Two-Tier Data Security Technique: LSB Image Steganography and Columnar Transposition Cipher

Article · April 2024

DOI: 10.15680/IJIRCCE.2024.1204001

2 authors, including:

Ikechukwu Onyenwe
Nnamdi Azikiwe University, Awka
49 PUBLICATIONS **164** CITATIONS

SEE PROFILE

IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

Two-Tier Data Security Technique: LSB Image Steganography and Columnar Transposition Cipher

Onyedinma, E.G[1], Onyenwe, I.E. [2]

Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria

ABSTRACT: Ensuring effective data security along communication channels is of great essence. Steganography and cryptography are two methods for protecting data from intruders while transmitting them over the network. They have proven to be effective in data security, confidentiality and integrity. However, each of these techniques has its own drawbacks. While cryptography renders transmitted data unintelligible by encrypting it, it attracts unwanted attention of attackers. Steganography on the other hand, conceals the fact that a message is being transmitted. However, if noticed, the message can be easily intercepted. Therefore, this work combines cryptographic technique and steganography to provide an enhanced data security technique. We employed a transposition cipher -Columnar Transposition cipher(CTC) and Least Significant Bit (LSB) steganographic technique in this work. Result of the work showed that while maintaining data security, no noticeable difference can be detected between the carrier file and the cover image.

KEYWORDS: Encryption, ciphertext, stego-object, cover file**.**

I. INTRODUCTION

With the emergence of the internet, connecting to persons, organizations or any computer, no matter how far apart has witnessed tremendous increase. Sensitive information like banking transactions, credit card information and confidential data can also be shared through the internet. Unfortunately, privacy and data security have been major challenges faced while transmitting data over the internet. Malicious threats, eavesdropping and other subversive activities have become common with transmitted data resulting in breach of the privacy, data integrity and security of the data being transmitted. As a result, different techniques have been adopted to secure data along the communication channel: Watermarking and fingerprinting techniques are basically used for protecting intellectual property [1]. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. Though this method keeps the data accessible, it is permanently marked [2]. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups. Basically, Steganography and cryptography are two commonly used techniques to maintain data confidentiality and integrity [3]. Cryptography provides an effective means of protecting secret data by rendering it unintelligible to unauthorized persons; however, the simple act of communicating with encrypted messages attracts attention. This can be problematic when it concerns a communication channel monitored by a third party, which can, at the slightest suspicion, destroy the communication between the two parties. Steganography, which has emerged as a powerful tool to protect and secure the transmitted data involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. It thus hides the existence of information by embedding information in undistinguished media contents that are unattractive to the attacker. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography does not change the structure of the secret message, rather it hides inside the media so that the change is not visible [4]. Cryptography on the other hand protects messages from unauthorized individuals by changing their meaning [5].

Cryptography has always had its ultimate role in protecting the confidentiality between the sender and the expected receiver. It is the art of keeping information secure by transforming it into a form that unintended recipients cannot understand. Thus, in cryptography, an original human readable message, referred to as *plaintext,* is changed by means of an *algorithm,* or series of mathematical operations, (known as encryption) into something that to an uninformed observer would consider unintelligible. This unintelligible message is called *ciphertext [6]*. To obtain the actual message by the intended receiver; the ciphertext is then decrypted using a known key. There are two techniques for

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

converting data into non-readable form: Transposition technique and Substitution technique. In substitution cipher, the plaintext is encrypted by swapping each letter or symbol in the plaintext by a different symbol as directed by the key. However, in Transposition cipher, the plaintext letters are rearranged in a different order based on the key. Thus, Transposition ciphers use the letters of the plaintext message, but they permute the order of the letters. Columnar Transposition is a cipher transposition technique that involves writing the plaintext out in rows, and then reading the ciphertext off in columns [7]. To conceal the existence of a secrete message, different forms of steganography can be adopted depending on the type of cover media used to embed the secrete data. These forms include: Text Steganography, Video Steganography, Audio Steganography, Network Steganography, E-mail Steganography and Image Steganography. Image Steganography refers to the process of hiding data within an image file. The hidden data can include text, images, audio, or any other form of binary information. The aim is to conceal information within digital images without altering their visual appearance. To achieve this concealment, the LSB, which is one of the simplest and most common techniques can be adopted. It consists of hiding a secret message in the least significant bits of the pixels of the image so that the distortions brought by the insertion process remain non-perceptible [3]. The reason is that for the human eye, variations in the value of the LSB are almost imperceptible. The insertion of secret message bits may be done sequentially or pseudo randomly.

