# SECURING THE ENCRYPTED COLOUR IMAGES

[1]S. Towseef Ahmed, [2]Dr.KCT.Swamy,

[3]SMD.Ansar, [4]M.Adnan Afrid , [5]A. Bharath Kumar , [6]Gummanuru Ganesh , [7]M. Ravi Chandra kumar

[1]Assistant Professor, [2]Associate Professor, [34567]UG Students

Dept. of Electronics and Communication Engineering(ECE), G.Pullaiah College of Engineering and Technology, Kurnool.

**Abstract***:* Digital image processing is used in many crucial applications. As color images are used to improve its quality and clarity it contains highly confidential data which should be protected from tampering or danger. A new approach mainly focuses on Reversible data hiding (RDH) and least significant bit (LSB) for encryption and decryption of the images. So that we get original data without any loss of pixels. In every previous technique the embedded data have caused some issues during encryption, data extraction and image restoration. The techniques which are mainly involved during the process are encryption of data and decryption of data.

A new strategy will produce better outcomes by decreasing data loss and enhancing efficiency, throughput, MSE and PSNR when comparing with the previous methods and the standard results. So that we can improve the quality of image during extraction and reduce the loss of data.

**Keywords:** *Cryptography, encryption, decryption, data extraction.*

## I. INTRODUCTION

The fact that color digital photographs are employed in so many critical and significant applications make them one of the most common and frequently used forms of digital data. These applications call for improving and eliminating noise from colored digital images, especially when they are subjected to noise of various kinds, which degrades the clarity of the digital image. Each color matrix(channel)in a digital color image can be impacted by noise, which will distort the image and make it unclear. A digital color image is made up of three 2D matrices. One matrix for each color (RGB) [1].

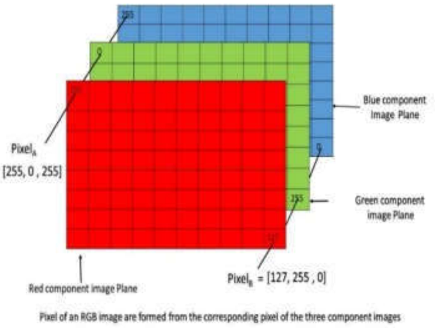

Pixel$_A$
[255, 0 , 255]
Blue component Image Plane
Green component image Plane
Red component image Plane
Pixel$_B$ = [127, 255 , 0]
255
0
255
0
255
Pixel of an RGB image are formed from the corresponding pixel of the three component images

Figure1: Colour image representation

Social networking platforms are being used to share text messages, some of which may be hidden or private, necessitating protection from the unauthorized access. These are two types of text messages: short and long, and no matter how long a secret text message is, it must have the proper security measure in place.in this studies we will use a technique that involves deducing a significant amount from a text messages ASCII symbol value [2]. Salt and pepper noise is one of the additive noise types that can arise in a picture during image capture or as a result of a bit mistake during transmission. It results in white and black blotches in the image because damaged pixels take either maximum value (255) or the minimum value (0). A median filter is used for noise reduction technique for this kind of noise. Lowering the peak signal to noise ratio between the two pictures while concurrently increasing the mean square error between the original image and the noisy image improves the quality of the color photographs [3]. Through various social media platforms, secret and private messages are extensively disseminated, necessitating the security of these messages from the risk of tampering and data thieves, as well as the pross of piercing these messages and understanding their contents. Data cryptography, data steganography, and a method known as crypto-steganography are only a few procedures used to protect sensitive communications [4]. For a number of reasons, including the fact that data is confidential or private or carries confidential information, digital data, including color digital images, requires the protection process during its communication in order to prevent intruders or unauthorized persons knowing its content. Data encryption which encrypts data using a private key, is used to carry out the data protection process [5]. Data cryptography which encrypts data before transmission and decrypts it once it has been received, can protect sensitive data from hackers. Color picture matrices can be downsized to one row matrices with a specified number of components. A secret private key (PK), which must be kept secret, can be used to secure data transmission [6]. One of the main methods for protecting and safeguarding sensitive information and preventing attempts to understand its content is cryptography. Data must be encrypted using cryptography to make it unintelligible to anyone attempting to intercept it. The encrypted data must then be recovered by using decryption, and the recovered data must watch the original data [7]. Histograms of colored images can be used as retrieval keys. In comparison to the size of the color image, the key is incredibly little.it is large in terms of the representation, though. Thus, a different approach is required to determine a shorter key length. Reshaping the 3D color matrix to a 2D grey matrix is one of the simplest ways to reduce the size of the image key(histogram). In this case, the key size is decreased from 6144 to 768(256*3 bytes). The key size will therefore be cut in half by eight times when the 3D color matrix is transformed into a 2D grey matrix [8]. A 3D matrix can be used to represent a true color image. These matrices are often very large for high resolution photos and can be readily utilized to store hidden messages or to store another image that does. In this project, we will incorporate a concealed message into a color image, which will subsequently be covered up by a larger color image using the technique of steganography [9]. A three-dimensional(3D) matrix that represents a true color picture has red as the first dimension, green as second and blue as the third. Digital color photos are among the most frequently used data formats on the internet due to the data link established between the sender and recipient via the internet. Many applications, including medical imaging systems, require specific and consistent security in data transport and storage due to the widespread use of color images by many users [10].

