Journal of Scientific & Industrial Research
Vol. 82, May 2023, pp. 546-551
DOI: 10.56042/jsir.v82i05.1090

A Smart Strategy for Data Hiding using Cryptography and Steganography

Tumma Srinivasarao[1]*, Adilakshmi Yannam[1], Baburao Markapudi[1], Kavitha Chaduvula[2] & Apparna Allada[1]
[1]CSE Dept, [2]IT Dept Seshdri Rao Gudlavalleru Engineering College, Gudlavalleru 521 356, Andhra Pradesh, India

Received 29 August 2022; revised 03 October 2022; accepted 07 October 2022

Confidential data maintained by Security sources has always been a substantial aspect of hampering unintended access. Technology is enhancing day by day towards information, especially in terms of multimedia file transmission. Combining cryptography and steganography, a crossover approach serves information security. Cryptography is a strategy for changing over from plain content Cipher Text. Steganography is the specialty of concealing plain text, which refers to hiding data within a message or file. The proposed method provides a hybrid system in designing and utilizing cryptography and steganography techniques, making the communication system reliable in resisting attacks. In this paper, the play fair cipher method is used to encode the hidden textual content, which provides security in terms of effective level. Play fair cipher represents the plain text as a data unit and converts these units into unknown forms. Later, Discrete Cosine Transform (DCT) and Logical Operation Exclusive OR (XOR) techniques were combined with masking encrypted messages inside the picture. Noble security level results and histogram analysis are the achievements' values that indicate the offers designed by a system.

Keywords: DCT, Histogram, Play fair cipher, PSNR, XOR

Introduction

The two techniques, Cryptography and Steganography, are commonly used for ensuring the classification, uprightness, and accessibility of data. Combining the modes of cryptography and steganography provides a strong, secure communication system for the mutual sharing of information over an insecure channel. Cryptography is the technique of maintaining the confidentiality of a message alone. It will protect confidential information by coding it into an indecipherable associate format. It is a mechanism for protecting and exchanging using secret codes. Cryptography defines secure communication within sight of vindictive outsiders known as enemies. Encryption performs computation and a secret key to change a contribution to ciphertext. A given mathematical assessment will convert the plaintext into ciphertext if a similar secret key is used.

Motivation: Cryptography assessments are always secured if an attacker can't finalize any plaintext or secret key features. These calculations are of two sorts symmetric key and asymmetric key. Symmetric key cryptography is a sort of –encryption where just one key, i.e, a secret key, is used to encode and decipher electronic data. This encryption method contrasts with asymmetric key cryptography, where two or three public and private keys are used to encode and disentangle messages. *Steganography* is a text-type file with hidden text where we can hide this text behind any image. Steganography is considering many alternative techniques, and XOR is the most widely used, giving maximum security.

Related works

An LSB strategy conceals data in the cover picture considering the pixel estimation of the shading or dark degree of each pixel.[1] This proposed method has a high payload and low detectable quality of secret data embedded in the cover picture when contrasted with the current Least Significant Bit (LSB) based calculations.[1] Similarly, an exchange-based encryption method has been verified for effective encryption. The technique suggests reallocating pixel esteems to different areas, utilizing a relative change procedure with four eight-digit keys.[2]

As per a consistent review of digital communication, enhancements in the research of steganography play an abnormal function in society.[3] For this explanation, it is significant that advanced steganography innovation and its suggestions take the lead in security aspects. Steganography and Steganalysis were treated equally in ethical concerns.

*Author for Correspondence
E-mail: srinivas123fast@gmail.com

A DNA ASCII table is suggested instead of a lookup table, and the secret key is produced in random order.[4]

Further, the quantum key distribution with amazing qubits probably would be reachable over significant distances when different defects are considered. Besides, existing test conspires at present don't offer genuine high-end security for the revealed locations concerning distances.[5]

'Catch the Curve' White Paper Series provides long-lasting battery worked gadgets that produce less warmth programming applications that run quicker and take less memory.[6] A K Means Clustering based on the data hiding estimation (KM-DH) approach outperforms bunch movement i.e., split pixels into pieces from starting at now scrambled picture. Viable split pixels discover a spot to dispense data. Authenticated individuals encode the picture pixels with their secret key to get the envelope picture. This stream passes by collecting the pixels to stuff the all-around scrambled picture of the last pieces to create a spot to distribute information utilizing K means Clustering techniques.[7] Three efficient techniques of steganography are utilized for concealing private messages. These three strategies are LSB-based steganography.[8] A Steganography-based RGB picture relies upon hereditary calculation (GA) to produce an irregular key that speaks to the best requesting of mystery (picture/text) squares to show away in the cover front image.[(9,10)] Inpicture Steganography, it is also possible to contrast specific components with the choice of pixels and deal through computerized watermarking in the domains of spatial frequency.[11–14]

Proposed System

Overview

This paper provides a solid association between source and objective over an unstable channel. This strategy gives two stages to concealing a secured message. The first is changing from plain content to encoding text using a valid play code. Sometimes, sending a scrambled message causes an impression, whereas undetectable text won't do such. The subsequent one covers up the encoded text in a picture by utilizing the combining activity of XOR strategy and DCT method.

