CRYPTO-STEGANOGRAPHY APPROACH FOR SECURE DATA TRANSMISSION USING IMAGE AND AUDIO FILES

S. Zaware
AISSMS Institute of Information Technology, Pune
sarikazaware@gmail.com

ABSTRACT

In today's world as the number of people who have means of approach to the internet or technology is growing rapidly, so the need to conceal the sensitive data from attackers is of vital importance. On daily basis copious amount data transmissions take place which need to be secure and care needs to be taken that the sensitive data does not fall in any wrong hands. Various systems have been actualized previously in which single tier security is provided which is not that coherent and the systems are quite vulnerable. In order to overcome this impediment, the proposed system in the paper consists of 2 tier security which includes keyless cryptography and steganography. In Cryptography plain text is converted into cipher text and secrete message is embedded at the sender side which is decrypted at the receiver side. Whereas steganography is the process of hiding data behind the images. The first phase in the proposed systems includes cryptography which uses random logic for encryption and the second phase includes steganography which uses GCD logic. All the algorithms used in this system are keyless which in turn adds up to more security and makes the system light weighted.

Keywords: *Cryptography, Steganography, Encryption, Decryption, secrete message, cipher text.*

1. Introduction

Internet plays an important role for data transmission and data sharing. It is a worldwide and publicized medium, some confidentiality data might be stolen, copied modified or destroyed. In the recent years, there has been rapid growth in the technology and data security has become a major issue for internet users. Cryptography and Steganography are the most used techniques by developers for securely transferring the data. Cryptography means converting a plain text into an unreadable text also known as cipher text. It is the process of encrypting the secret message at senders' side and then decrypting the message at receivers' side so that even if someone steals the data in between it won't be of any use. At present large number of cryptography algorithms have been created with the primary objective of converting the text in to unreadable format for secure transmission. Cryptography mainly involves two types of keys: Symmetric key and Asymmetric key transmission (Prashanti et al., 2017). In symmetric key transmission a common key is used for encryption and decryption of the message. In asymmetric key transmission different keys are used for encryption and decryption of the message. Asymmetric key is more secure but requires more time for encryption than symmetric encryption.

The term Steganography (Gupta et al. 2014) is derived from the Greek word "steganos" which means Covered and "graphein" means writing (Mehboob et al. 2008). It is method of hiding the secret data inside the cover image such that only the receiver knows that the message is present in the image. It is very difficult for the third party to even detect that the message is being sent. Steganography can be classified as keyless, symmetric and asymmetric. In symmetric and asymmetric the key is privately shared between the sender and the receiver. The key is shared prior to sending the message. The process of steganography is highly based on the type of media used to hide the message (Mehboob et al. 2008). Commonly used medium include text, image files, audio files and the protocols used in network transmission. Most of the times image steganography is preferred media because the difference in the image after encryption is impossible to detect with naked eyes.

2. Literature Review

Our Work proposes a two-tiered secured system for data transmission using keyless cryptography and steganography which can be efficiently used for secured transmission of data. There are number of related works available. An Enhanced Text to Image Encryption Technique using RGB Substitution is proposed in (Joshy et al. 2017). The proposed model works in such a way that if anyone decrypts the image in which the data is hidden then he gets another image, which further confuses him whether the actual information is in text or in image format. Even when the same characters are repeated it cannot be tracked, since each character is assigned with random values whenever it repeats. And the AES encryption technique used make the data secure, for transmitting it over an insecure network. A new scheme for solving the problem of embedding positions based on edges is proposed in (Rashid & Majeed, 2019). For more clarity the algorithms used were divided into two main schemes: Embedding Scheme and Extraction Scheme. The proposed used color images as cover, after separating selected cover image into their components, then one of the components used to find the edge position to be used as an index for the embedding positions at the other color image components. In this paper it was determined that depending on the structure of the image the threshold value is selected dynamically (i.e. the schemes does not use the same threshold value of edge detection for different images but it will be different depend on the image). This makes the proposed method in the paper more secure because this threshold value can be used as a key between the sender and the receiver, also the value of the threshold changes when the cover image is changed.