Steganography and cryptography have been noted to be individually insufficient for complete information security [8]. One of the challenges with cryptography is that visible encrypted messages, no matter how unbreakable they are, arouse interest. This in turn will steer an attacker to devise means of decrypting or intercepting the message. One of the benefits of utilizing Steganography over Cryptography alone is that the proposed secret message does not attract attention to itself as an object of scrutiny. However, steganography techniques depend on the confidentiality of the data encoding system and once the encoding system is known, the steganography system can be known or tracked. Therefore, a more reliable and strong mechanism can be achieved by combining both techniques [8]. Combining these strategies can ensure an improved secret information security which will probably meet the requirements for security and robustness for transmitting important information over open channels [1]. Thus, the use of Steganography as an additional feature to cryptography provides a protective layer to the unintelligible message thereby further strengthening the security, robustness and confidentiality of important data transmitted over an open channel.

II. RELATED WORK

The number of reported threats to data security is continuing to increase in the past few years and is becoming a serious security challenge [3]. Current studies suggest that these threats can be nullified using cryptographic and steganographic techniques. The combination of both techniques; utilizing individual advantages of cryptography and steganography provide a more robust and stronger framework with a better security compared to the individual techniques.

Embedding the secret message in more than one cover object was proposed by [9]. Using this approach, achieving higher level of security depends on the number of cover objects used not minding the cryptographic technique used. This technique however is faced with challenge of handling many cover objects which not only requires several algorithms to be implemented but also increased overhead on resource utilization. In [10], Hash Least Significant Bit (H-LSB) with Affine cipher algorithm was proposed to provide more security to data in a networked environment. Nevertheless, Affine cipher being a monoalphabetic substitution algorithm can be cracked very easily once detected. The Blowfish cryptography algorithm was used by [11] for secret image encryption. The secret image was selected in a BMP format and encrypted using the Blowfish algorithm. Next, the encrypted image was embedded into video frames using LSB embedding method. The Blowfish provided stronger and faster performance compared to some other algorithms like RC6, RC4, DES, 3DES, and AES. However, it has a small block size, more so, the video frames adopted for the steganography could result to loss of data or degradation due to conversion and compression. In the study carried out by [12], LSB embedding technique was adopted while Advanced Encryption Standard was utilized to encrypt the secrete message. In the proposed method, before the hiding process, the sender had to select the image of size 512*512 and select the secret message as well as secret key. The Receiver then applies the decryption algorithm to get the original image and supply the same secret key to retrieve the secret message. The technique was effective for secret communication and provided better security though without compression.

In [13], they also proposed the use of cryptography and steganography for data security. For the cryptography process, they proposed the use of SCMACS (Secure Cloud Migration Architecture using Cryptography and Steganography). This technique encrypts data using one's complement method. The strength of this approach lies in the fact that the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

symmetric key method generates a dynamic value for the private Key that gets changed for each data that needs to be transferred, thus making it very safe. Nevertheless, the system was not implemented to ascertain its effectiveness.

Another research, [14] proposed a hybrid data compression algorithm to increase the input data to be encrypted by RSA (Rivest-Shamir-Adleman) cryptography method. This technique can be used to decrease the amount of every transmitted data aiding fast transmission while using slow internet or take a small space on different storage media. The plain text is compressed by the Huffman coding algorithm, and also the cover image is compressed by Discrete wavelet transform (DWT) that compacts the cover image through lossy compression in order to reduce the cover image's dimensions. For steganography, the least significant bit LSB was used. The mechanism resulted in more effective visual quality, security and storage capacity. Elliptic curve cryptography (ECC) combined with Hill cipher was proposed in [15]. In this method, ECC algorithm was used to produce a key, and this key was employed to generate ciphertext through the Hill cipher algorithm. The resulting ciphertext and DCT coefficients of an image were embedded into the base image using LSB watermarking. This combination of both steganography and cryptography results in increased authority and ownership of the data for sub-optimal media applications. Another study [16] used MD5 algorithm to encrypt the message. The input message in MD5 algorithms was processed into blocks of 512 bits, divided into 32 bits of sub-blocks of 16 pieces. The output of the MD5 algorithm was hash value of 4 blocks of 32 bits. Again, RGB shuffling was used by the authors to encrypt image in order to distort it. Thereafter, the conventional LSB technique was employed. The study produced an effective result. The one-time pad (OTP) was used to encrypt the message in the study of [17]. Here, the authors affirmed that OTP is computationally efficient both in terms of encryption and decryption. For the steganography, LSB was adopted. [18] proposed a practical public-key steganography method based on elliptic curve cryptography and a generative model for the message encryption while LSB was utilized for the steganography. The result demonstrated improved data security and efficiency. Sweeping computational ghost imaging (SCGI)-based encryption system was employed in [19]. This is intended for increased data security and speedier data transport. The LSB was used to conceal the image. This strategy also resulted in smaller, more compact data packages and higher bitrates.