Play fair cipher is a valid code that is an exact replacement, where sets of letters are scrambled rather than a single letter. At first, a key table is made. The key table is a 5×5 lattice of letter sets that go about as the key for encoding the plain content. Each of the 25 letter sets must be one of a kind, and one letter of the letters in order (typically J) is discarded from the table as we need just 25 letter sets rather than 26. If the plain content contains J, I supplanted it at that point. The sender and the beneficiary choose a specific key. In a key table, the principal characters going left to directly in the table is the expression, barring the copy letters. The remainder of the table will be loaded up with the leftover letters of the letter-set in common request.

Framework

The proposed one has a specific design and layout. Method of copying secret information within the image is given in Fig. 1. Extracting hidden information from the image is given in Fig. 2.

Results and Discussion

The simulation-based experimentation involves several steps, including translating the framework

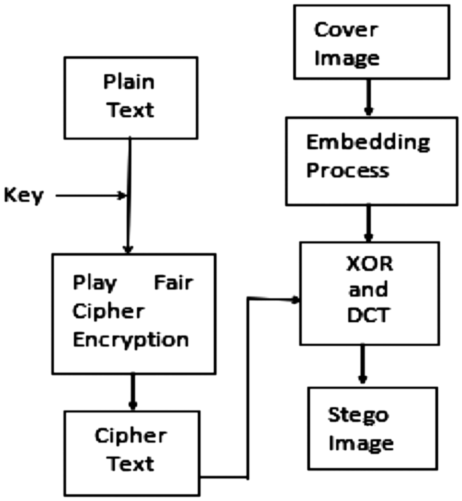

Fig. 1 — Process of hiding

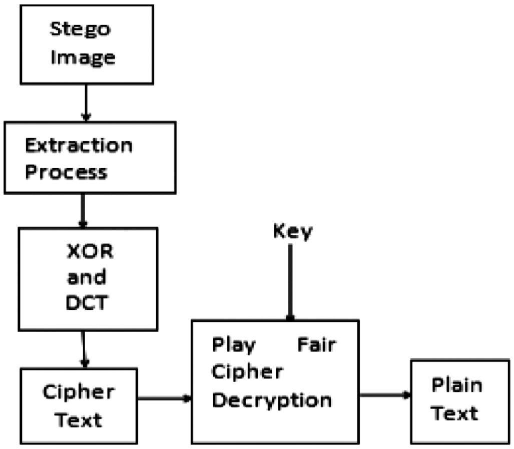

Fig. 2 — Process of extraction

presented in Fig. 1 and Fig. 2 into an algorithm. The algorithm formulation is necessary to develop the application that can take the input and provide the proposed encrypted out in terms of the images. The algorithm provides the steps for embedding and extraction as well. The typical steps are data encryption following the framework of Fig. 1 and decryption that implements Fig. 2 framework, while the last part is steganography.

Process of Embedding and Extraction

The process of embedding and extraction involves several steps presented in the form of an algorithm as follows.

Algorithm:

Input and output

Input: Confidential text in an understandable form.

Output: Confidential text in cipher.

Data Encryption

```
Step 1: Create the variable A for the Cipher Text.
Step 2: The keys chosen should be <=26 alphabets,
    If Key1>26 && Key2>26
    Error="used wrong key"
Step 3: If number of keys are < 26
    compute the number of characters of the Plaintext.
    For i=1 to length (PlainText)
Step 4: Determine the index value of the PlainText using find function.
    M=find (index==Plaintext (i))
Step 5: Compute the value of CipherText.
    A=mod (Key1*(M-1) + Key2, 26)
Step 6: The obtained CipherText value is in number form,
    convert number form to character using char function.
    cipher=char(A)
```

Data Decryption

```
Step 1: Declare variable M for Plaintext..
Step 2: Calculate the length of CipherText.
Step 3: Determine the index value of the CipherText using findfunction.
Step 4: compute the PlainText
    M=mod (Key1_inverse*(A-1) - Key2, 26)
Step 5: The obtained PlainText value is in number form,
    convert number form to character by using charfunction.
```

To hide data in images a hybrid technique of XOR and

DCT are used to improve the capacity of hiding and PSNR

Steganography on XOR (embed text content)

Input: Image.