A new steganography method for Embedding Message in JPEG Images is proposed in (Darbani et al. 2019). In this study, a steganography technique in JPEG images is proposed. Since a part of data may be lost after the discretization (or quantization) of frequency values in the JPEG compression procedure, in the proposed method, the embedded message is added to the image after the discretization stage. The method utilizes two adjacent pixels in the steganography process. For this purpose, two less significant bits of each pixel are considered for the embedding. The embedding process is performed according to a replacement table. Based on the bit's values in the embedded message, the pixel bits may be changed (increased or decreased). In order to evaluate the performance, two criteria, PSNR and maximum capacity of steganography have been calculated. The methods used in the paper are able to keep more amounts of secret data while the quality of the images is almost similar to the original.

Researcher (Ramalingam et al. 2020) proposes video cryptography; this is applicable to our current research. But the focus of proposed research is audio and video cryto- stegno analysis instead of complete audio file.

The research work proposed in (Duan et al. 2020) is applying image elliptic curve and deep neural network for image steganography. They propose high capacity image steganography and considering pay load parameter. But in case of security it is not always the requirement to high capacity images every time.

Researcher (Varalakshmi, 2020) elaborated the role of image steganography in cybercrime. They presented the application of this proposal for society use effectively. The model proposed (Kanojia et al. 2019 and Bhagat et al. 2018) is basically a hybrid of both steganography and cryptography. They have developed a technique in which the cover image is used to hide data such that first it is converted into the 85-bit stream from 7-bit stream and then the hiding place is determined by a secret key. This hiding place is not directly visible and only be recovered with the use if the secret key. This makes our technique more reliable and promising. The recovery of data just follows the reverse path. The results confirm the power of our technique and in future we will develop more robust way to increase the capacity of our technique.

Author of research paper (Zaware, 2019) successfully implemented the secure result generation system. The results are tested on different input files. The input files are in .txt format and its contents are like university mark sheet. The mark sheet generation system, presented in this research is very effective and secure way to store and retrieve the original documents from the universities or colleges. It is also the best way to save a lot of digital space which is required by universities to preserve the result copy of the student. As originals are kept in encrypted format followed by QR code it is very secure and no one cannot be tampered. Any QR code scanner can scan this QR code printed on result but it will get the encrypted cipher text as the output, as it cannot be decrypted by any QR code reader.

3. Workflow of Crypto-Steganographic System

Cryptography and steganography are the most commonly used technologies whenever we consider about the secured data transmission over the internet. In this new era of technology, everyday a new encryption method is proposed which requires an encryption key and the mapping database for it. In our method we are proposing a method with keyless encryption and decryption. This method is very light weighted and secure as there is no such separate key is required. The key to decrypt that message is itself encrypted within the message. In the traditional key encryption method if the key is somehow stolen by the third person then the data can be misused. Therefore, the proposed system is more secure because there is no involvement of transmission secret key.

In our system there two main parts of encryption

A. Text to text cryptography
B. Text to image steganography

By having these 2-way encryptions, the security of the system increases.

A. Text to text cryptography

In proposed system the encryption in first phase depends upon the length of the secret message. Each letter is first converted into its Unicode value. This Unicode value is added into the total length of the message. The result of this is considered as a Unicode and the symbol associated with that Unicode is used for that letter. By this method every time the encryption letter changes with the change in the length of the message. For decrypting the message this process is used in reverse manner. The Unicode of each letters is decreased by the total length of the message and then it is converted into the actual letter.