## II. LITERATURE REVIEW

Shivani Khosla1, Paramjeet Kaur stated that Data transmission over internet has quickly developed, making it simpler to convey data accurately and quickly to its destination. In addition, anybody may hack into systems and alter or otherwise misuse sensitive data. In this research video steganography using digital watermarking method is presented as a reliable and effective security solution. With some common criteria and principles culled from the literature, this study reviews and analyses the various digital watermarking and steganography techniques now in use.

This paper examined various embedding and security techniques. The least significant bit (LSB) is most effective method for blending a secret message or picture with cover material is spatial domain, according to an analysis of these techniques. The finest transform domain approaches for securing the secret message are DWT and DCT. DCT is frequently used in digital picture watermarking and has excellent resilience [11].

N. Askari, H.M. Heys, and C.R. Moloney An Extended Visual Cryptography Scheme With the use of pictures sent as shares, Visual cryptography generates a hidden picture that can be viewed. Since sharing photographs are designed to include relevant colour images, extended visual cryptography with biometric security techniques. Here we present a technique for halftone image processing that improves the quality of both the recovered secret picture and the sharing images in an expanded visual cryptography scheme.

In this study without going into further detail, we looked into extended visual cryptography. We have demonstrated the ability to make high quality photographs are shared employing an intelligent pre-processing of halftone photos based on the characteristics of the original hidden images scheme, and the recovered image. Be aware that alternative applications, the pre-processing method may also be useful for multiple image visual cryptography, which hides several photos in sharing [12].

Usha B.A1, N K Srinath2, N K Cauvery3 Analysis of Image Steganography is the technique of hiding information to convey it so that only the intended recipient is aware of the message’s existence. Techniques used in steganalysis aim to dispel any doubts regarding the existence of a message. A clandestine transmission of the message is impossible if suspicion is aroused. Viewing the statistical characteristics of the image or medium in which the hidden message is present is one technique to find it. In this article, we describe the nature of such attacks and give our findings based on the analysis of the current counter measures.

In this paper we have documented and outlined the present situation in the extremely fascinating subject of steganalysis here. Future research on defence against statistical attacks in steganalysis has a lot of potential given its board reach and crucial applications, The techniques utilised in the status quo are sufficiently sophisticated and can offer enough defence against recent threats. However, it is inevitable that attacks strategies will advance given the increased knowledge of steganography and the availability of the transmission medium for pictures and secret information [13].

Gurpreet Kaur, Kamaljeet Kaur states Cryptography is the process of sending data securely from one person to another without any loss of content. To do this, a message is first encrypted by the sender using computer software and a secret key, and then it is given to the recipient for decryption using the same programme and key Data integrity and data privacy the main goals of cryptography are sender authentication and non-repudiation of data accountability. In cryptography, the message is frequently garbled and incomprehensible. Communication does happen occasionally, but it is recognized or detected. Interception of message can be harmful even when the information is concealed in the cypher since it still demonstrates that the sender and recipient are in communication [14].

Sandeep Katta Recursive Information Hiding in Visual information (images, text, etc.) can be encrypted using the cryptographic technique known as visual cryptography such that when the information is decoded, a visual image is produced. This study presents a technique for secret picture information concealment using random grids. Recursively, the shares of the bigger secret are used to hide the new secret information.

