ISSN No:-2456-2165

Enhanced Security using Elliptic Curve Cryptography Combined with Hill Cipher

Dr. T. Madhavi Kumari[1]; K. Shyam Kumar[2]
[1](Professor of ECE, JNTUH University College of Engineering, Science and Technology Hyderabad, India)
[2](ECE, JNTUH University College of Engineering, Science and Technology Hyderabad, India)

Abstract:- Technology has improved significantly, and usage of smart systems has increased the risk to secure data and privacy. Since most operating systems come with built-in apps that aren't secure, there is rapid increase in risk of information or data cloning, forgery, tampering, counterfeiting, etc. End users will suffer an unrecoverable loss as a result, particularly with regard to social media personal data and banking applications. An efficient and robust technique which has Hill cipher combination with elliptic curve cryptography is proposed to deal with major threats and improve data security. This technique uses LSB (Least Significant Bit) watermarking to embed DCT coefficients of an image and ciphertext of message into base image. Using Hill Cipher algorithm, the ciphertext is produced. Elliptic Curve cryptography (ECC) and combination with Hill cipher to increase complexity, considering the fact that it has poor data security and is readily cracked. The key is generated by using ECC algorithm, and this key is used with the Hill cipher technique to produce ciphertext. Cryptography and Steganography both combined provide the data with greater legitimacy and ownership for media applications. Without a proper key, it proves difficult to get the hidden message and the image. For multimedia applications, the performance of hiding data and image in image data has been analyzed.

***Keywords*:-** *Steganography, Cryptography, Elliptic Curve Cryptography, Hill Cipher, Self-Invertible Matrix, Discrete Cosine Transform, Least Significant Bit.*

I. INTRODUCTION

As multimedia items like photographs, audio clips, and video files take up a lot of storage space when uploaded to the cloud [1], the risk to data security and privacy has grown as more digital information and data are exchanged over the internet [2]. Due to the risk of unauthorized copying, copyright protection and ownership identification are becoming crucial issues [3]. In comparison to knowledge-based procedures like identity cards, passwords, etc., biometric-based authentication systems are becoming more and more successful[4]. The approach needed to remedy this issue is digital watermarking [5]. However, this paper focuses on improving the data privacy, security.

Steganography is used to conceal data and eliminate the possibility that it contains sensitive information [6]. The assurance of secure information becomes crucial, especially for economic data like money and interest rates. To increase security and data privacy, several approaches have been enhanced.

II. LITERATURE REVIEW

An improved safe cryptographic system based on the Paillier cryptosystem was presented by S. Xiang and X. Luo [1]. Mirroring Ciphertext Group (MCG) and modular multiplicative inverse operation are utilized to recover the data in this system. A technique that combines information concealing and encryption was suggested by Xinyi Zhou et al. in [2]. The Rivest Shamir Adleman (RSA) algorithm is used to transform the key message into the bitstream before encrypting it. Secret data and the smallest amount of green are XORed in logic, and the outcome is embedded in the smallest amount of red or blue. When compared to the conventional Least Significant Bite (LSB) method, the Peak Signal to Noise Ratio (PSNR) improved. Through a partition-wise quantification Singular Value Decomposition (SVD), Tao Wang et al. [3] devised a technique for scrambling a picture and embedding a watermark. Two types of amplitude modulation-based watermarking techniques were given by Anil K. Jain et al. in their paper [4]. The user's face data is kept in fingerprint representations in the second case, whereas fingerprint minutiae data is stored in the first case. A watermarking approach based on the Integer Discrete Cosine Transform (DCT) method was presented by Ayush Vashistha et al. in [5]. The Fast Fourier Transform (FFT) filter was used to improve the fingerprint's binary image, which was then segmented and binarized. A hybrid encryption scheme employing the Advanced Encryption Standard and RSA algorithm was presented by M. Elhoseny et al. in [6]. The suggested method starts by utilizing 2D-DWT-1L or 2D-DWT-2L to encrypt the secret data and then conceal the end result in a cover picture. A technique where the input data is encrypted and decrypted using the RSA algorithm was proposed by Y. K. Singh et al., [7]. A stego picture is created by placing the encrypted data in an image and then using the DCT method, enhancing the stego image. From Elliptic Curve Cryptography, the Key is generated and cipher-text is generated by Hill Cipher using this key. Elliptic Curve Cryptography and Hill Cipher (ECCHC) combination not only increases the security but it also makes system more efficient compared to the traditional Hill cipher Algorithm.