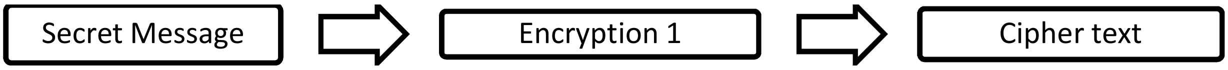


Figure 1: Text to text cryptography

Algorithm1: Text to text cryptography
Step 1: Get the Unicode of the secret message for each letter.
Step 2: Get the total length of the secret message.
Step 3: Add the total length into the Unicode to get a new Unicode for each letter.

$$C = \sum_{0}^{n+1} unicode(S_0^n) + (n)$$

Where, C = ciphertext
S = secret message
n = total length of message

Step 4: Generate a new character formed by the new Unicode for each letter.
Step 5: Make a new message by using these new characters.
Step 6: Store this new message as *ciphertext* for further encryption.

B. Text to image steganography

In the first phase the text is encrypted into another text. In this phase, the system will encrypt that text into an image. For this the system uses a sample image to hide the text behind it. First image is converted into its bitmap where each pixel represents its RBG value. The text is treated as a pixel so every letter in the text acts as one pixel. These pixels are plotted in the sample image by replacing some of its pixels. For choosing which pixels to be replaced are decided by using the GCD logic (Whiting). In this the GCD of the length and width of the image is found and it stored in n. After this, every nthpixel of the image is used for the replacement. When the replacement is done a new image is formed and this image is used for the transmission. While decrypting the image again GCD is found and the pixels on that result are converted back into the text

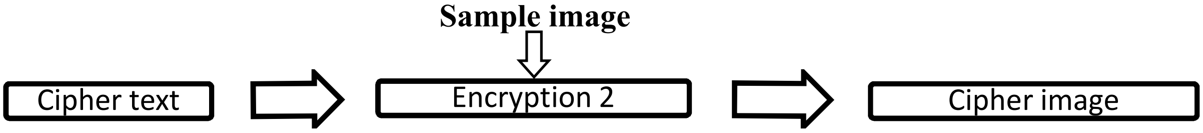


Figure 2: Text to image steganography

Algorithm2: Text to image steganography
Step 1: Get the *cypher text* convert it into binary.
Step 2: Get the sample image for encryption.
Step 3: Convert the image into its RBG format.
Step 4: Calculate the GCD of the height and width of the image.
Step 5: Store GCD into *n*.

GCD (length, 0) = length

GCD(length , width) = GCD (width , length – width $[\frac{length}{width}]$ *)*

Step 6: Replace each n^{th} pixel of the image by each symbol in cipher text.
Step 7: Store the next n^{th} pixel value as 0.
Step 8: Convert the RBG format into the new image.
Step 9: Store the new image as cipher image.

The combination of algorithm1 and algorithm2 completes the encryption part of the whole system. The encrypted image is transmitted over the network. Once the receiver receives the encrypted image the system decrypts the data from the image using the same logic in reverse manner. The workflow for the entire system is given in Figure 3.