Output: Image which hides confidential data.

```
Step 1: Scan the image.
Step 2: Change the image to the gray scale one.
Step 3: Change the image size to required size.
Step 4: Convert the message to its binary.
Step 5: Traverse every pixel of the image.
Step 6: Get message to be embedded.
Step 7: If message bit = XOR, set temp=0.
Step 8: If message bit! = XOR, set temp=1.
Step9: Update outputimage to inputimage+temp.
Step 10: Finally, mention input image also as output
```

In this proposed system, four different cover pictures were used to insert encrypted confidential information. In the beginning stage, the key is encoded and will be hidden in apicture and transmitted to the destination. On the receiver side, hidden confidential data is initially extracted and decoded. This specifies a mixed approach that combines the technique of cryptography and steganographic algorithms for developing the information's consistency and maintaining the image's robustness. This combination is tested with Mean Square Error, Peak signal to noise ratio, and histograms. If the input and output image square measures are equal, then MSE is zero. The MSE was measured using exploitation Eq. 1

$$\text{MSE} = 1/\text{n} \sum_{i=1}^{n} (Yi - yi)^2 \qquad \ldots (1)$$

Distortion within the stegono-image is measured by PSNR, which is measured in decibels (dB). In the grayscale image, if the PSNR value is greater than 35 dB, then we can't distinguish the difference between the input and output image.

$$\text{PSNR} = 10 \log_{10} (255^2 / \text{MSE}) \text{ dB} \qquad \ldots (2)$$

The dataset of cover and stegono images are presented in Fig. 3. The MSE and PSNR values can be referred from Table 1. The histogram analysis

Table 1 — Results of MSE and PSNR

COVER IMAGE	MSE	PSNR
Fabled	0.97	48.9
Lena	1.1	46.9
Office	0.73	49.4
Tiger	1.18	48.7

assesses the compatibility of the projected one. If the graph remains the same after embedding the data, then the proposed one is effective. Both Fig. 4 and Fig. 5 are the bar graphs of the input pictures before and after the embedding method.

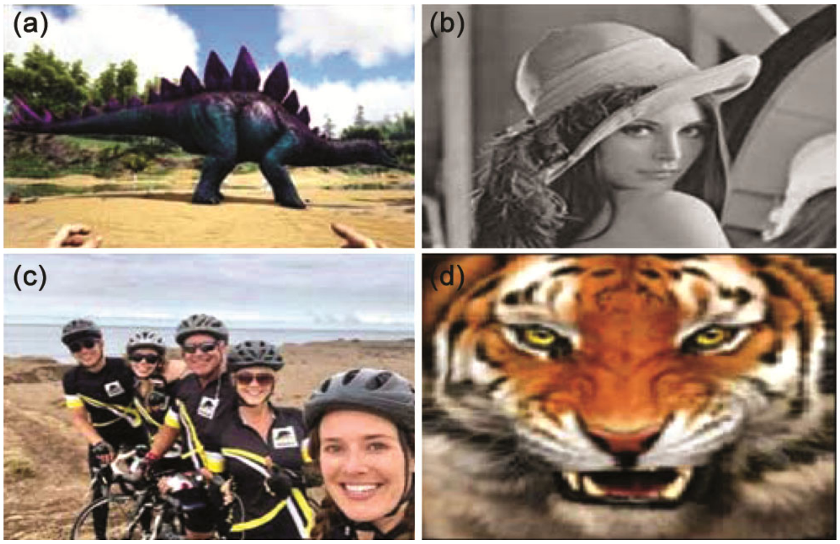

Fig. 3 — Dataset of cover and stegono images: (a) Fabled cover, (b) Lena cover (c) Office cover, and (d) Tiger cover