ISSN No:-2456-2165

III. PROPOSED METHOD

Cryptography, the study of the process of encoding and decoding information, has evolved as an effective tool for protecting digital communication's privacy, integrity, and validity. Cryptographic techniques use mathematical procedures to convert plain text, readable data into ciphertext, which seems random and unintelligible. Only authorized person with the right decryption algorithm or key may reverse this procedure and access the original communication. Steganography goes beyond cryptography by masking data, making it impossible for unauthorized parties to decode the secret message. Steganography, which is derived from Greek terms "steganos" (which means "covered or concealed") and "graphein" (which means "writing"), has a long history dating back thousands of years. Steganography works on the basis of that the human vision and other sensory perception systems are restricted in their ability to notice small changes in digital material.

The proposed method is a combination of cryptography and steganography techniques by embedding a text/image into an image. Encrypting embedded information is considered too more efficient and secure. This method achieves a great level of data security, privacy. Without a proper cryptoanalysis, it is very hard to retrieve the plain text from a stego-object. Using Hill Cipher, we can encrypt the text. But the problem with this approach is, the ciphertext is easily broken and has less adequate security. So, to add some complexity, ECC is combined with Hill cipher. At first using ECC, the key is generated and using this key, generate the key matrix for Hill Cipher algorithm and this hill cipher generates the ciphertext. After performing this encryption algorithm, there is a need of proper key to decrypt ciphertext. The ciphertext generated is taken as JSON object and encrypted into the base image.

This method's subsequent step is to combine a picture into a base image. We initially apply a DCT to the picture and take into account the DCT coefficients for that. We translate these DCT coefficients, which vary from 0 to 255, using basic mathematical operations. The DCT coefficients are converted to a JSON object, and then using the Least Significant Bit technique, the full JSON object is embedded into the base picture. We can simply use a bit xor technique to extract our JSON item during decryption while utilizing the same LSB. Fig 1 Depicts the Suggested Method's Layout.