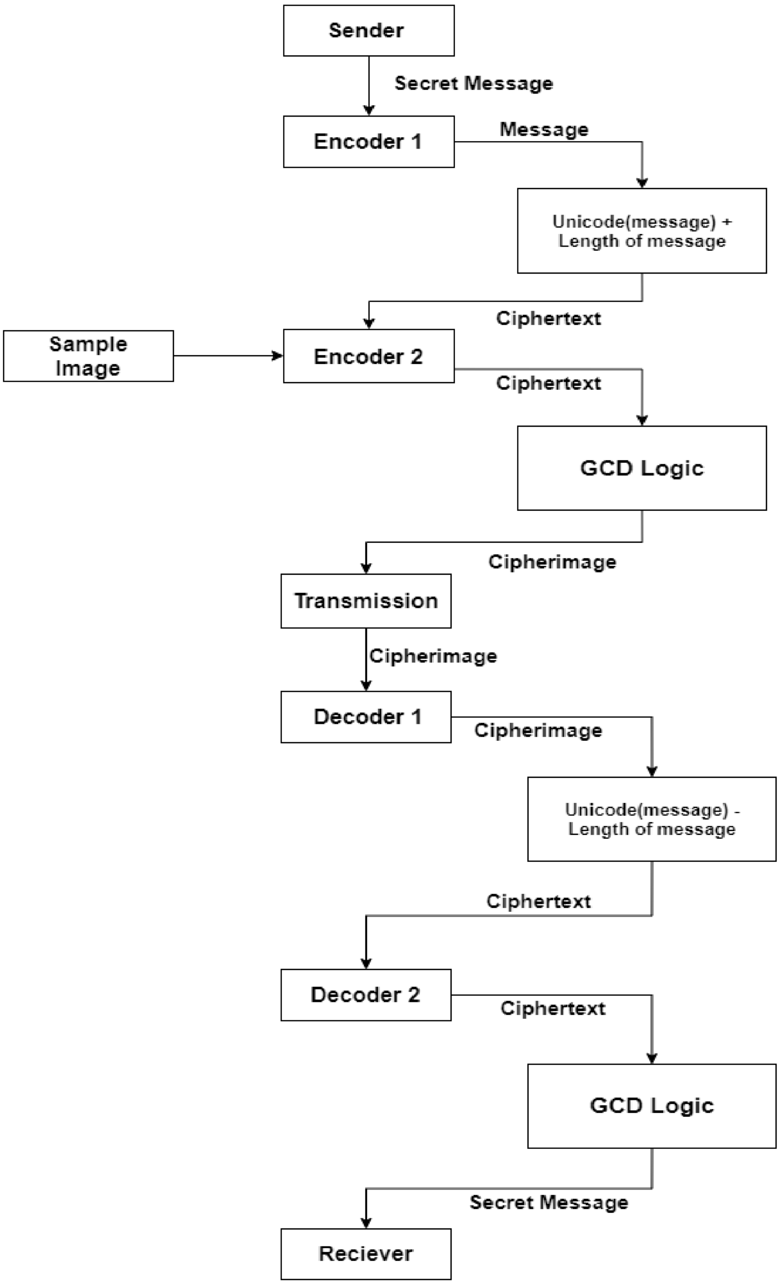
