A Two-Layer Image-Steganography System for Covert Communication Over Enterprise Network

Arome Junior Gabriel(✉), Adebayo Olusola Adetunmbi, and Preye Obaila

Federal University of Technology, P.M.B. 704 Akure, Nigeria
{ajgabriel,aoadetunmbi}@futa.edu.ng,
preyeobaila@gmail.com

Abstract. Computers find application in virtually all aspect of human existence, especially in today's modern world. Although this comes with a lot of benefits, it also comes with a number of undesirable consequences. Chief among these consequences is the rising concerns for security of information and even loss of privacy. Steganography, an Information hiding technique could be a fitting solution to these security issues. This paper presents an improved Steganography technique for ensuring the security of the widely spread and used internet materials or information that are shared globally with risk of vulnerability of attack. In this current research work, Elliptic Curve Cryptography (ECC) and Discrete Cosine Transform (DCT) Steganography were combined together to achieve effective security in the proposed system. A given plain text or secret message is first converted to a cipher text using ECC. The resultant encrypted text is then hidden under a cover-image using DCT-based image steganography technique to produce a final output called stego-image. To the Human Visual System (HVS), the stego-image remains the same as the original cover image. This ensures that the hidden secret message gets delivered to the target recipient without any suspicion. Standard metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), as well as average computation time, were used to evaluate the performance of the proposed steganography system. The results indicate better performance compared to the conventional steganography systems. Thus the proposed system is a 2-level steganography system effective for storing sensitive data and even for securely transferring information over an open/enterprise network.

Keywords: Cryptography · Cyber security · Information-Hiding · Information security · Steganography

1 Introduction

The world has in recent times witnessed an explosive upsurge in technological advancement. Indeed, in today's electronic or modern world, computers and other forms of information technology finds application in so many, if not all aspects of human lives as reported in literature [1–10]. It must be said that computers and their

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12254, pp. 459–470, 2020.
https://doi.org/10.1007/978-3-030-58817-5_34

networks are here to stay, and they offer a wide range of benefits for users. All these come with several other concerns among which is security (privacy, confidentiality, integrity, non-repudiation and authentication) of information and/or individuals. In today's electronic world, access and exchange of all kinds of information ranging from text, audio, video and even images, is quite easy via the Internet [10]. The serious concern however, is that, sharing information over enterprise or open networks exposes such information to all sorts of internet-based attacks [9]. There is a serious need to have a mechanism for ensuring that the protection of sensitive/secret information is guaranteed. Data hiding (information hiding) which plays an important role in information security over the internet can be a viable solution to this problem. Data hiding involves embedding secret data subtly in a cover-media by marginally adjusting the elements of the cover-media. Cryptography method does not conceal the presence of information but rather, it changes a text to a cipher-text which is more like gibberish that cannot be understood. In contrast, steganography deals with hiding the mere existence of a secret communication [11]. So a steganographic system embeds secret information or messages in a text, audio, video or image file so that its existence is not detected by unauthorized persons.

The organization of the rest of this paper is such that, a review of related research works is presented in Sect. 2. In Sect. 3, a vivid discussion on the design of the proposed 2-layer steganography system is presented. Section 4 presents the discussion of experiments' results or findings. Finally, the conclusion of the paper is presented in Sect. 5.

2 Related Works

Quite a number of related works can be found online in other repositories. A summary of the most related ones is presented in this section.

In [12], the authors presented a research on text-based steganography. They used as cover-media, texts written in Malayalam local language. This cover-media was used for hiding secret messages towards ensuring enhanced information secrecy or security. Their research made use of use of two matrices for indexing the alphabets in the common language. These matrices were laden with the alphabet letter and their indices in increasing order. A method for Unicode extraction was designed towards finding the Malayalam text that is corresponding to a given English text. The indexes were selected diagonally. However, the limitation of their work lies in the fact that the hidden word is subject to breach from a cryptanalyst.