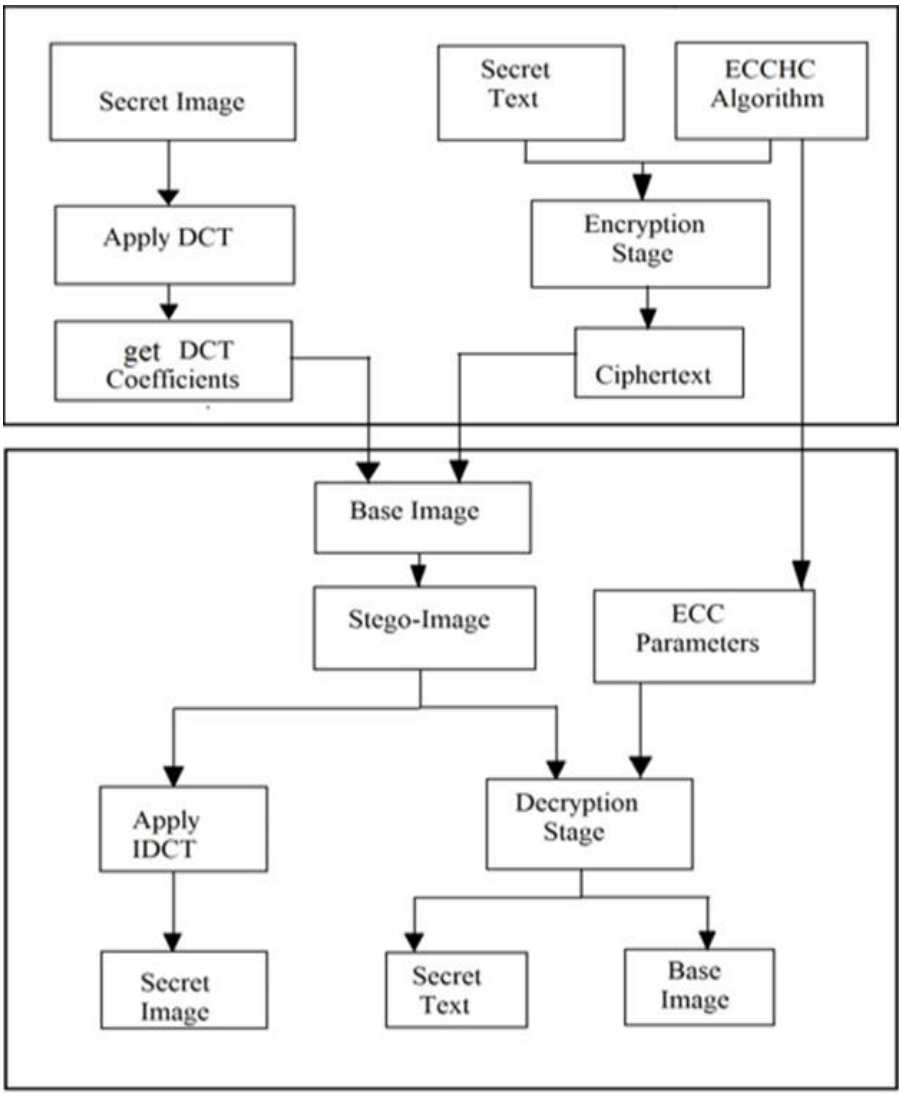

Fig 1 Block Diagram to Proposed Method

ECC is an asymmetric cryptographic technique that is entirely based on elliptic curve arithmetic. We employ ECC over finite fields for cryptography. The primary benefits of ECC are lower computation power and quicker and shorter key generation. The security of a 160 bit ECC encryption key is the same as that of a 1024 bit RSA encryption key. Steps involved in the ECC are:

A. Key Generation

The first and most critical step is the production of public and private keys. Because ECC is an asymmetric algorithm, the message is encrypted by the sender using the receiver's public key, and the message is decrypted by the receiver using its private key. The random numbers 'a' and 'b' are chosen to represent the sender and recipient private keys. The following equation is used to produce the public key.

$$P_A = a * O$$

$$P_B = b * O$$

Here 'O' is the point agreed by sender and receiver on the curve and 'a','b' are the private keys of the sender (User A) and receiver (User B) respectively and the P_A, P_B are the public keys of sender and receiver respectively.

The user will multiply their private key with other users public key to initially get key K.

$$K = a * P_B = (x, y)$$

Then computes.

$$K_1 = x * O = (K_{11}, K_{12})$$

$$K_2 = y * O = (K_{21}, K_{22})$$

Now the key matrix K used for Hill cipher algorithm is

$$K = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$$

The text is decrypted using the inverse matrix of this key matrix, however it might not always be present. The text could not then be decrypted by the recipient. Therefore, the idea of a self-invertible matrix, or K = K-1, which is the key matrix itself is the inverse of the matrix, is employed to overcome this problem. Therefore, during the decryption phase, there is no need to compute the inverse matrix.

Self-invertible matrix K_m is

$$K_m = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$$

Here K_{11}, K_{12}, K_{21}, K_{22} are 2 X 2 matrices of K_m. where

$$K_{11} = K$$

$$K_{12} = (\ I - K_{11})\ N \bmod 127$$

$$K_{21} = 1/N\ (I + K_{11}) \bmod 127$$

$$K_{22} = -\ K_{11} \bmod 127$$

In above 'I' is the identity matrix and 'N' is any random number then the self-invertible matrix is as follows

$$K_m = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}$$

B. Encryption

Let M represent the message that has to be encrypted. The message's ASCII values are divided into blocks of size 4, and each block is multiplied by the self-invertible key matrix.

To obtain the ciphered values, use modulo 127. To obtain the ciphered text, these ciphered values are then mapped to the appropriate character. Consider a image that needs to be encrypted, and then apply DCT to the image. Accept DCT coefficient values and normalize them to fall between 0 and 255. The 16-bit format is chosen since these values are floating-point numbers.