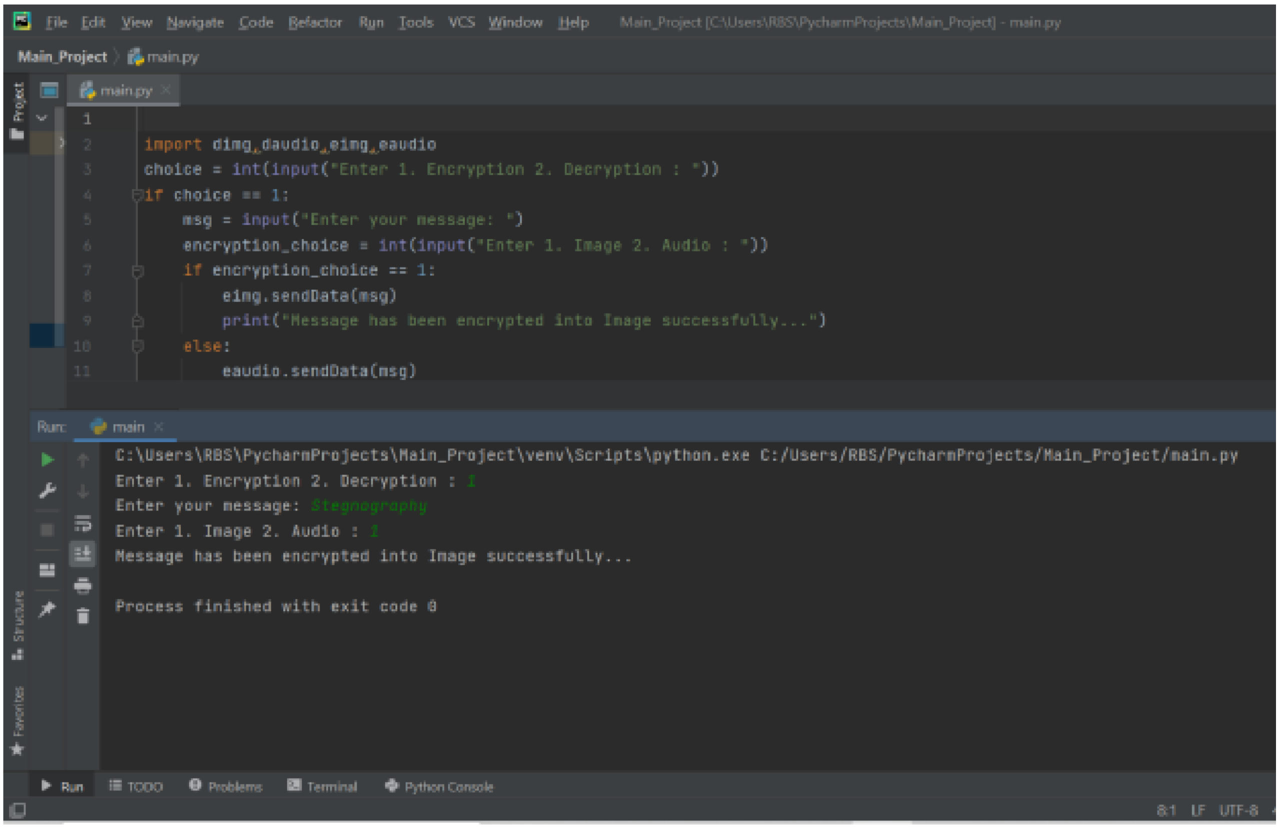


