A SURVEY ON RECENT APPROACHES COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY

Sultan Almuhammadi and Ahmed Al-Shaaby

College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals,
Dhahran, Saudi Arabia

ABSTRACT

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, a secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. Cryptography and steganography are two important techniques that are used to provide network security. In this paper, we conduct a comparative study of steganography and cryptography. We survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present a classification of these methods, and compare them in terms of the algorithm used for encryption, the steganography technique and the file type used for covering the information.

KEYWORDS

Cryptography, encryption, decryption, steganography, stego-image.

1. INTRODUCTION

Information security has grown as a significant issue in our digital life. The development of new transmission technologies forces a specific strategy of security mechanisms especially in state of the data communication [1]. The significance of network security is increased day by day as the size of data being transferred across the Internet [2]. Cryptography and steganography provide significant techniques for information security [3].

The most important motive for the attacker to benefit from intrusion is the value of the confidential data he or she can obtain by attacking the system [2]. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks [4]. A solution for this issue is using the advantage of cryptography and steganography combined in one system [5, 3].

This paper presents a historical background of the art of cryptography and steganography in Section 2, and shows the differences between these techniques. Section 3 gives a literature survey about methods which combine steganography techniques and cryptography techniques. Section 4

David C. Wyld et al. (Eds) : ITCS, SIP, CST, ARIA, NLP - 2017
pp. 63– 74, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70306

presents a comparative analysis of the surveyed methods. The conclusion is in Section 5 with some useful remarks.

2. BACKGROUND

Cryptography and steganography are two approaches used to secure information, either by encoding the information with a key or by hiding it [1, 6, 7, 8]. Combining these two approaches in one system gives more security [5, 9]. It is useful to explain these approaches and discuss the benefits of combining them.

2.1 CRYPTOGRAPHY

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many services, like: confidentiality, key exchange, authentication and non-repudiation. Cryptography provides these services for secure communication across insecure channels, Figure 1 shows the cryptography system [10].

There are three types of cryptographic schemes for securing the data: public-key cryptography, secret key cryptography, and hash functions. These schemes are used to achieve different objectives. The length and type of the keys used depend on the type of encryption algorithm [10].

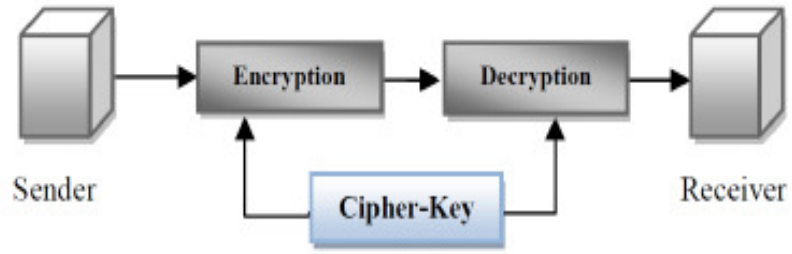

Figure 1: Cryptography System [11]

2.1.1. Symmetric-Key Cryptography

The technique of symmetirc-key encryption is also known as the symmetric-key, shared key, and single-key encryption. In this technique, the same secret-key is used for both encryption and decryption sides. The original information or plaintext is encrypted with a key by the sender. Then the same key is used by the receiver to decrypt the message and obtain the plaintext. The key is known only by those two parties who are authorized to do the encryption and decryption [12]. The technique provide good security for transmission. However, there is a difficulty in the key distribution. If the key is stolen the whole data security is compromised. Moreover, a secure mechanism is needed for safe key-exchange process. Examples of symmetric-key schemes include DES and AES algorithms [12].