In [13], a steganography scheme based on adaptive circular queue image steganography plus RSA cryptosystem is proposed. The objectives was to use both cryptography and steganography to achieve the security of information. For the text to be encrypted RSA cryptography was used, while the resultant cipher-text is embedded in a randomly chosen grey image using a circular queue Least Significant Bit (LSB) steganography technique. RSA is characterized by a very slow key generation procedure. Besides, there is considerable difficulty in the choice of either large prime numbers or small prime numbers.

A research that adopted Genetic Algorithm and cryptography for the development of an image steganography architecture was carried out in [14]. The objective was to develop a secure communication mechanism using a combination of Advanced Encryption Standard (AES) cryptography scheme and a Genetic Algorithm-LSB steganography scheme. A given secret message or text was encrypted AES and then the resultant cipher-text is embedded in a selected cover-image using the steganography scheme. The AES scheme used however presents a limitation in that, there is problem of how to securely exchange the encryption key between a sender and a receiver. Besides, the LSB method can result in much alteration or distortion of the cover-image. This leads to easy detection or attack from attackers. Indeed, since the genetic algorithm competed for space, it is most likely for every information to compete just for a single pixel space which will make the stego different from the cover image.

In [15], a steganography graphical password scheme is proposed for Near Field Communication (NFC) smartphone access control system. The objectives was to create a novel and secured NFC ESGP smartphones security system to ensure convenient and secure use of these smartphone by their owners, as a key access to control systems. They extended the boundary of the capabilities of the technology via the creation of a new and secured NFC ESGP smartphones security system. The combination of both the NFC and the ESGP was in order to achieve higher security compared to the existing one. The work was however exclusively meant for smartphone users only.

The authors in [16] studied the embedding efficiency of LSB steganography technique in spatial and transform domains. Their major goal was to embed a large secret message in a given image using different LSB techniques such as $\pm$ embedding, F5 algorithm with or without matrix embedding. The LSB technique was combined with matrix embedding and F5 algorithm which is applied on both spatial and frequency domain of a given image. If LSB occurs on distortion, it can easily be altered, and wasted by more filtering, compression or a smaller than the original format or size transformation, which gave a very serious limitation to the work.

While working towards improving the properties of images with embedded secrets as well as eliminating the tendency of huge computational complexity in steganography systems, the papers in [17] used particle swarm optimisation algorithm as well as AVX instructions available in modern CPUs. These allow for parallel operations that are vital in image steganography.

An Optical Character Recognition (OCR) based Steganography technique where, messages, in their feature forms, are embedded in a cover image was proposed in [18]. Character level features were extracted from images which contain the textual messages, and embedded in the cover image, thus strengthening the data hiding objective of steganography. They reported impressive results.

In the study titled “Image Steganography and Steganalysis based on LSB”, as reported in [19], Olomo et al. in [19] proposed a new LSB steganography method towards improving on the 1-byte least significance method. The results they presented showed remarkable performance of their model. This work however considered images, and requires some extension to be able to handle audio files as cover media.

An important angle to research in steganography is the audio steganography which uses audio files as cover media for hiding the existence of secret messages. Some authors have carried out studies in audio steganography. For instance, a survey of audio

steganography methods for transmitting data securely was carried out in [20]. The authors posited that LSB is the simplest steganography method, but that when it comes to robustness against attacks, spread spectrum method offers more. Another research effort in the direction of audio steganography is that reported in [21]. The authors developed an efficient audio steganography system that has increased robustness against attack. Their proposed system is reportedly able to embed text messages in both MP3 and MP4 audio file formats, with remarkable effectiveness. As a drawback, audio steganography systems seem to have far more complexities, hence incur more computational overheads than simple-image based ones.

The need for more robust information security systems, especially those that are capable of providing resistance to common classical and quantum attacks has led other researchers to proposing the idea of combining post quantum cryptography with steganography. Such systems were reported in the research papers in [6, 9]. A Quantum image Least Significant Qubit information hiding algorithm that uses a novel enhanced quantum representation (the NEQR) was presented in [22]. The authors demonstrated the algorithm hides the message in the frequency spectrum of an image thereby improving the security of the message.

