security. Finally, the scrambled OR is then hidden in an appropriate carrier and safely delivered. Through a decoding procedure, the secret data is recovered from the carrier when the recipient receives the message, allowing for a four-level security to be established during the exchange [20].

The research conducted by Padmavathi et al., (2013), involved a detailed performance analysis of the hybrid models which includes DES, AES, and RSA in conjunction with the LSB substitution approach. Based on their respective performances, the investigation conducted by the authors clarified the three encryption methods in every given application. The study found that because AES was the optimal option as it used lesser buffer space and provided faster encryption and decryption speeds in comparison to DES and RSA along with LSB. The point was also proved by the Sridevi et al., (2013), where used AES in combination with LSB for secretly transferring the data. They also mentioned that this model resulted in enhanced levels of security when compared to using single technique at a time[22].

To recapitulate, this approach of using both the techniques together can be a successful means of sharing sensitive data and information with enhanced security. The hybrid model can be highly efficient, robust, extremely fast and a reliable method that aids in preventing the data from the possible attacks to a largeextent.

Conclusion

The primary goal of the paper was to provide a detailed overview of the steganography and

cryptography techniques. The aim of both the techniques, as mentioned in the manuscript was to secure the data over the transmission channel. The two techniques are coherent with each other and are used by individuals or organizations for the common goals of protecting the confidential information, maintaining integrity and ensuring unavailability of information being shared to the attackers and these are a few major fields in ensuring computer security.

Furthermore, the wide applications along with their limitations that the two techniques offer have also been listed. The discussion on the comparison between the techniques provided an overview about the understanding of the two techniques further in detail. Class A and Class B classifications were also presented with the conclusion that Class A were more used in comparison to Class B. Then, a comprehensive review of the studies conducted for the hybrid model have been presented as the usage of the single technique makes the system more vulnerable and hence, the author would recommend the future research to focus largely on the development of the robust and advanced models incorporating both steganography and cryptography. These systems must be able to leverage the advantages of both the techniques and should also pave a path for multi-layered security and hence, improving the resistance to the evolvingthreats.

Table 1: Comparison Between Cryptography & Steganography

Aspect	Cryptography	Steganography
Objectives	To maintain confidentiality, authenticity and also integrity of data	To conceal the information inside a known data or media
Processing Complexities	Requires complex algorithms	Less computationally intensive
Medium to Carry Data	Uses text-based encryption generally	Typically, uses digital media
Type of Attack	Cryptanalysis	Steganalysis
Usage of Key	The key is required for both encryption and decryption	Optional usage of key. Key is used for extraction and embedding purposes, enhancing security.
Detection Difficulty	The presence of the data can be encrypted very easily but the decoding of the data is quite difficult	The presence of the data is difficult to detect and the encrypted data can be exposed using steganalysis
Data Size Impact	The size of the encrypted	The encrypted data does not
	data may be very large in comparison to the actual data	generally result in the increase of the size of the medium.
Output	Ciphertext	Stego-object

References

1. Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., &Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In*IOP conference series: materials science and engineering* (Vol. 518, No. 5, p. 052003). IOPPublishing.
2. Mishra, R., &Bhanodiya, P. (2015, March). A review on steganography and cryptography. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 119-122).IEEE.
3. Almuhammadi, S., & Al-Shaaby, A. (2017). A survey on recent approaches combining cryptography and steganography. *Computer Science Information Technology (CS IT)*,63-74.
4. Sathiaraj, S. F. G., Pingale, G. S., Majumdar, S., Shaikh, S. J., &Thakare, B. S. (2019, July). Secure Transfer of Image-Acquired Text Using a Combination of Cryptography and Steganography. In *2019 1st International Conference on Advances in Information Technology (ICAIT)* (pp. 146-152).IEEE.
5. Rahmani,M.K.I.,Arora,K.,&Pal,N.(2014).Acrypto-steganography:Asurvey. *International Journal of Advanced computer science and applications*, *5*(7).
6. Rajyaguru, M. H. (2012). Crystography-combination of cryptography and steganography with rapidly changing keys. *International Journal of Emerging Technology and Advanced Engineering, ISSN*,2250-2459.
7. Kumar, P., & Sharma, V. K. (2014). Information security based on steganography & cryptography techniques: A review. *International Journal*, *4*(10),246-250.
8. Saini, J. K., & Verma, H. K. (2013, December). A hybrid approach for image security by combining encryption and steganography. In *2013 IEEE second international conference on image information processing (ICIIP-2013)* (pp. 607-611).IEEE.
9. Rakhra, M., Kumar, R., &Walia, H. (2021, September). A Review on Data hiding using Steganography and Cryptography. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-4).IEEE.
10. Mathe, R., Atukuri, V., &Devireddy, S. K. (2012). Securing information: cryptography and steganography. *International Journal of Computer Science and Information Technologies*, *3*(3),4251-4255.
11. Manoj, I. V. S. (2010). Cryptography and steganography. *International Journal of Computer Applications*, *1*(12),63-68.
12. Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7),1062-1078.
13. Conklin, W. A., Arthur, G. W., Cothren, C., Davis, R. L., & Williams, D. (2009). Principles of computer security: Comptia security+ and beyond. *NetwSecur*, *3*,18.
14. Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(4), 307-312.
15. Jirwan, N., Singh, A., & Vijay, S. (2013). Review and analysis of cryptography techniques. *International Journal of Scientific & Engineering Research*, *4*(3),1-6.
16. Raphael, A. J., & Sundaram, V. (2011). Cryptography and Steganography- ASurvey. *International Journal of Computer Technology and Applications*, *2*(3).
17. Gisin, N., Ribordy, G., Tittel, W., &Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145.
18. Dhamija, A., & Dhaka, V. (2015, October). A novel cryptographic and steganographic approach for secure cloud data migration. In *2015 international conference on green computing and internet of things (ICGCIoT)* (pp. 346-351). IEEE.
19. Vijayakumar, P., Vijayalakshmi, V., &Zayaraz, G. (2016). An improved level of security for dna steganography using hyperelliptic curve cryptography. *Wireless Personal Communications*,

89,1221-1242.

20. Karthikeyan, B., Kosaraju, A. C., & Gupta, S. (2016, March). Enhanced security in steganography using encryption and quick response code. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 2308-2312).IEEE.

21. Padmavathi, B., & Kumari, S. R. (2013). A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution. *IJSR, India*, *2*,2319-7064.

22. Sridevi, D. R., Vijaya, P., & Rao, K. S. (2013). Image steganography combined with cryptography. *Council for Innovative Research Peer Review Research Publishing System Journal: IJCT*,*9*(1).

23. Priyadharshini, A., Umamaheswari, R., Jayapandian, N., &Priyananci, S. (2021, February). Securing medical images using encryption and LSB steganography. In 2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT) (pp. 1-5).IEEE.