2.1.2. Asymmetric-Key Cryptography

This technique is also known as public-key cryptography. It uses two keys, knows as public and private keys, which are mathematically associated, and separately used for encrypting and decrypting respectively. For each user, A, both keys are needed for the scheme to run. The key used for encryption is publicly available, hence it is called user A's public-key, K_{pub_A}. Therefore, all other users can access the public-key K_{pub_A} and encrypt messages to be sent to the user A. On the other hand, the private-key K_{pri_A} is only known by the user A who uses it for decryption. As a main requirement in this scheme, it is computationally infeasible to obtain private-key K_{pri_A} from the public-key K_{pub_A}. An example of asymmetric-key cryptosystem is RSA [10].

2.1.3. Hash Functions

A hash function is a one-way collision-free function with a fixed-length output. Hash functions are also called message digests. A hash function is an algorithm that does not use any key. However, a fixed-length hash value is calculate based on the input data such that it computationally infeasible to obtain the input data from the hash value, or even any input string that matches the given hash value. Hash functions are usually used to produce digital fingerprints of files and to guarantee the integrity of the files [10].

2.2 STEGANOGRAPHY

Steganography can be defined as the art of hiding data and communicating hidden data through apparently reliable carriers in attempt to hide the existence of the data itself. So, there is no knowledge of the existence of the message in the first place. Steganography techniques often use a cover, like an image or another file, to hide the secret information. If a person views the cover which the information is hidden within, there shall be no clue that there is any hidden data under the cover. In this way, the individual won't endeavour to decode the data. Figure 2 shows an overview of steganography system [10].

The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, ciphertext, or anything which can be represented in the form of a bit string. After the secret date is embedded in the cover object, the cover object is called a stego object. The stego object is sent to a receiver by selecting the suitable channel, where a decoder system is used with the same stego method to extract the secret information [10].

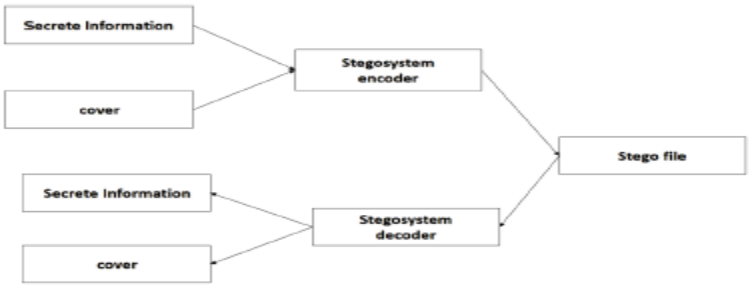

Figure 2: Steganography System

There are various types of steganography. Here are some of the common types:

1. **Text Files:** The technique of embedding secret data inside a text is identified as text stego. Text steganography needs a low memory because this type of file can only store text files. It affords fast transfer or communication of files from a sender to receiver [1].

2. **Image Files:** It is the procedure in which we embed the information inside the pixels of image. So that, the attackers cannot observe any change in the cover image. The least significant bit (LSB) approach is a common image steganography algorithm [1].

3. **Audio Files:** It is the process in which we hide the information inside an audio media. There are many approaches to hide secret information in an audio files, like: Phase Coding and LSB [1].

4. **Video Files:** It is the process of hiding some secret data inside the frames of a video [1].

2.3. Benefits of combine the Steganography and Cryptography

It is noted that steganography or cryptography alone is insufficient for the security of information in all scenarios. However, if we combine these systems, we can generate more reliable and strong systems [9].

The combination of these two strategies will improve the security of the secret information. This combination will fulfill some desired features, like: memory usage, security, and strength for sensitive information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without dragging the attention of eavesdroppers who does not even know of the existence of the secret information being transmitted [5].

3. LITERATURE REVIEW

The significance of network security is increasing day by day as the size and sensitivity of data being transferred across the Internet increase. This issue pushes the researchers to do many studies to provide the needed security. A solution for this issue is using the advantage of cryptography and steganography combined in one system. Many studies propose methods to combine cryptography with steganography systems in one system. These methods were deceased in previous surveys available on this topic, such as [1] published in 2014, which aims to give an overview of the methods proposed to combine cryptography with steganography systems. The authors introduced 12 methods which are combined steganography and cryptography and made a comparative analysis. This comparative has been implemented on the basis of the requirements of security, namely: authentication, confidentiality, and robustness. Another survey [12] was published in 2014. This survey presented many steganographic techniques combined with cryptography, AES Algorithm, Alteration Component, Random Key Generation, Distortion Process, Key Based Security Algorithm.