In this research, we have described a technique for hidden picture information concealment using random grids. The advantage of the offered method over the recursive information concealment plan via visual cryptography is that it generates shares of a secret picture size that are the same as its original size without any expansion. The suggested method serves as a stenographic channel for embedding secret information that might be used for authentication and can be used for safe distribution information storage [15].

## III. METHODOLOGY

### 3.1 Existing method:

The current system utilizes a substantial amount of memory, CPU time, and processing time. This article primarily discusses how the Data Encryption standard was developed using the MATLAB programming language. DES is one of the symmetric encryption techniques mostly used in the image cryptography techniques. The main of which are encryption and decryption using Binary codes. The existing system has been proposed several histograms based reversible hiding schemes. Image stenography is a method of hiding images in other images so that they can send data securely over the internet. While applying this method to the videos loss of information takes place. i.e., loss of pixel information. As it cannot recover the actual picture without any loss and the visual clarity of the image will be low. It cannot extract the original embedded bits so it is not effective.

### 3.2 Proposed Method:

In this proposed method, by employing a secret public cryptosystem and the RDH and LSB algorithm to reserve space prior to encryption. The suggested technique makes easy for the user to embed data for the encrypted picture. This allows for data extraction and picture recovery without any data loss because the image is reversible. The RDH and LSB algorithm have been mined because they can recover the original picture from the marked image without any loss of data. By using RDH technique the image can be embedded more than 10 times as large of a content. Using the companding approach, more detail bits are inserted into the detail sub bands and the size of the message bits for the cover image should also include the location map, the companding error, the threshold, and the compressed location map the side information restoration of the original coefficients.

With this method, the original cover picture may be restored without any loss of information content. It is very effective that it can extract the embedded bits and the embedded data rate is very high so that the visual quality of the images is pretty good.

### 3.3 Module Description:

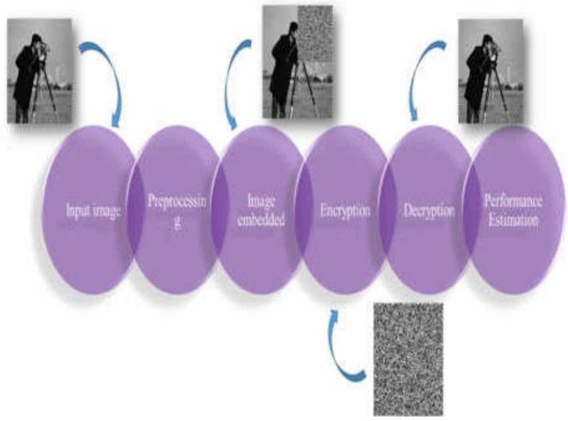


Figure 2: System architecture

#### 3.3.1 Input Image:

A rectangular array of numbers makes up a picture(pixels). Each pixel is a measurement of a different aspect of a scene over a limited region. There are several ways to measure the characteristics, but often we either measure the average brightness of the image after applying red, green, and blue. An eight-bit integer is often used to represent he values, providing a brightness range of 256 levels. We can take the image using “imread” command. Through “imshow” we can display the image. The “imtool” command launches the image viewer application, which offers a unified environment for viewing pictures and carrying out certain typical image processing operations.

#### 3.3.2 Pre-processing:

The term pre-processing describes operations on images at the most fundamental abstraction level. These operations lessen rather than increase the information content of the picture if entropy is a measure of information. By minimizing undesirable distortions or boosting particular visual features that are crucial for later processing and analysis activities, pre-processing seeks to enhance picture data. Despite geometric adjustments to the photographs, it seeks to improve the picture data by lowering unintended distortions or boosting certain components of the image that are essential for post-processing.

### 3.3.3 Image resize:

Increasing or decreasing the size of an image is called image resizing. Raster graphics images must be scaled by creating a new picture with more or less pixels. Without data loss, When the number of pixels is reduced (scaled down), there is typically a noticeable quality reduction. So that image resizing will be done here i.e., 256 X 256.

### 3.3.4 Image Embedded:

During image embedded using the companding approach, more message bits are inserted into the detail sub bands. The cover picture should additionally include as side information the message bits, the size of the location map, the companding error, the threshold, and the compressed location map in order to resolve the original coefficients. Depending on how the embedded message and the cover picture are related, there are two categories of data embedding applications. The first category is made up of stenographic applications, where the cover image is a poly to hide the fact that communication is even happening and the content has nothing to do with it. The sender and the decoder are not interested in the contents of the cover picture.