C. Decryption

The LSB technique extracts the DCT coefficients and the ciphertext from the stego image. The receiver can create the self-invertible key by employing the ECCHC decryption technique with the correct sender private key. The original text may be obtained by multiplying the four-blocks-long ciphertext with this matrix. By applying Inverse Discrete Cosine Transform (IDCT) to the obtained DCT coefficients, the hidden image may be recovered. Using the LSB-based method, the original base image may be recovered by calculating XOR values between the original image and the stego image.

D. Embedding Process

Both Cryptography and steganography are two main stages of the embedding process.

➢ *Cryptography Steps:*

- *First step is Key generation which is responsible to perform User Authentication.*
- *The Steps involved for key generation are*

- ✓ Sender and receiver agrees on a point 'O' on the elliptic curve.
- ✓ Private key and public key are generated for sender.
- ✓ Private key and public key are generated for receiver.
- ✓ Secret key is generated for sender and receiver based on the condition that both sender and receiver must know the private each other.

- *Using Hill cipher, the text which is the secret message is encrypted with the key generated using the ECC algorithm.*
- *DCT is performed to the secret image which is to be encrypted and these DCT coefficients are embedded.*

➢ *Steganography Steps:*

- *The encrypted data is embedded into the base image using the LSB method.*
- *The LSB of an image's pixel value and the secret data to be concealed are combined using the XOR method. The outcome is stored in the base image's least significant bit.*

Since the total shift is negligible, the human visual system is unable to detect the modification in the original image. This approach is strongly advised because to its simplicity and little image quality reduction.

E. Extracting Process

- *The receiver receives the stego image.*
- *The secret key is created from the sender's private key if the one receiving has been verified using the ECC parameters (D1 and D2).*
- *Multiplying the secret key with encrypted ciphertext will reveal the hidden message.*
- *The extracted DCT coefficients allow for retrieval of hidden image.*

F. Advantages of Proposed Method

- *Using both methods in succession improves data privacy, ownership, and security.*
- *ECC use lowers overall processing overhead.*
- *The security against assaults are increased when ECC and Hill cipher method are used together.*

IV. RESULTS

The first step in this mechanism is that both the sender and receiver must know their private keys. The private key should be lesser than the agreed point on the curve by both sender and receiver. Generation of private and public key for both sender and receiver are illustrated in Fig.2. Using private key and the point agreed, the public key is generated.

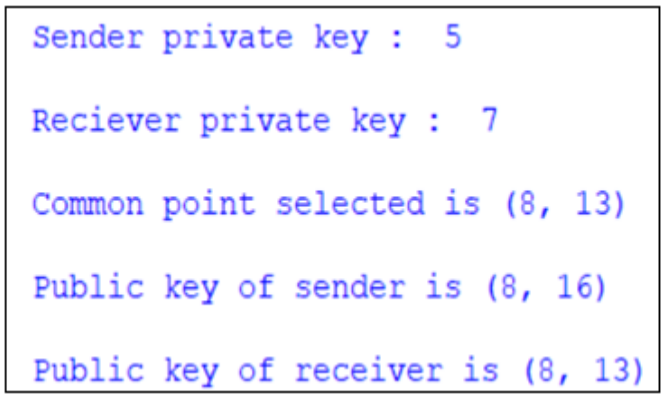

Fig 2 Generation of Private and Public Key for Sender and Receiver

The creation of the secret key, as depicted in Fig. 3, is the step that follows. Using the private key of user1 and the public key of user2, the secret key of user1 is formed, and the secret key of user2 is produced using the private key of user2 and the public key of user1. If both the sender's and the receiver's private keys are known to one another, two users are verified to transmit the message. This figure also shows the self-invertible matrix generated using mathematical equations discussed in key generation concept.