There has been a continuous rise in the number of data security threats in the recent decays. It has become a matter of concern for security experts. Cryptography and steganography are the best techniques to face these threats. Today, researchers are proposing a blended approach of both techniques to achieve a higher level of security when both techniques are used together.

In [13], the authors proposed an encrypting technique by combining cryptography and steganography to hide the data. In the cryptography process, they proposed an effective technique for data encryption using one's complement method, that they called as SC-MACS. It used a symmetric key method where both sender and receiver share the same key for encryption and decryption. In steganography part, they used the LSB method.

In [14], the authors proposed a highly-secure steganography technique by combining DNA sequence with Hyper-elliptic Curve Cryptography. This approach achieved the benefits of both techniques to obtain a high level of secure communication, besides other benefits of applying DNA cryptography and steganography. The algorithm hides a secret image in another cover image by converting them into DNA sequence using the nucleotide to the binary transformation table. On the sender side, the embedding method includes three steps. First, it converts the values of a pixel of both the cover image and secret image to their respective DNA triplet value utilizing characters to the DNA triplet conversion. Second, it converts the triplet values to binary values format. In the final stage, it applies the XOR logic between binary values of both secret image and cover image to generate a new image which called stego-image.

In [15], the authors presented a new technique called multi-level secret data hiding which integrates two different methods of encryption, namely: visual cryptography and steganography. The first step of this method is to use a method called halftoning, which is used to reduce the pixels and simplify the processing. After that visual cryptography is performed, it produces the shares which form the first level of security, and then steganography is applied using the LSB method to hide the shares in different media like image, audio, and video.

The work in [16] presents a method based on combining both strong encryption algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. An encryption algorithm is employed first to encrypt the secret message before encoding it into a QR code. They used AES-128 to encrypt a message, in UTF-8 format, and converted it into base 64 format to make it compatible for further processing. The encoded image is scrambled to achieve another security level. The scrambled QR code is finally embedded in a suitable cover image, which is then transferred securely to deliver the secret information. They utilized a LSB method to accomplish the digital image steganography. At the receivers side, the secret data is retrieved through the decoding process. Thus, a four-level security has been rendered for a secret message to be transferred.

In [17], the authors presented an image steganography method. At first, they used DES algorithm to encrypt the text message. They used a 16 round DES with 64-bit block size. After that the K-Means Clustering of the pixels which clusters the image into numerous segments and embedded data in every segment. There are many clustering algorithms used for image segmentation. Segmentation includes a huge set of information in the form of pixels, where every pixel additional has three components namely red, green and blue (RGB). After the formation of the clusters, the encrypted text is separated into K segments. These segments are to be hidden in each cluster. They used the LSB method for this purpose.

In [18], the authors concluded that cryptography or steganography alone cannot be used for transmission of data because each has its own weaknesses. So, they proposed a system in which both technigues are used to create a secure system. They claimed that it is nearly impossible for a third party to breach the system and gain confidential data. The system used the TwoFish

algorithm for encryption, while a new approach for performing the steganography is used which called Adaptive B45 steganography technique.

In [19], the authors presented a method to extend the embedding capacity and to enhance the quality of stego-images. The Adaptive Pixel Value Differencing, which is an improved form of Pixel Value Differencing, was utilized as the Steganographic system. AES was utilized as the Cryptographic system. In their method, they used an image as a cover to hide the secret data. These covering images should be in grayscale of size 256 x 256 bits. If the size is higher, they brought it to this range. If the cover image is a color image, they changed it into the grayscale range. They used APVD algorithm to embed the data into the cover image. The resultant stego-image is then encrypted using AES algorithm. It is important to notice here that the encypted stego-image is left uncovered.