3 The Proposed 2-Layer Image Steganography System

In order to handle the shortcomings observed in the existing works and provide an improved solution, this current research work (paper) proposes a steganography model that will be used to hide a text (information)'*M*' in an image, in a way that, to the HVS, no visible difference between the cover-image (i.e. image without information) and stego-image (i.e. image with information) will be noticed. The proposed system is made of two (2) modules – The Cryptography (ECC) as well as the Steganography (using DCT on images) modules.

The ECC module makes use of prime Elliptic curve cryptography to provide for a high level of security with smaller key size compared to RSA cryptographic scheme that work based on the difficulty of solving Integer Factorisation Problem. In elliptic curve mathematics operations are carried out on the coordinate points of an elliptic curve using the formula in Eq. 1.

$$E : y^2 + a_2 x_y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{1}$$

The general expression can then be simplified to yield;

$$y^2 = x^3 + Ax + B \tag{2}$$

when $a_2 = a_3 = 0$, x ranges from 0 to arbitrary selected number- 1,while A and B are integer constants.

The encryption procedure is formalised as in Eq. 3 and 4:

$$E_1 = \gamma c \tag{3}$$

$$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B \tag{4}$$

where E_1 *and* E_2 are cipher points which transform to a code table where the cipher text will be derived from. The communication is done between two parties. α is the first party's private key_1, β is second party's private key_1, ϒ stands for a point selected on the elliptic curve, A_1 is the first party general public key_1, A_2 is the first party specific public key, B is the second party private key_2, B_1 is the second party general public key_1, A_B is first party public key for the second party,B_A is the second party specific public key for the first party, c is an agreed point on the elliptic curve.

The decryption process makes use of the Eq. (5)

$$M = E_2 - (\propto E_1 + \propto B_1 + B_A) \tag{5}$$

where M is the plain message after decryption

Discrete Cosine Transform offers a way for hiding large amount of data. It provides high security, a good invisibility and prevents loss of secret message. In DCT the choice of replaceable pixels is based on whether a given pixel has DCT coefficient below threshold are considered as potential pixels. The threshold value here is taken as zero. Hence, the pixels with DCT coefficient value below zero are used for data hiding. The general formula for DCT is:

$$c(u,v) = \propto (u) \propto (v) \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) \cos\left[\pi \frac{(2x+1)u}{2N}\right] \cos \pi \frac{(2y+1)v}{2M} \tag{6}$$

For Embedding, a cover-image is chosen. Then, the DCT coefficient of carrier image is determined. Then traverse through each pixel in the cover-image to the end of the secret image. If the DCT coefficient value is below a stipulated threshold then, replace LSB(s) with MBS(s) of pixels in secret image. Insert 1 at the location in the key matrix, to retrieve the information back get the stego image, traverse through each pixel in the stego image till end. Check the key matrix for the location if it is 1, then extract LSBs from stego image otherwise move on to next pixel get estimate of secret image (Fig. 1).