### 3.3.5 Encryption:

Digital messages are converted into secret codes through the process of encryption to ensure their security and secrecy up until the recipient receives them. Therefore, this technique transforms a message sent by a sender such that it is shielded from all third-party applications and hackers until it reaches the recipient. The original communication is referred to as the "plaintext", While the encrypted version is referred to as the "cipher text". While encryption is used to send secret and manipulate-proof data such as payment information, emails, or personal data. Various encryption techniques based on mathematical processes are used to encrypt the data. The field of study that deals with these methods is called cryptography.

Sensitive information must be encrypted. When information is sent, it is encrypted to prevent unauthorised access. The protected data is referred to as cipher text/cypher image and the original data is referred to as plain text/image. Encryption is the process of transforming plaintext or a picture into cypher text or another image.

### 3.3.6 Decryption:

Decryption is frequently used to combat encryption. Basically, it is used for decoding the information that is added during encryption side so that we get the original information without loss of data. Data can only be decrypted by an authorized user since decryption needs a secret key or password. The system extracts the jumbles data during decryption and reorganizes it into words and visuals that both the reader and the machine can comprehend. So, by using this decryption technique we are getting the original content at the receiver's side without loss of any pixel information.

## IV. EXPERIMENTAL RESULTS :

During observation we have taken four images for calculating PSNR and MSE of the various images. For the image1 shown in below figure3 consider it as an input during pre-processing the image is resized into 256*256 size. At room reservation the image is segmented into 4parts so that each segment starts to encrypt we can see encryption process in figure 7&8. The output of the figure 8 is encrypted image.

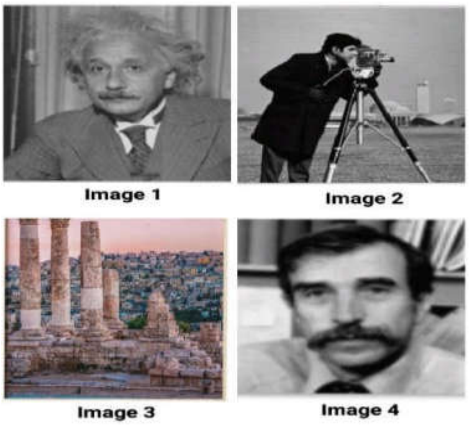


Figure 3: Used color images

During Decryption is frequently used to combat encryption. Basically, it is used for decoding the information that is added during encryption side so that we get the original information without loss of data. So that we get the original information at the output side.