In [20], the authors conducted a performance analysis survey on various algorithms like DES, AES, RSA combined with LSB substitution technique which serves well to draw conclusions on the three encryption techniques based on their performances in any application. It has been concluded from their work that AES encryption is better than the other techniques as it accounts for less encryption and decryption times, and uses less memory as buffering space.

In [21], the authors performed a modern method in which Huffman encoding is used to hide data. They took a gray level image of size m x n as a covering image and a p x q secret image. Then, they executed the Huffman encoding over the secret image and every bit of Huffman code of a secret image is hidden into a cover image using LSB method.

In [22], the authors suggested a new steganographic technique based on gray-level modification for true color images using a secret key, cryptography and image transposition. Both the secret key and the secret information are first encrypted using multiple encryption algorithms (Bit-Xor operation, stego key-based encryption, and bits shuffling). These are, later, hidden in the cover image pixels. In addition, the input image is changed before data hiding. Image transposition, Bit-Xoring, stego key-based encryption, bits shuffling, and gray-level modification introduces five various security levels to the suggested technique, making the recovery of data is very difficult for attackers.

In [23], the authors proposed an approach which uses Blowfish to encrypt the secret information before embedding it in the image using LSB method.

In [24], the authors encrypted the secret data using AES algorithm and hashed the key using SHA-1 to prevent attacks. After that, they used the LSB technique to embed the encrypted information in an image, video or audio. The receiver must recover the key which is hashed at the sender side. The secret data can be hidden in any type of media which affords more security.

In [25], hiding information using steganography and cryptography is discussed. A new approach is explained to secure data without decreasing the quality of the image as a cover medium. The steganographic method is used by finding the similarity bit of the message with a bit of the most significant bit (MSB) of the covering image. They used divide and conquer approach for finding the similarity. The outcomes are the bit index position, which is later encrypted using DES algorithm.

In [26], the authors proposed a new method. First, the secret message is changed into cipher text using RSA algorithm and next they hide the cipher text in an audio media using LSB audio steganography technique. At the receiver side, the ciphertext is extracted from audio media then decrypted it into a message by using RSA decryption. So, this technique combines the characteristic of both public-key cryptography and steganography to provide a higher level of security.

In [27], the authors used Blowfish algorithm to encrypt a secret image. They claimed that Blowfish is faster, stronger, and provides better performance than RC6, RC4, DES, 3DES, and AES. They selected a secret image in BMP format and encrypted it by Blowfish. Then, they used LSB method to embed the encrypted image into video frames. This method provides authenticity, integrity, confidentiality and non-repudiation.

The paper [28], is similar to the method mentioned in [27] but the only difference is that the text is selected to be a secret message instead of an image, and it is encrypted using Blowfish algorithm. Next, an image is used to be a cover object with the LSB method to embed the encrypted text into this cover.

In [29], the authors proposed a new strategy employs RSA algorithm with a key of size 128 for encrypting the secret information before embedding it into a cover image, and use F5 steganographic algorithm to embed the encrypted message in the cover image gradually. They selected Discrete Courier Transform (DCT) with random coefficients to embed the secret message by the F5 algorithm. They applied matrix embedding to reduce the changes to be made to the length of the message. This strategy gives a fast system, with a high steganographic capacity, and can prevent observing and analytical attacks.

In [30], the authors have proposed a novel visual cryptographic technique. This technique is suitable for both Grayscale and Bitmap color images. In this approach, the theory of Residual Number System (RNS) was utilized based on the Chinese Remainder Theorem (CRT) for shares creation and shares stacking of a given image. First, they embedded a secret image in a cover image to make a stego-image. An 8-bit pixel of the stego-image is selected and added with an 8-bit key to produce a cipher pixel. They use addition modulo 256 and a pseudo-random number generator with a mixed key generation technique to generated the key. After they encrypted the stego-image, they mapped the cipher pixel into RNS of n elements. Finally, they collected and send the n elements. This approach is extremely fast, secure, reliable, efficient and easy to implement.