III. PROPOSED WORK

Both Least Significant Bit (LSB) steganography and Columnar Transposition Cipher are adopted in this work to enhance data security, confidentiality and integrity. The plaintext will first be encrypted using columnar transposition cipher. A chosen key out of random will initiate the transposition process. After which the ciphertext is embedded in a cover image using the LSB technique.

Columnar Transposition Cipher

A transposition cipher is one in which plaintext symbols are rearranged (i.e., transposed or permuted) to produce ciphertext. The method of transposition may be either mathematical or typographical in nature. The order of plain-text letters is modified based on some selected permutation. The plain-text is divided into blocks of size b (the length of the permutation). The letters in each block are reordered based on the permutation. These blocks can be written into a matrix. Constructing the Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. Both the width of the rows and the permutation of the columns are usually defined by a keyword. Algorithm for single columnar transposition is as follows:

- Chose a key of a fixed length
- Write the plaintext row-by-row in rectangular form but with a fixed column which is equal to the chosen key.
- Re-arrange the column into alphabetical column using the key as the determinant.
- Read the message column-by-column.
- The message read becomes the ciphertext

For example, to transpose ” **Life and death are in the mouth power**” ;
Step 1: Assume the key is FAVOUR,
Step 2:

F A V O U R
L I F E A N
D D E A T H
A R E I N T
H E M O U T

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

H P O W E R

Step 3:

A F O R U V
I L E N A F
D D A H T E
R A I T N E
E H O T U M
P H W R E O

Step 4: the ciphertext becomes: ***idrepldahheaiownhttratnuefeemo***

LSB steganography

The LSB approach is an essential and widely used technique in image steganography. It involves replacing the least significant bits of the cover image with secret data in order to embed information. The altered bits are typically invisible to the human eye, making it difficult to detect the hidden message. This technique can be used for hiding images in 24-bit, 8-bit or grayscale format. Supposing we have an image with pixel values ranging from 0 to 255, the least significant bit of each pixel can be modified to hide a secret message. For instance, if the pixel value in binary: 01101100. The LSB is the right most bit which is 0 in this case. To embed a bit of 1 therefore, means changing the LSB to 1 (01101101). This slight modification is often visually indistinguishable, especially with large cover image files.

The following algorithm embeds a message in a cover image:

1. Convert the image to grayscale
2. Resize the image if needed.
3. Convert the message to its binary format
4. Initialize output image as input image
5. Traverse through each pixel of the image and perform the following:
   i. Convert the pixel value to binary
   ii. Get the next bit of the message to be embedded
   iii. Create a variable *temp_var*
   iv. If the message bit and the LSB of the pixel are same, *temp _var is set to 0*
   v. If the message bit and the LSB of the pixel are different, *temp _var is set to 1*
   vi. Update the pixel of output image as output image = i*nput image pixel value + temp_var*
6. Repeat updating until all the bits in the message are embedded
7. Finally, write the input image and the output image to a file.

Description of terms

The following terms are usually associated with cryptography:

- Plaintext -It is the original message that is being protected.
- Ciphertext - is the encoded message which is the result of transforming a plaintext using encryption.
- Key − A key is a set of mathematical values, formula or process that is used to obtain the ciphertext. It determines how a plaintext message is encrypted or decrypted.

The following terms are usually associated with steganography:

- Cover file- the file used to conceal data.
- Secrete Message - Real data that you can mask within a cover file. The message may be in the form of standard text, audio, video or image.
- Stego-object − an object with a hidden message.
- Stego-Key - Messages can be embedded in cover files with the use of a key. This key known to only the sender and receiver controls the hiding process by ensuring non detection and /or recovery of the embedded data.

As observed in Fig 1; the plaintext (secrete message) is encrypted using an encryption algorithm (Columnar transposition) to generate a ciphertext. Both the cover file (X) and ciphertext (M) to be hidden are fed into a steganographic encoder as input. Steganographic Encoder function, f(X, M, K) embeds the secret message(ciphertext) into a cover file using the Least significant bit encoding. The resulting stego object has similar features with the cover file with no visible changes. To retrieve the ciphertext, the stego object is then fed into Steganographic Decoder. The resultant ciphertext is now decrypted using the decryption key. The programming language used is python.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

The proposed technique is depicted in Fig 1.