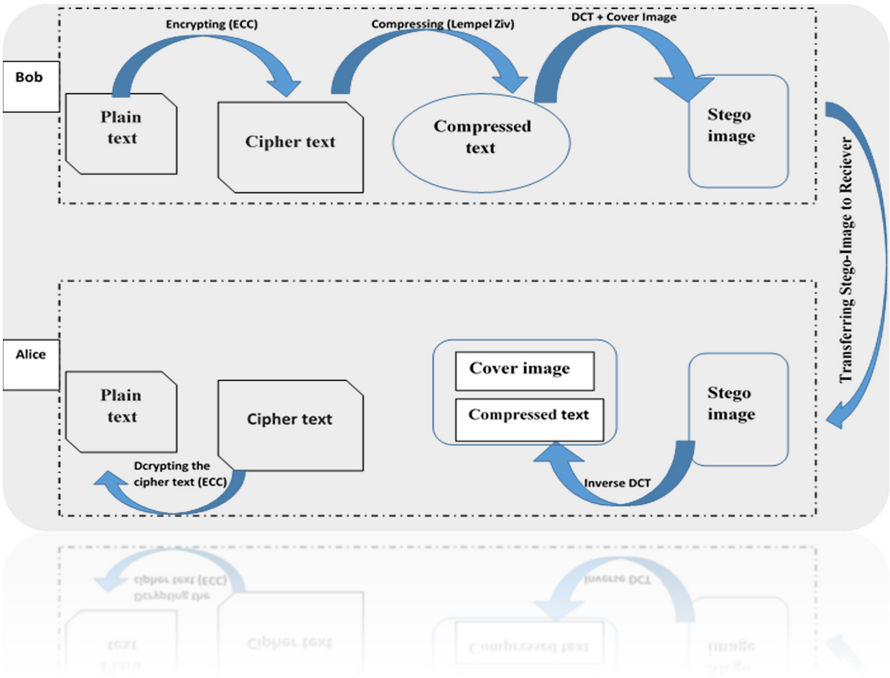

Fig. 1. Conceptual architecture of the proposed system

4 Results and Discussion

The developed system was implemented using MATLAB (R2017a version) programming language on Windows 10 Operating System platform with hardware configuration of 4 GB RAM, 2.0 GHz processor speed and 500 GB of hard disk.

In this research three different images were used as cover images, but any other image can also be used. These images are used to hide different ranges of secret text. To test the result, different sizes of the secret text files (37 KB, 122 KB, 140 KB, 143 KB, and 918 KB) were gotten and then hidden under an image and the quality of the image is tested using PSNR and also a steganalysis software to determine if the image can easily be detected by hackers. The images used for testing are presented in Fig. 2:



Fig. 2. Images used as cover files in this experiment

4.1 System Performance Evaluation Metrics

The proposed/developed system was evaluated based on the following metrics; *Peak Signal-to-Noise (PSNR)*, and *Mean Square Error (MSE).* These metrics are further highlighted as follows;

A Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE)
The Peak Signal-to-Noise Ratio (PSNR) is the metric that was used to access the quality of the resultant stego-image. If the PSNR value is greater than the Mean Square Error (MSE) value then the image has a very good quality. Otherwise, the resultant stego-image is regarded as not of good quality, which implies that the steganography system that produced that stego-image is inefficient.

Results obtained from our experiment shows that the PSNR obtained in all cases have higher values when compared to the corresponding MSE values. This indicates that the proposed system yields good stego-images (Table 1).

The mathematical formula or relations used is for computing the Peak Signal-to-Noise Ratio (PSNR) and the Mean Square Error (MSE) is as defined in Eqs. 7 and 8;

$$PSNR = 10log_{10}MSE \tag{7}$$

$$MSE = \left(\frac{1}{N}\right)^2 \sum \sum_{N} \left(x(i,j) - \bar{x}(i,j)^2\right) \tag{8}$$

Table 1. PSNR and MSE measurements

Cover-image Size (Kb)	Image_1		Image_2		Image_3	
	PSNR	MSE	PSNR	MSE	PSNR	MSE
37	39.6566	7.0375	38.8870	8.4163	35.1439	9.8925
122	39.7091	6.9530	39.0197	8.1491	35.1700	9.7733
140	39.6940	6.9772	38.9815	8.2211	35.1625	9.8074
143	39.6930	6.9787	38.9796	8.2246	35.1622	9.8089
918	39.6533	7.0429	38.8796	8.4163	35.1423	9.8997

$$T \propto S \tag{9}$$

B Steganalysis Testing

Ben 4D steganalysis software was used to carry out the system performance evaluation with respect to its resistance to steganalysis. Three different cover-images (see Fig. 2) were checked to determine the maximum size of test secret file they can contain/embed conveniently before their level of distortion becomes visible to the HSV. These images were also passed through the Ben4D software to determine their maximum embedding capacity just before a steganalysis software is able to detect such distortions. Table 2 shows the highest KB of test secret file each cover-image can take before distortions becomes detectable. Results as shown in Table 2 reveals that, image_1 starts experiencing a little decrease in its luminance component when a large size of 917 KB test file was hidden under it.