In [31], the combination of cryptography and image steganography is achieved by utilizing both AES and LSB algorithms. The authors uses the LSB method to embed the secret information into an image file and they used AES algorithm for encrypting the stego-image. The authors concluded that this technique is effective for secret communication.

4. COMPARATIVE ANALYSIS OF SURVEYED METHODS

In this section, we briefly summarize the differences between cryptography and steganography. Then present a comparative analysis of the methods surveyed in Section 3. Table 1 shows the differences between the steganography and cryptography. The comparison is in terms of:

definition, objective, carrier, number of input files, importance of the key, visibility, security services offered, type of attack, attacks, resultant output, and applications.

Table 1: Cryptography vs Steganography

Criteria/Method	Steganography	Cryptography
Definition	Cover writing [7, 1]	Secret writing [7, 1]
Objective	Maintaining existence of a message secret, Secret communication [7, 1,5]	Maintaining contents of a message secret, Data protection [7, 1, 5]
Carrier	Any digital media [7, 1, 6, 10, 8]	Usually text based [7, 1, 6, 10, 8]
Input file	At least two [6]	One [6]
Key	Optional [6, 7, 8, 1]	Necessary [6, 7, 8, 1]
Visibility	Never [6, 1, 7]	Always [6, 1, 7]
Security services offered	Authentication, Confidentiality,Identification [10]	Confidentiality, Identification, Data Integrity and authentication Non-repudiation [6, 7, 1, 10]
Type of Attack	Steganalysis: Analysis of a file with an aim of finding whether it is stego file or not [6, 1, 10, 8]	Cryptanalysis [6, 1, 10, 8]
Attacks	Broken when attacker reveals that steganography has been used. known as Steganalysis. [6, 5, 7, 1]	Broken when attacker can under-stand the secret message. known as Cryptanalysis [6, 5, 7, 1].
Resultant Output	Stego file [6, 1, 8]	Ciphertext [6, 1, 8]
Applications	Used for securing information against potential eavesdroppers [10]	Used for securing information against potential eavesdroppers [10]

According to the methods surveyed in Section 3, we observed that most of these approaches apply the encryption (cryptography) before the covering (steganography). We classify these methods as Class-A. On the other hand, we classify the methods in which steganography is performed before cryptography as Class-B. This is a useful classification since the methods in the same class usually have similar features. The proposed classes, A and B, of the surveyed methods are illustrated in Figures 3 and 4 respectively.

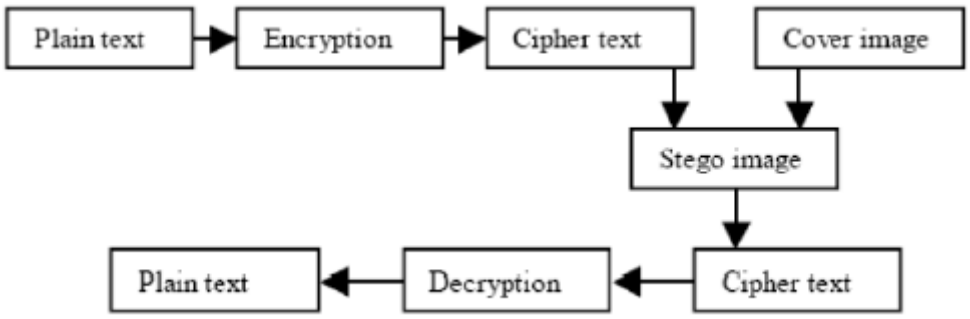

Figure 3: Class A [32]