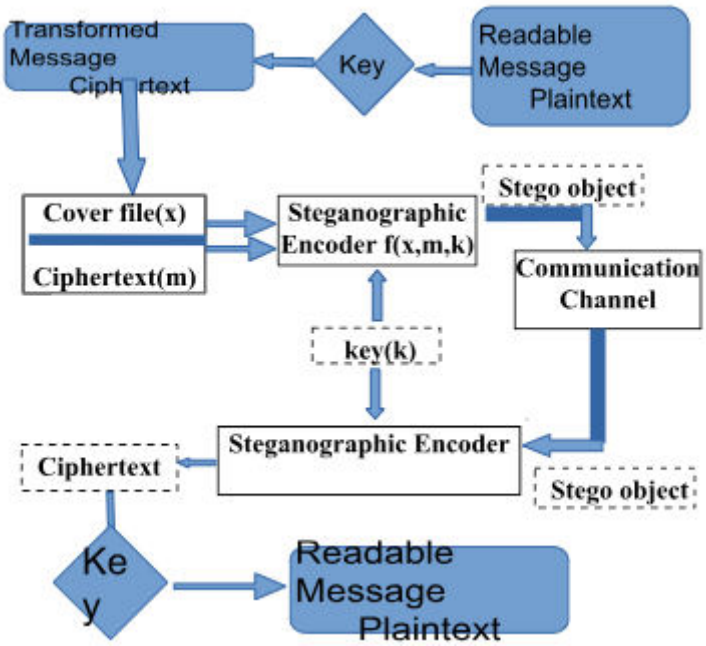

Fig. 1: Architecture of the Proposed combination of CTC and LSB

IV. RESULTS AND DISCUSSION

Three different images of different sizes and formats were used for the evaluation. Fig2a-2l are the results obtained with the cover images and stego images. Fig 2a, 2e and 2i are cover the images. Fig2c, 2g and 2k are the stego images (they contain the encrypted message to be transmitted to the recipient). Fig2b, 2d, 2f, 2h, 2j, and 2l are the corresponding histograms respectively.

Fig2a: Img1

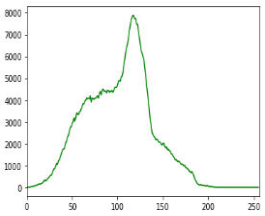

Fig2b:Img1_histogram

Fig2c:Stego1

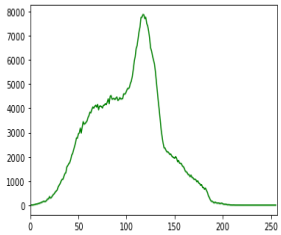

Fig2d:Stego1_histogram

Fig2e:Img2

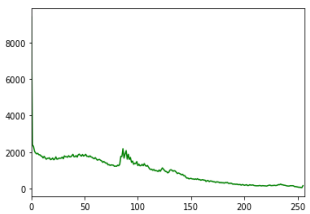

Fig2f:Img2_histogram

Fig2g: Stego2

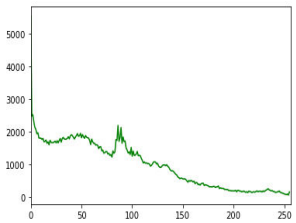

Fig2h:Stego2_histogram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

Fig2i: Img3

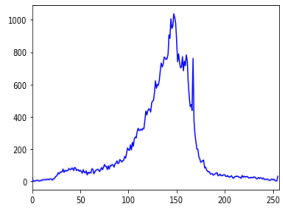

Fig2j:Img3_histogram

Fig2j:Stego3

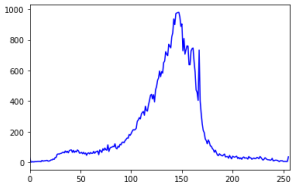

Fig2k:Stego3_histogram

Results show that there is no noticeable difference visually between the cover images and the stego images. A very closer look at the histograms will show very minute difference. Image Histogram is a graphical representation of the intensity distribution of pixel in an image. It is a graph showing the number of pixels in an image at different intensity levels of image. From the result, it is obvious that transmission of the encrypted message using the LSB steganography will not arouse suspicion.

Cover image	MSE	PSNR
Image 1	0.10381666666666667	51.71259961550959
Image 2	1.0357674932718186	31.091761395241676
Image 3	2.7819175360158965	42.16556278724216

Table 1: statistical analysis of the cover images and stego images.