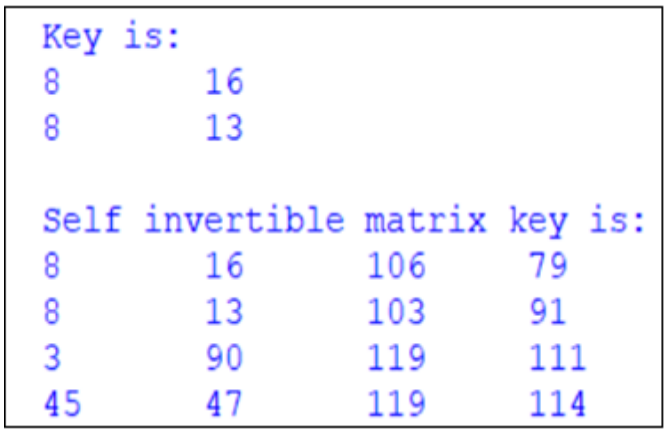

Fig 3 Secret Key and Self-Invertible Matrix Generation

Figure 4 depicts the encryption of the provided text 'Shyam Kumar Kurapati @123$' to ciphertext using an ECC-generated key and the Hill Cipher cryptography technique.

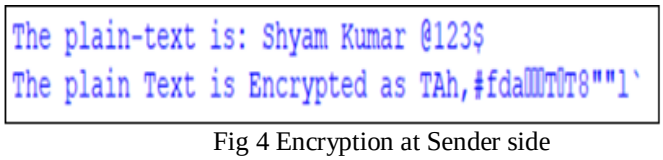

Fig 4 Encryption at Sender side

- *Fig5 is Secret Image that Needs to be Hidden in the base Image*

Fig 5: Secret Image

In Fig 6 shows secret image DCT coefficients. These DCT coefficients and text encrypted are embedded using LSB approach into base image.

./data/Nature.png
[[[14.708, -3.972, 0.141, -0.499], [14.866, -3.873, 0.151, -0.512], [14.647, -3.976, 0.173, -0.509], [14.533, -4.041, 0.163, -0.518], [14.58, -4.016, 0.165, -0.514], [14.655, -4.013, 0.127, -0.492], [14.625, -4.024, 0.129, -0.502], [14.597, -4.023, 0.145, -0.511], [14.575, -4.044, 0.141, -0.498], [14.53, -4.06, 0.145, -0.508], [14.58, -4.041, 0.137, -0.503], [14.6, -4.034, 0.135, -0.5], [14.605, -4.038, 0.131, -0.49], [14.63, -4.023, 0.133, -0.49], [14.63, -4.034, 0.122, -0.485], [14.572, -4.058, 0.131, -0.486], [14.586, -4.046, 0.133, -0.493], [14.572, -4.051, 0.131, -0.502], [14.608, -4.033, 0.133, -0.494], [14.647, -4.018, 0.129, -0.488], [14.644, -4.024, 0.124, -0.487], [14.724, -3.999, 0.102, -0.483], [14.713, -4.006, 0.098, -0.489], [14.677, -4.01, 0.116, -0.493], [14.752, -3.984, 0.106, -0.477], [14.733, -3.986, 0.116, -0.478], [14.697, -4.0, 0.114, -0.495], [14.638, -4.024, 0.127, -0.487], [14.492, -4.069, 0.161, -0.509], [14.48, -4.069, 0.169, -0.509], [14.508, -4.051, 0.169, -0.516], [14.442, -4.081, 0.176, -0.517], [14.331, -4.118, 0.196, -0.535], [14.397, -4.098, 0.18, -0.527], [14.436, -4.088, 0.173, -0.514], [14.444, -4.085, 0.167, -0.522], [14.442, -4.085, 0.173, -0.515], [14.472, -4.07, 0.171, -0.515], [14.442, -4.086, 0.169, -0.519], [14.3, -4.125, 0.214, -0.526], [14.192, -4.161, 0.231, -0.547], [14.106, -4.195, 0.245, -0.552], [14.015, -4.234, 0.251, -0.568], [13.929, -4.268, 0.265, -0.573], [13.784, -4.323, 0.288, -0.584], [13.696, -4.356, 0.304, -0.592], [13.676, -4.365, 0.314, -0.577], [13.618, -4.388, 0.32, -0.587], [13.477, -4.448, 0.333, -0.603], [13.324, -4.509, 0.355, -0.613], [13.493, -4.424, 0.345, -0.617], [13.507, -4.415, 0.355, -0.601], [13.479, -4.439, 0.339, -0.608], [13.51, -4.434, 0.329, -0.6], [13.582, -4.398, 0.322, -0.606], [13.657, -4.362, 0.316, -0.606], [13.629, -4.382, 0.312, -0.602], [13.535, -4.43, 0.32, -0.595], [13.49, -4.452, 0.32, -0.599], [13.593, -4.399, 0.318, -0.597], [13.61, -4.385, 0.325, -0.595], [13.582, -4.408, 0.314, -0.598], [13.665, -4.375, 0.302, -0.59], [13.693, -4.372, 0.29, -0.583], [13.771, -4.338, 0.278, -0.584], [13.826, -4.32, 0.271, -0.571], [13.94, -4.27, 0.257, -0.568], [14.103, -4.207, 0.231, -0.554], [14.206, -4.162, 0.229, -0.532], [14.189, -4.184, 0.206, -0.544], [14.248, -4.163, 0.2, -0.53], [14.381, -4.099, 0.188, -0.53], [14.439, -4.086, 0.175, -0.513], [14.486, -4.071, 0.161, -0.513], [14.503, -4.063, 0.157, -0.516], [14.575, -4.04, 0.145, -0.5], [14.611, -4.026, 0.143, -0.491], [14.602, -4.037, 0.133, -0.493], [14.6, -4.038, 0.135, -0.49], [14.627, -4.027, 0.127, -0.495], [14.616, -4.037, 0.12, -0.499], [14.589, -