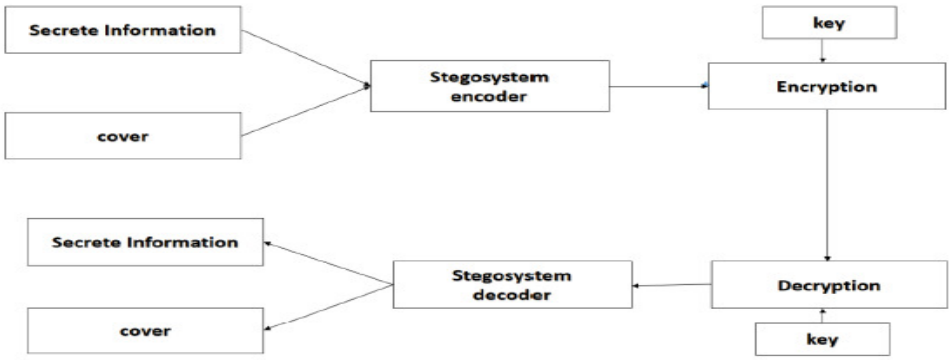

Figure 4: Class B

We included in this study the encryption algorithm used in surveyed methods. The algorithms used in these methods are: AES, DES, Twofish, Blowfish, RSA, etc. Another aspect of this study is the steganography technique and the file type used for covering.

Our study shows that Class-A methods are more popular in the research than the ones of Class-B. Class-A methods have higher security levels and less risk exposing than Class-B since ciphertexts in Class-A is hidden by the steganography technique. While in Class-B, the encrypted stego-image is exposed.

According to the authors of the methods in Class-B, which are mentioned in the literature review, the method of Class-B usually provides larger space for hiding information inside the cover object, because the encryption process is applied to all data inside the cover object. The drawback of this class is that the output file of the encryption process will be vulnerable to suspect of the existence of a secret data inside it. Table 2 summarizes these results.

Table 2: A Comparative Analysis of Surveyed Methods

System	Year	Class	Encryptosystem	Stegosystem	File Type
[13]	2015	A	SCMACS	LSB	Any In Image
[14]	2016	B	HECC	DNA&XOR	Image In Image
[15]	2016	A	VCS	LSB	Image In any
[16]	2016	A	AES-128	QR Code&LSB	Text In Image
[17]	2016	A	DES	LSB	Text In Image
[18]	2016	A	TwoFish	B45	Text In Image
[19]	2015	B	AES	APVD	Any In Image
[20]	2013	A	AES	LSB	Text In Image
[22]	2015	A	Multiple Encryption	XOR	Text In Image
[23]	2015	A	Blowfish	LSB	Text In Image
[24]	2012	A	AES KEY SHA-1	LSB	Any in Any
[25, 32]	2015	B	DES	Same Bit & MSB	Text In Image
[26]	2015	A	RSA	LSB	Text In Audio
[27]	2013	A	Blowfish	LSB	Image In Video
[28]	2013	A	Blowfish	LSB	Text In Image
[29]	2014	A	RSA Key 1024bit	F5	Text In Image
[30]	2013	B	VCS	LSB	Image In Image
[31]	2013	B	AES	LSB	Text In Image

5. CONCLUSION

In this paper, the concepts of cryptography, steganography and their applications in the security of digital data communication across network is studied. A comprehensive technical survey of recent methods which combined steganography and cryptography is presented. Combining these two techniques is found to be more secure than applying each one of them separately.

A detailed comparison of methods combining cryptography and steganography techniques is presented. A useful classification of these methods is proposed. Our study shows that Class-A methods are more common than Class-B and provide better security with less exposing of the encrypted data. The only advantage of Class-B as claimed by the authors of the surveyed methods in this class is providing more capacity for the secret information.

REFERENCES

[1] M. K. I. Rahmani and N. P. Kamiya Arora, \A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp.149{154, 2014.

[2] J. V. Karthik and B. V. Reddy, \Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

[3] M. H. Rajyaguru, \Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250{2459, 2012.