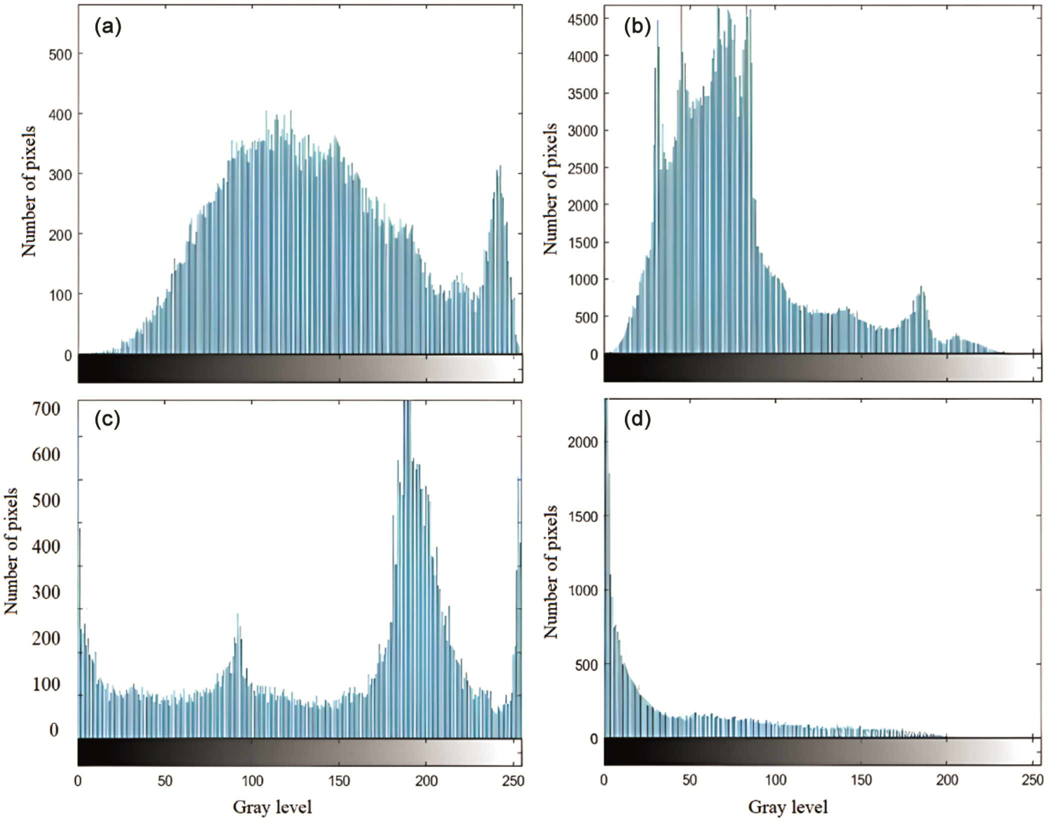

Fig. 4 — Dataset histograms of cover pictures (a) fabled, (b) Lena, (c) Office, and (d) Tiger

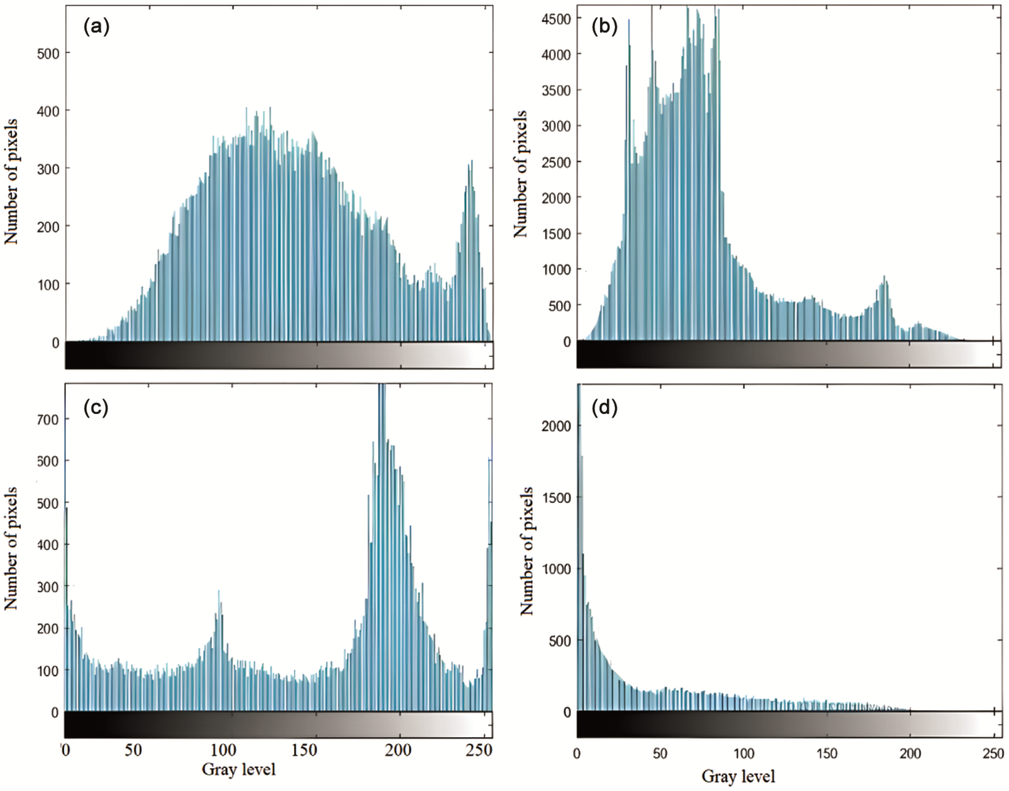

Fig. 5 — Dataset histogram images of stegono images: (a) fabled, (b) Lena, (c) Office, and (d) Tiger