Table 2. Result of Ben 4D steganalysis on output of the proposed system.

	Image_1	Image_2	Image_3
Maximum text size before distortion (Kb)	917	917	528
Cover-image characteristics	YCC[1089, 0, 0] RGB[255, 255, 255]	YCC[1056, -26, 31] RGB[255, 254, 247]	YCC[1057, -10, 20] RGB[255, 255, 255]
Stego-image characteristics	YCC[1075, 0, 0] RGB[255, 255, 255]	YCC[1056, -26, 31] RGB[255, 255, 255]	YCC[1056, -26, 31] RGB[255, 254, 247]

Anyone who is interested in hiding a larger text file will be ready to take some form of trade-off time.

C Other Figures and Tables

This sub-section shows the effect of the LZW compression algorithm on some of our ciphertexts, as well as the computation time of the newly developed steganography system versus the existing RSA_DCT based steganography system.

The chart shown in Fig. 3 illustrates the impact of the LZW compression algorithm on the ciphertexts generated by the encryption sub-system of our proposed system. The algorithm obviously reduced the sizes of ciphertexts. The implication is that, the compression allows for more room in the selected cover-image, for the storage or embedding of more secret information. Another implication is that, the size of the

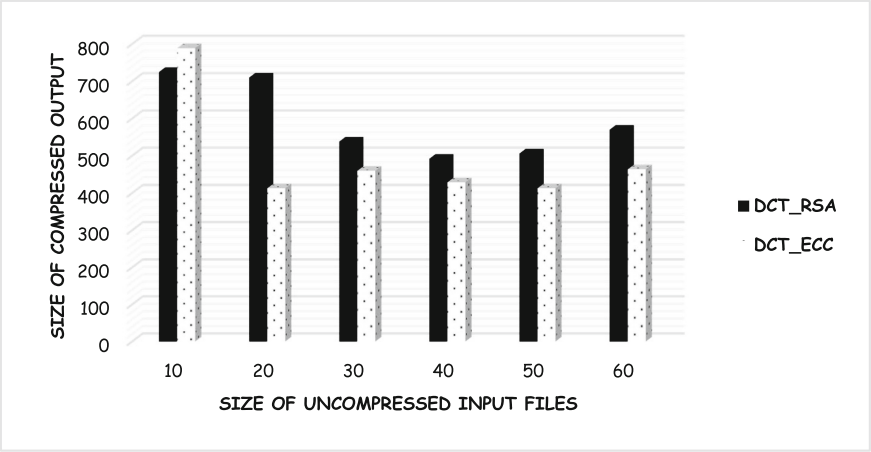

Fig. 3. Illustration of the performance of LZW compression algorithm

resultant output is greatly reduced compared to what is obtainable if compression was not involved. This means that the proposed system is also suitable for resource constrained environments like those obtainable in Internet of Things (IoT).

A performance comparison of the newly developed DCT_ECC based system versus the existing traditional RSA based solutions in terms of the entire computation time was carried out, and the results are as presented in the diagram in Fig. 4. The computation time here refers to the time it takes to encrypt given secret message or data and embed the resultant cipher-text in a chosen cover-image.