Figure: 3: Workflow of Crypto-steganographic system

4. Result Analysis

After the first phase of the proposed system the cipher text of the secret message is shown in the figure below:


File Edit View Navigate Code Refactor Run Tools VCS Window Help Main_Project [C:\Users\RBS\PycharmProjects\Main_Project] - main.py
Main_Project main.py
main.py
Run: main
Run TODO Problems Terminal Python Console
8:1 LF UTF-8

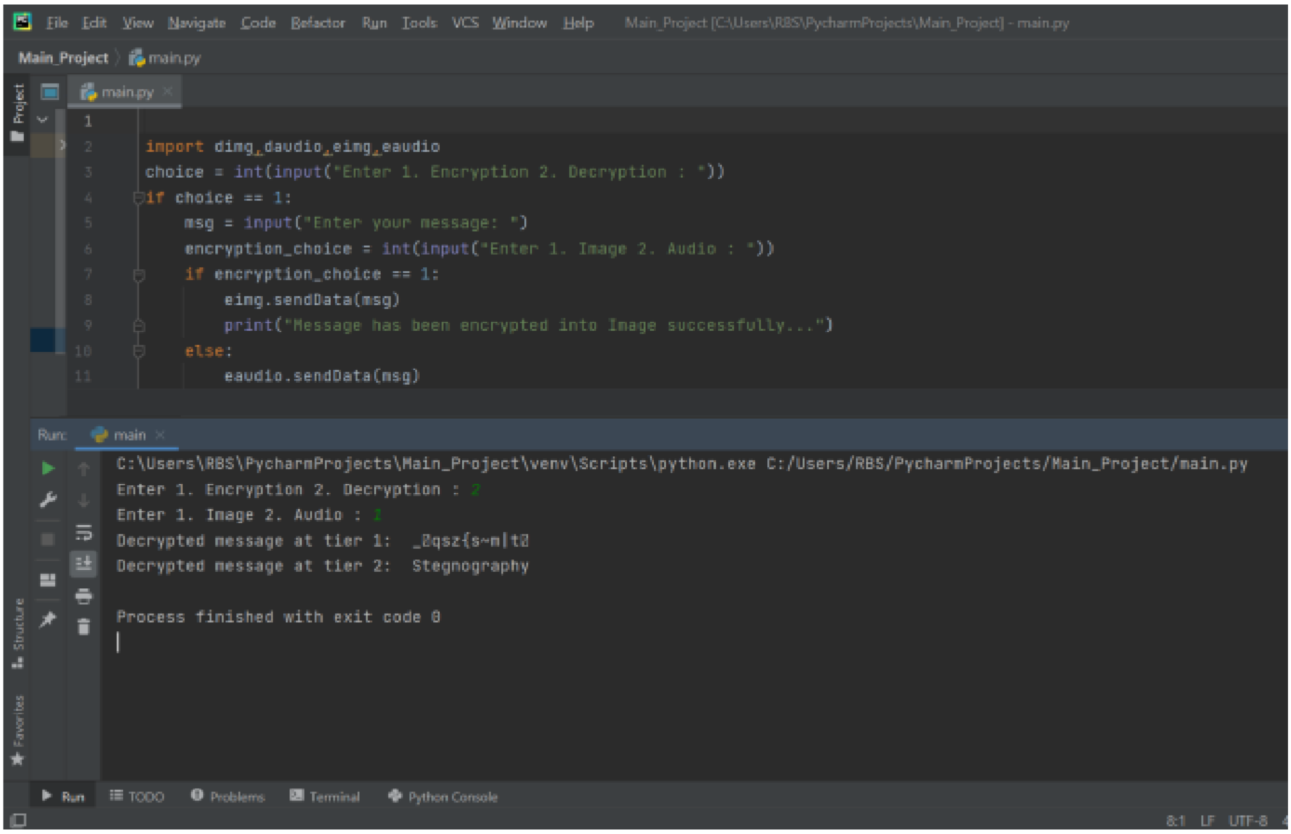
```

import dimg,daudio,eimg,eaudio
choice = int(input("Enter 1. Encryption 2. Decryption : "))
if choice == 1:
    msg = input("Enter your message: ")
    encryption_choice = int(input("Enter 1. Image 2. Audio : "))
    if encryption_choice == 1:
        eimg.sendData(msg)
        print("Message has been encrypted into Image successfully...")
    else:
        eaudio.sendData(msg)
```

```
C:\Users\RBS\PycharmProjects\Main_Project\venv\Scripts\python.exe C:/Users/RBS/PycharmProjects/Main_Project/main.py
Enter 1. Encryption 2. Decryption : 1
Enter your message: Stegnography
Enter 1. Image 2. Audio : 1
Message has been encrypted into Image successfully...

Process finished with exit code 0
```

Figure: 4: Text to Text Cryptography Example 1


File Edit View Navigate Code Refactor Run Tools VCS Window Help Main_Project [C:\Users\RBS\PycharmProjects\Main_Project] - main.py
Main_Project main.py
main.py
Run: main
Run TODO Problems Terminal Python Console
8:1 LF UTF-8

```

import dimg,daudio,eimg,eaudio
choice = int(input("Enter 1. Encryption 2. Decryption : "))
if choice == 1:
    msg = input("Enter your message: ")
    encryption_choice = int(input("Enter 1. Image 2. Audio : "))
    if encryption_choice == 1:
        eimg.sendData(msg)
        print("Message has been encrypted into Image successfully...")
    else:
        eaudio.sendData(msg)
```

```
C:\Users\RBS\PycharmProjects\Main_Project\venv\Scripts\python.exe C:/Users/RBS/PycharmProjects/Main_Project/main.py
Enter 1. Encryption 2. Decryption : 2
Enter 1. Image 2. Audio : 1
Decrypted message at tier 1:  _▯qsz{s~m|t▯
Decrypted message at tier 2:  Stegnography

Process finished with exit code 0
```

Figure: 5: Text to Text Cryptography Example 2

The cipher text for each letter changes with the change in the length. In Figure 4, the letter 'H' is converted into symbol (') and in Figure 5, the same letter is converted into symbol (\).