Conclusions

The main contribution of this work is developing a high-end model with maximum security that uses a hybrid approach of steganography and cryptography. The technique unifies the advantages of both methods and nullifies the complexities involved in implementation. Play fair cipher is a cryptography technique that contributed to a practical encoding framework, and the technique is a symmetric encryption, which provides maximum security and agility. The proposed method is evaluated using metrics like Mean Square Error, Peak Signal to Noise Ratio, and histograms. The results show that the MSE values are low and PSNR Values are maximum. However, this emphasizes that the embedding and encryption process is recoverable only with the respective secret key. This also ensures the quality of the retrieved image when compared with the input.

References

1 Khan Z, Shah M & Naeem M, Threshold-based steganography: A novel technique for improved payload and SNR, *Int Arab J Inf Technol*, **13(4)** (2016) 380–386.

2 Nag A, Singh J P, Khan S, Ghosh S, Biswas S, Sarkar D & Sarkar P P, Image encryption using affine transform and XOR operation, *Proc* Int Conf Signal Process Commun Comput Netw Technol, 2011, DOI: 10.1109/ICSCCN.2011.6024565).

3 Artz D, Digital Steganography: Hiding data within data, *IEEE Int Comput J*, **5(3)** (2001) 75–80.

4 Kishore D R, Suneetha D & Pradeep G G S, An improved method of DNA data encryption using XOR based data segments, *Int J Rec Technol Eng*, **8(1)** (2019) 1834–1838.

5 Brassard G, Lütkenhaus N, Mor T & Sanders B C, Limitations on practical quantum cryptography, *Phys Rev Lett*, **85(6)** (2000) 1330–1333.

6 An elliptical curve cryptography (ECC) Primer, Why ECC is the next generation of public key cryptography, *The Certicom Catch the Curve White Paper Series* (2004) 1–24

7 Janani S, Shalini M, Parkavi K & Chandrasekar A, Autonomous data hiding in an encrypted image using KM-DH algorithm, *Int J Innov Technol Explo Eng*, **9(2)** (2019) 4950–4952

8 Maiti C, Baksi D, Zamider I, Gorai P & Kisku D R, Data hiding in images using some efficient steganography techniques, in *Signal Processing, Image Processing and Pattern Recognition* edited by Th Kim, H Adeli, C Ramos, B H Kang, SIP 2011, *Commun Comput Inform Sci*, **260** (Springer, Berlin, Heidelberg) (2011) 195–203, https://doi.org/10.1007/978-3-642-27183-0_21 **260**

9 Essa R J, Abdulah N A & Al-Dabbagh R D, Steganography technique using genetic algorithm, *Iraqi J Sci*, **59(3A)** (2018) 1312–1325.

10 Ramadhan j, Mstafa & Bach C, Information hiding in images using steganography techniques, *Northeast Conf American Soc Eng Edu* (Norwich University) March 2013, DOI:10.13140/RG.2.1.1350.9360

11 Abuali M S, Rashidi C B, Salih M H, Raof R A & Hussein S S, Digital image steganography in spatial domain a comprehensive review, *J Theor Appl Inf Technol*, **97(19)** (2019) 5081–5102.

12 Alturki F & Mersereau R, A novel approach for increasing security and data embedding capacity in images for data hiding applications, *Proc* Int Conf *Inf Technol Code Comput* (IEEE) 2001, DOI:10.1109/ITCC.2001.918796

13 Malladi R, Srinivas C & Gupta N, Time-slot assignment based channel access scheme for reliable transmission in VANET, in *Communication and Computing Systems* edited by B M K Prasad, K Singh, S Pandey, R O'Kennedy (CRC Press, London) 2019, https://doi.org/ 10.1201/9780429444272.

14 Abod Z A, Hybrid approach to steganography system based on quantum encryption and chaos algorithm, *J Babylon Univ Pure Appl Sci* **26(2)** (2018) 280–294.