[4] D. Seth, L. Ramanathan, and A. Pandey, \Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975{8887) Volume, 2010.

[5] H. Abdulzahra, R. AHMAD, and N. M. NOOR, \Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978{960, 2014.

[6] P. R. Ekatpure and R. N. Benkar, \A comparative study of steganography & cryptography," 2013.

[7] N. Khan and K. S. Gorde, \Data security by video steganography and cryptography techniques," 2015.

[8] M. K. I. Rahmani and M. A. K. G. M. Mudgal, \Study of cryptography and steganography system," 2015.

[9] C. P. Shukla, R. S. Chadha, and A. Kumar, \Enhance security in steganography with cryptography," 2014.

[10] P. Kumar and V. K. Sharma, \Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.

[11] J. K. Saini and H. K. Verma, \A hybrid approach for image security by combining encryption and steganography," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607{611.

[12] H. Sharma, K. K. Sharma, and S. Chauhan, \Steganography techniques using cryptography-a review paper," 2014.

[13] A. Dhamija and V. Dhaka, \A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICG-CIoT), 2015 International Conference on. IEEE, 2015, pp. 346{351.

[14] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, \An improved level of security for dna steganography using hyperelliptic curve cryptography," Wireless Personal Communications, pp. 1{22, 2016.

[15] S. S. Patil and S. Goud, \Enhanced multi level secret data hiding," 2016.

[16] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, \Enhanced security in steganography using encryption and quick response code," in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308{2312.

[17] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, \Image steganography method using k-means clustering and encryption techniques," in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206{1211.

[18] A. Hingmire, S. Ojha, C. Jain, and K. Thombare, \Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption," International Educational Scientific Research Journal, vol. 2, no. 4, 2016.

[19] F. Joseph and A. P. S. Sivakumar, \Advanced security enhancement of data before distribution," 2015.

[20] B. Padmavathi and S. R. Kumari, \A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution," IJSR, India, 2013.

[21] R. Das and T. Tuithung, \A novel steganography method for image based on huffman encoding," in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on. IEEE, 2012, pp. 14{18.

[22] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, \Secure image steganography using cryptography and image transposition," arXiv preprint arXiv:1510.04413, 2015.

[23] T. S. Barhoom and S. M. A. Mousa, \A steganography lsb technique for hiding image within image using blowfish encryption algorithm," 2015.

[24] S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew, and N. Joseph, \Advanced cryptographic steganography using multimedia files," in International Conference on Electrical Engineering and Computer Science (ICEECS-2012), 2012.

[25] M. A. Muslim, B. Prasetiyo et al., \Data hiding security using bit matching-based steganography and cryptography without change the stego image quality," Journal of Theoretical and Applied Information Technology, vol. 82, no. 1, p. 106, 2015.

[26] A. Gambhir and A. R. Mishra, \A new data hiding technique with multilayer security system." 2015.

[27] M. H. Sharma, M. MithleshArya, and M. D. Goyal, \Secure image hiding algorithm using cryptography and steganography," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp. 2278{0661, 2013.

[28] A. Singh and S. Malik, \Securing data by using cryptography with steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.

[29] M. Mishra, G. Tiwari, and A. K. Yadav, \Secret communication using public key steganography," in Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014, pp. 1{5.

[30] R. H. Kumar, P. H. Kumar, K. Sudeepa, and G. Aithal, \Enhanced security system using symmetric encryption and visual cryptography," International Journal of Advances in Engineering & Technology, vol. 6, no. 3, p. 1211, 2013.

[31] D. R. Sridevi, P. Vijaya, and K. S. Rao, \Image steganography combined with cryptography," Council for Innovative Research Peer Review Research Publishing System Journal: IJCT, vol. 9, no. 1, 2013.

[32] P. Budi, R. Gernowo, M. Si, B. Noranita, S. Si, and M. Kom, \The combination of bit matching-based steganography and des cryptography for data security," 2013.