Results of Table 1 show that there are also striking resemblance between the cover image and stego image. Low MSE (Mean Square Error) shows that they are similar while high MSE is an indication of strong difference. Again, high PSNR (Peak Signal to Noise Ratio) shows similarity while low PSNR shows dissimilarity.

V. CONCLUSION AND FUTURE WORK

We have been able to establish that cryptography and steganography can be combined to enhance data security. We firstly rendered the secrete message unintelligible by scrambling it using columnar Transposition cipher. This ciphertext was then embedded into a cover image to conceal the fact that a message is being transmitted. At the receiving end, the stego image is decoded with a key and the concealed message extracted. The ciphertext is then decrypted with the appropriate key to give the plaintext. The system proved effective with the evaluated parameters. To further strengthen this work, more than one transposition can be performed on the plaintext.

REFERENCES

1. Vikas T. (2012). Data Hiding in Image using least significant bit with cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4.
2. Nagham H., Abid Y., Badlishah A. Osamah A. (2012). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3):168-187
3. Mustafa T. et al (2019) Combination of Steganography and Cryptography: A short Survey. IOP Conf. Ser.: Mater. Sci. Eng. 518 052003. doi:10.1088/1757-899X/518/5/052003
4. Johnson N. and Jajodia S (1998) Exploring steganography: Seeing the unseen Computer 31.
5. Katz J, Menezes A , Van O. and Vanstone S(1996) Handbook of applied cryptography CRC press.
6. Josh F.(2022). What is cryptography? How algorithms keep information secret and safe. https://www.csoonline.com/article/569921/
7. Malay B. And Raisoni G. (2014) . Implementation of Cryptography Technique using Columnar Transposition. International Journal of Computer Applications (0975 – 8887), Second National Conference on Recent Trends in Information Security.
8. Aung P and Naing T (2014) A novel secure combination technique of steganography and cryptography International Journal of Information Technology, Modeling and Computing (IJITMC) 2 55-62.
9. Khalil C. and Hikmat F. (2011). Combining Steganography and Cryptography: New Directions. International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208. The Society of Digital Information and Wireless Communications (ISSN 2220-9085)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204001 |

10. Ako M and Roza H. (2016). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 143 – No.4.
11. Sharma M , Arya M and Goyal M (2013) Secure image hiding algorithm using cryptography and steganography IOSR Journal of Computer Engineering (IOSR-JCE).
12. Sridevi D , Vijaya P and Rao K(2013) Image steganography combined with cryptography Council for Innovative Research Peer Review Research Publishing System Journal: IJCT 9 1
13. Dhamija A and Dhaka V (2015): A novel cryptographic and steganographic approach for secure cloud data migration In Green Computing and Internet of Things (ICGCIoT).International Conference on (pp. 346-351) IEEE.
14. Wahab O., Khalaf A., Hussein A. and Hamed F. (2021). Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques,in *IEEE Access*, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
15. Gladwin S. and Lakshmi P. and Gowthami(2020). Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images. *International Conference on Artificial Intelligence and Signal Processing (AISP)*, Amaravati, India, 2020, pp. 1-5, doi: 10.1109/AISP48273.2020.9073306.
16. Rosalina, Nur Hadisukmana,(2020)." An Approach of Securing Data using Combined Cryptography and Steganography ", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.6, No.1, pp.1-9, 2020. DOI: 10.5815/ijmsc.
17. Omnia M. Mohammed E, Mohamed K, Afra A. , Khalid S(2022). Hybrid multistage framework for data manipulation by combining cryptography and steganography. Bulletin of Electrical Engineering and Informatics vol. 11, No. 1, February 2022, pp.327~335 ISSN: 2302 -9285, DOI:10.11591/eei.v11i1.3451
18. X. Zhang, K. Chen, J. Ding, Y. Yang, W. Zhang and N. Yu,(2024). "Provably Secure Public-Key Steganography Based on Elliptic Curve Cryptography," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3148-3163, 2024, doi: 10.1109/TIFS.2024.3361219.
19. Rajabi-Ghaleh S, Olyaeefar B, Kheradmand R and Ahmadi-Kandjani S (2024) Image security using steganography and cryptography with sweeping computational ghost imaging. *Front. Phys.* 12:1336485. doi: 10.3389/fphy.2024.1336485
20 David Tidmarsh (2023). Guide to Steganography: Meaning, Types, Tools, & Techniques. https://www.eccouncil.org/cybersecurity-exchange

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details