Fig 6 DCT Coefficients of Nature Image (Secret Image)

Fig 7 Base Image

- *The base Image is Shown in Fig.7 and the Embedded Image is shown in Fig.8.*

Fig 8: Embedded Image
(Data and Image Coefficients are Encrypted into this Image)

At decryption side, with the help of receiver's private key and using LSB approach encrypted data is retrieved. The decrypted text is shown in Fig 9.

```
enter common point to start decryption:8
enter reciever private key to start decryption:7
The encrypted text obtained from embedded image is : TAh,#fdaÌÌñÛT8""1`
Decrypted text: Shyam Kumar @123$
Recovered image: ./output/Nature.png
```

Fig 9: Decrypted Text from Embedded Image

- *The Secret Image is Saved as Nature.png and it is shown in Fig10.*

Fig 10: Reconstructed Secret Image using IDCT
(Inverse Discrete Cosine Transform)

V. CONCLUSIONS

The secret data to be sent (text and picture) is encrypted, and the crypto data is embedded in the base image. On the receiver side, after decryption , secret data which is encrypted is extracted from the stego image. Text encryption was accomplished employing a combination of elliptic curve cryptography algorithm and the Hill cipher,

which reduced computing cost. The hidden picture is subjected to DCT, and these DCT coefficients were included in the base image. The encrypted message and coefficients of DCT for secret image were embedded in the picture using the LSB technique. Data privacy and ownership have been improved by combining the properties of cryptography with steganography.

REFERENCES

[1]. S. Xiang and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group", IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 11, pp. 3099-3110, Nov. 2018.

[2]. X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," 2016 in IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, 2016, pp. 1-4.

[3]. T. Wang, "Digital image watermarking using Dual-scrambling and singular value decomposition," 2017 in IEEE International Conference on Computational Science and Engineering (CSE) Guangzhou, 2017, pp. 724-727. doi: 10.1109/CSE-EUC.2017.141.

[4]. A. K. Jain and U. Uludag, "Hiding biometric data," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494- 1498, Nov. 2003. doi: 10.1109/TPAMI.2003.1240122.

[5]. A. Vashistha and A. M. Joshi, "Fingerprint based biometric watermarking architecture using integer DCT", 2016 in IEEE Region 10 Conference (TENCON), Singapore, 2016,pp.2818-2821.doi: 10.1109/TENCON.2016.7848556.

[6]. Y M. Elhoseny, G. Ram´ırez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, ´ A. N and A. Farouk, "Secure Medical Data Transmission Model for IoT Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596- 20608, 2018.

[7]. S. Lahiri, P. Paul, S. Banerjee, S. Mitra, A. Mukhopadhyay and M. Gangopadhyaya, "Image steganography on coloured images using edge based Data Hiding in DCT domain," 2016 in IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-8.