After the phase 2 of the proposed system the sample image as in Figure 5 is embedded into the image shown in Fig 7.The difference between the two images as shown in Figure 6 and 7 is not recognizable by the naked eyes.

Figure: 6: Sample Image before Encryption

Figure: 7: Sample image after Encryption

The Encryption and decryption of the secret message is successful after both the phases of the proposed system.

5. Conclusion

Most often to provide security with the help of cryptography or steganography or even both which includes transference of secret key. But we have proposed a system which combines both cryptography and steganography with keyless transmission which improves security at greater extent. In this system the cryptographic method involves a different technique which uses message length and its Unicode value for encryption and similarly steganographic method also uses different technique which uses format like bmp, jpg etc. We have tested the system on different size of images from 250 x 150 to350 x 250. We found the result in such a way that the data hidden in the cover image does not affect the original size of the image. More than 90% of the image is preserved and only the intended receiver knows its existence.

6. Future Scope

The main objective of crypto-steganography system is to hide the message in to image. When we are considering message, it doesn't face any problem related to size. We have tested the above system for up to 5 to 6 sentences and it works efficiently. But in future if we think to extend this system for providing security to the document then we need to do some enhancement into the algorithm which we have used. In present system we are first encrypting the message and then this cipher text is hidden in the image using LSB substitution with GCD logic. But for the enhancement of this system we can use RGB substitution, AES, Random key dependent algorithms in combination; so that this system can be used for providing security to preservation of documents.

References

1. Bhagat, Jayti, Gupta, P. and Kohli, N. (2018), "Image Steganography Using Improved Algorithms to Enhance Security and Payload of Traditional LSB Substitution." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE.
2. Darbani, A., AlyanNezhadi, M.M. and Forghani, M. (2019), A New Steganography Method for Embedding Message in JPEG Images, 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), Tehran, Iran, pp. 617-621

3. Duan, X., Guo, D., Liu, N., li, B., Gou, M., and Qin, C. (2020), “A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network", IEEE Access publication February 4, 2020
4. Gupta, R. and Singh, T. P. (2014), "New proposed practice for secure image combing cryptography steganography and watermarking based on various parameters," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, pp. 475-479
5. Joshy, A., Baby, K. X. A., Padma, S. and Fasila, K. A. F. (2017), "Text to image encryption technique using RGB substitution and AES," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, pp. 1133-1136.
6. Kanojia, Pallavi & Choudhary, V. (2019). LSB Based Image Steganography With The Aid of Secret Key and Enhance its Capacity via Reducing Bit String Length. 257-262. 10.1109/ICECA.2019.8821917
7. Mehboob, B. and Faruqui, R. A. (2008), "A stegnography implementation," 2008 International Symposium on Biometrics and Security Technologies, Islamabad, pp. 1-5
8. Prashanti, G., Jyothirmai, B.V. and Chandana, K.S. (2017), "Data confidentiality using steganography and cryptographic techniques," 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, pp. 1-4.
9. Ramalingam, M., Nor Ashid Mat Isa and Puviarasi. (2020), “A secured data hiding using affine transformation in video steganography", 3rd International conference on computing and network communication 2019, Procedia Computer Science 171 (2020) 1147–1156
10. Rashid, R. D. and Majeed, T. F.(2019), "Edge Based Image Steganography: Problems and Solution," 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, pp. 1-5.
11. Varalakshmi, R. (2020), "Digital steganography for preventing cybercrime using artificial intelligence technology", Journal of critical reviews ISSN - 2394-5125, vol 7, issue 6.
12. Whiting E (n.d.) accessed on 31st December 2020 from https://dev.to/erikwhiting88/let-s-hide-a-secret-message-in-an-image-with-python-and-opencv- 1jf5
13. Zaware, S. (2019), “Secure Digital Document Generation Using QR Code” Journal of Adv Research in Dynamical & Control Systems, ISSN: 1943-023X, Vol. 11, Special Issue-08, and 3241-3249