These times it takes (in milliseconds), to encrypt and embed a given secret information (text) in a chosen cover-image to yield a stego-image, were recorded and plotted to yield the chart in Fig. 4. It can be clearly deduced that newly developed system

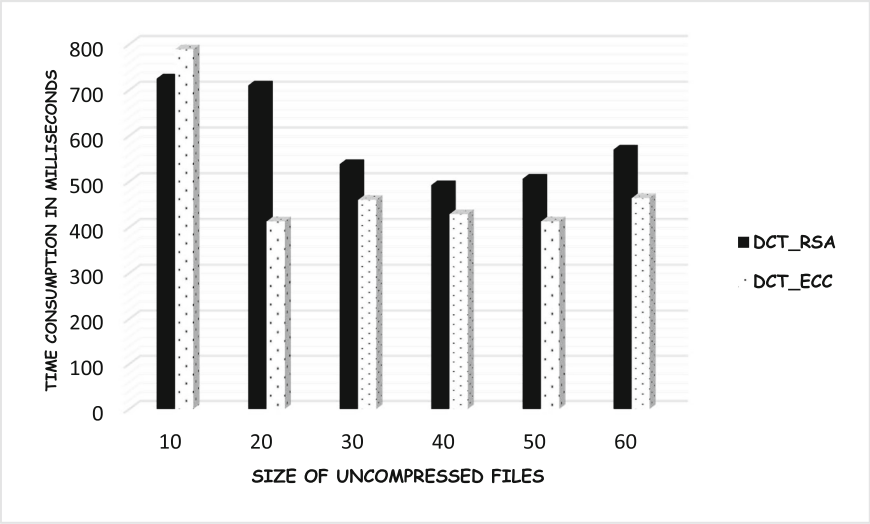

Fig. 4. Performance comparison of our system versus existing RSA-based

records lesser computation times, and therefore can be said to have outperformed the conventional RSA-based one.

5 Conclusion

Although a number of techniques for securing information whether in store or while being exchanged exist, there is a serious need for improvement, as individuals with malicious intents are growing in skills at circumventing existing security solutions. Steganography, an information hiding technique is effective for secure/covet communication, while not even arousing the suspicion of attackers.

In this paper, an improved image-based steganography system that uses Discrete Cosine Transform (DCT), Elliptic Curve Cryptography (ECC) and Lempel-Ziv techniques was developed. Results shows that this system has high capacity for hiding secret messages in cover images. This will enable confidential communications between entities even across enterprise networks. Due to the ECC used, small sized cipher texts are produced after encryption, as against what is obtainable when RSA crypto-system is used for encryption. This counts for robustness on the part of our technique.

Furthermore, the Lempel-Ziv algorithm also helps with compression. This reduces the eventual size of the cipher-text further before embedding same in a selected cover-image.

The performance analysis of the developed system as shown by the output of the Ben4D steganalysis software as well as the PSNR and MSE standard metrics, reveals the robustness of the proposed system for security of information whether in store or in transit across enterprise communication networks.

The work has been able to develop a robust 2-layer steganography system that would be very useful in securing and sharing large amount of sensitive data or information without arousing suspicion.

References

1. Alese, B.K., Gabriel, A.J., Olukayode, O., Daramola, O.A.: Modelling of risk management procedures for cybercrime control systems. In: Proceedings of the World Congress on Engineering (WCE 2014) London, United Kingdom. ISBN 978-988-19252-7-5
2. Daodu, M.N., Gabriel, A.J., Alese, B.K., Adetunmbi, A.O.: A Data Encryption Standard (DES) based web services security architecture. Ann. Comput. Sci. Ser. Tibiscus Univ. **14** (2), 53–58 (2016)
3. Kuboye, B.M., Gabriel, A.J., Thompson, A.F., Joseph, V.O.: Analysis of algorithms in Long Term Evolution (LTE) network. J. Comput. Sci. Appl. **25**(2), 59–71 (2018)
4. Gabriel, A.J., Egwuche, O.S.: Modelling the employees' activities of public service sector using production rules. Anale. Seria Informatică **13**(2), 65–68 (2015). Vol. XIII fasc. 2 – 2015 Annals. Computer Science Series, University of Timisoara, Romania
5. Iwasokun, G.B., Egwuche, O.S., Gabriel, A.J.: Neural network- based health personnel monitoring system. Afr. J. Comput. ICT IEEE **8**(1), 79–87 (2015)
6. Gabriel, A.J., Alese, B.K., Adetunmbi, A.O., Adewale, O.S., Sarumi, O.A.: Post-quantum crystography system for secure electronic voting, open computer science. DeGruyter **9**, 292–298 (2019)
7. Agboola, A.H., Gabriel, A.J., Aliyu, E.O., Alese, B.K.: Development of a fuzzy logic based rainfall prediction model. Int. J. Eng. Technol. **3**(4), 427–435 (2013). ISSN 2049-3444
8. Alabi, O., Thompson, A.F., Alese, B.K., Gabriel, A.J.: Cloud application security using hybrid encryption. Commun. Appl. Electron. **7**(33) (2020)
9. Gabriel, A.J., Alese, B.K., Adetunmbi, A.O., Adewale, O.S.: Post-quantum crystography; a combination of post-quantum cryptography and steganography. In: The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), Technically Co-Sponsored by IEEE UK/RI Computer Chapter, London, UK, pp. 454–457, 9th–12th December 2013
10. Gabriel, A.J., Alese, B.K., Adetunmbi, A.O., Adewale, O.S.: Post-quantum crystography based security framework for cloud computing. J. Internet Technol. Secured Trans. (JITST) **4**(1), 351–357 (2015)
11. Malik, A., Sikka, G., Verma, H.K.: A high capacity text steganography scheme based on LZW compression and colour coding. Eng. Sci. Technol. Int. J. 4–11 (2016)
12. Vidhya, P.M., Paul, V.: A method for text steganography using malayalam text. Proc. Int. J. Comput. Sci. **46**, 524–531 (2015)
13. Jain, M., Kumar, S.: Adaptive circular queue image steganography with RSA cryptosystem. Elsevier Perspect. Sci. **8**, 417–420 (2016)
14. Sethi, P., Kapoor, V.: A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography. Proc. Comput. Sci. **2016**(87), 61–66 (2016)
15. Cheong, S., Ling, H., Teh, P.: Encrypted steganography graphical password scheme for near field communication smartphone access control system. Elsevier Expert Syst. Appl. **41**(14), 3561–3568 (2014)
16. Malathi, P., Gireeshkumar, T.: Relating the embedding efficiency of LSB steganography. Elsevier Proc. Comput. Sci. **2016**(93), 878–885 (2016)

17. Snasel, V., Kromer, P., Safarik, J., Platos, J.: JPEG steganography with particle swarm optimization accelerated by AVX. Special Issue Paper (2019). https://doi.org/10.1002/cpe.544. Wiley; https://onlinelibrary.wiley.com
18. Chatterjee, A., Ghosal, S.K., Sarkar, R.: LSB based steganography with OCR: an intelligent amalgamation. Multimed Tools Appl. **79**, 11747–11765 (2020). https://doi.org/10.1007/s11042-019-08472-6
19. Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F., Mmaskeliunas, R.: Image steganography and steganalysis based on Least Significant Bit (LSB). In: Singh, P.K., Panigrahi, B.K., Suryadevara, N.K., Sharma, S.K., Singh, A.P. (eds.) Proceedings of ICETIT 2019. LNEE, vol. 605, pp. 1100–1111. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-30577-2_97
20. Balgurgi, P.P., Jagtap, S.K.: Audio steganography used for secure data transmission. In: Kumar, M.A., Selvarani, R., Kumar, T. (eds.) Proceedings of International Conference on Advances in Computing. Advances in Intelligent Systems and Computing, vol. 174. Springer, Heidelberg (2013). https://doi.org/10.1007/978-81-322-0740-5_83
21. Adeboje, O.T., Adetunmbi, A.O., Gabriel, A.J.: Embedding text in audio steganography system using advanced encryption standard and spread spectrum. Int. J. Comput. Appl. (0975–8887) **177**(41), 46–51 (2020). https://doi.org/10.5120/ijca2020919
22. Wang, S., Sang, J., Song, X., Niu, X.: Least Significant Qubit (LSQb) information hiding algorithm for quantum for quantum image. Measurement **73**, 352–359 (2015)