### 4.1 OBSERVATION

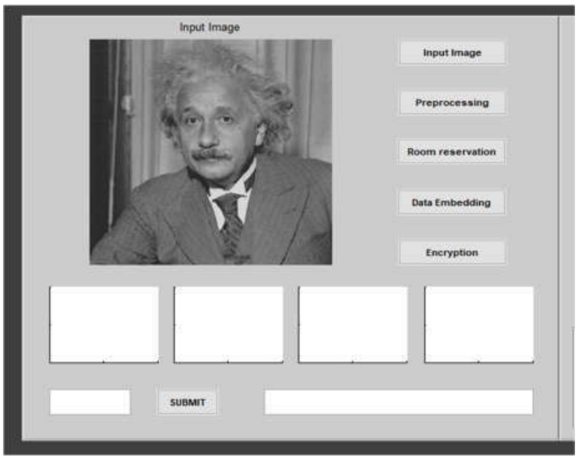


Figure 4: Input image

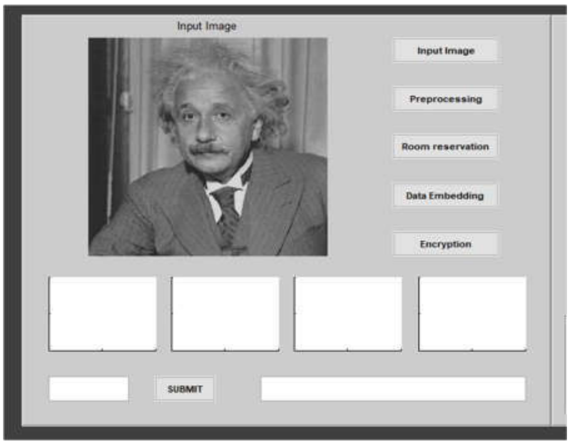


Figure 5: Pre-processed Image

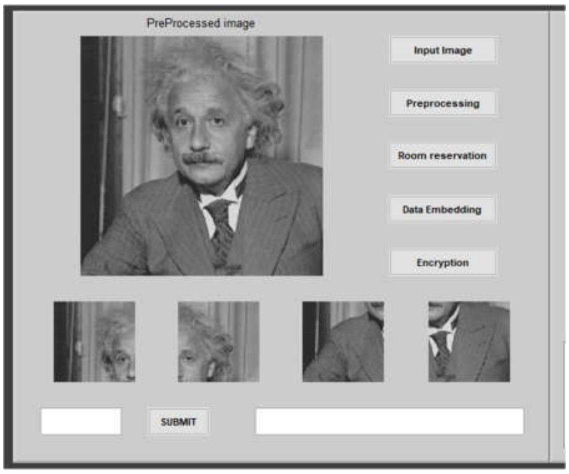


Figure 6: Room reservation

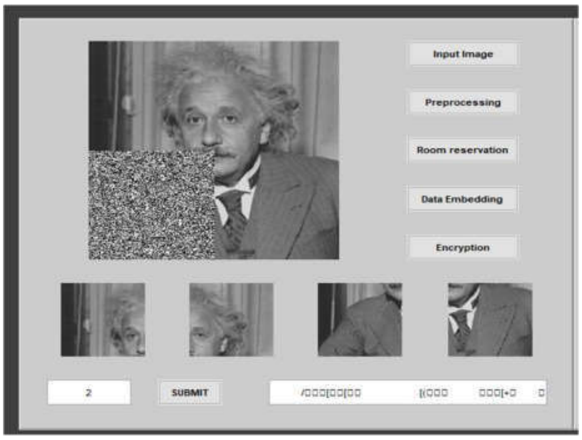


Figure 7: Data Embedding

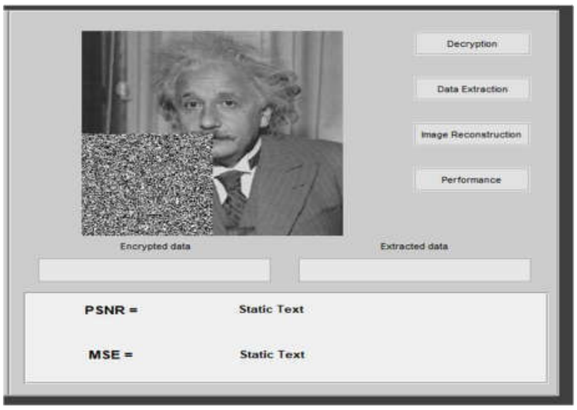


Figure 8: Encrypted image

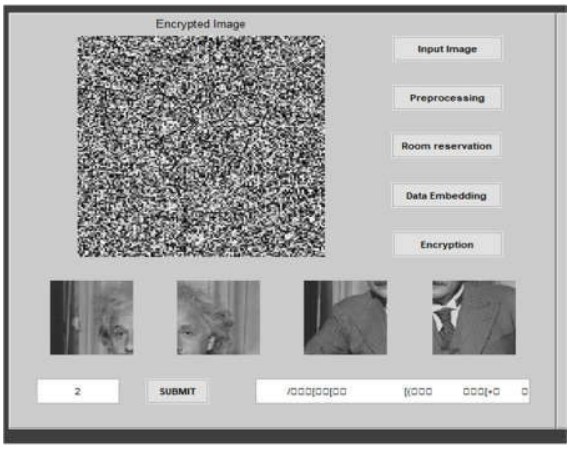


Figure 9: Encryption

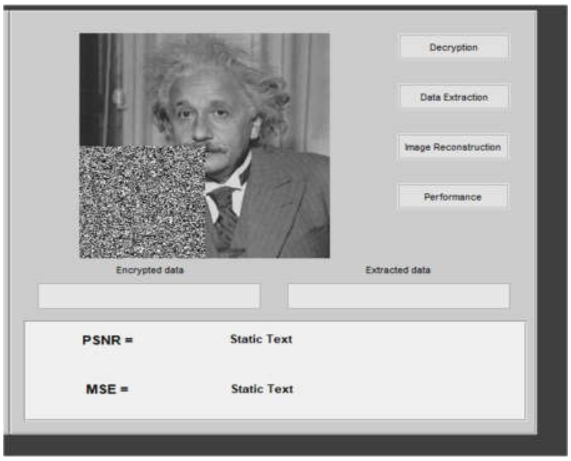
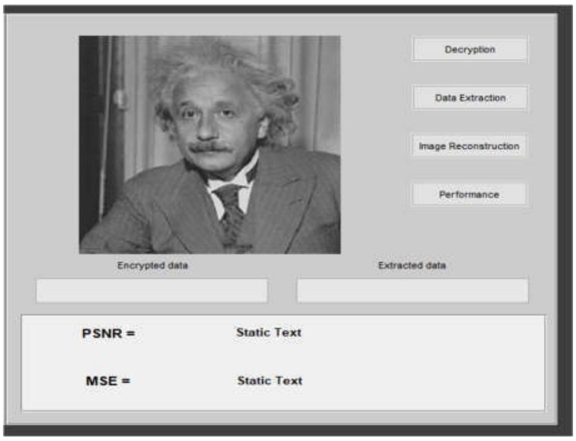


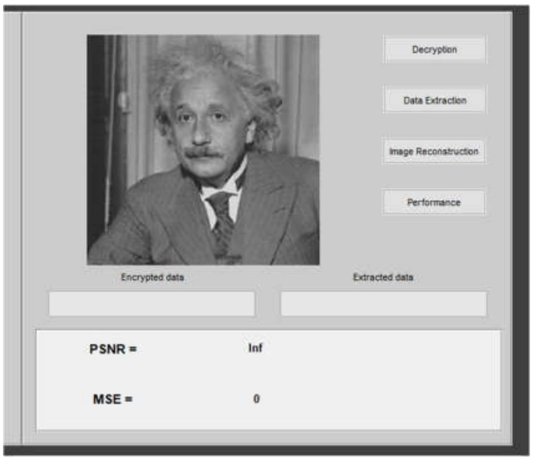
Figure 10: Decryption



PSNR = Static Text

MSE = Static Text

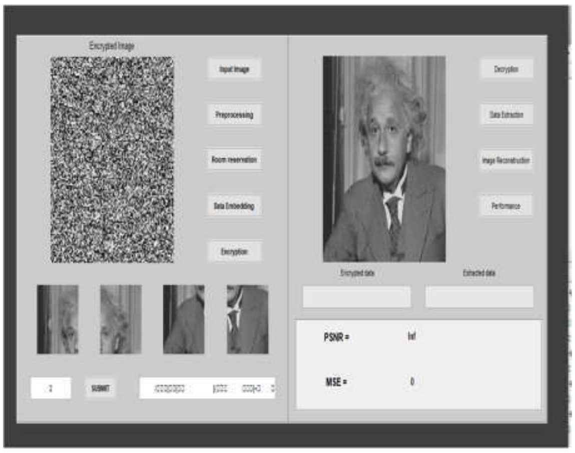
Figure 11: Data Extraction



PSNR = Inf

MSE = 0

Figure 12: Performance



2

PSNR = Inf

MSE = 0

Figure 13: Final Image

### 4.2 RESULTS

| Image number | PSNR | MSE |
|---|---|---|
| 1 | Inf | 0 |
| 2 | 96.2956 | 1.52588 |
| 3 | 77.0014 | 0.001297 |
| 4 | 72.2302 | 0. 00389099 |

Table 1: Calculating MSE and PSNR values

### V. CONCLUSION :

By using this proposed techniques, total loss of data can be recovered as possible at the time of data extraction as it takes less amount of lossless of data, reversible data hiding and least significant bit combined at embed and retrieve the data. Images encrypted by the public key cryptography so we can conclude that prevention of data attacks is reduced and data security is extended highly. This method can restore original image without any loss of data and without any error visual clarity and quality of the image will be high with this method the data will be transferred secretly with high security level.

## REFERENCES

[1] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[2] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume174, issue 8, 2017, pp:12-17.

[3] Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.

[4] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering andScience, vol. 6, issue 1, pp. 49-55, 2022.

[5] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Rounds Reduction and Blocks Controllingto Enhance the Performance of Standard Method of Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp.648-656, 2021.

[6] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 451-458, 2021.

[7] Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.

[8] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods,TELKOMNIKA, vol. 17, issue 3, 2018.

[9] Mohammed Abuzalata; Ziad Alqadi, Jamil Al- Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103

[10] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.

[11] Shivani Khosla1, Paramjeet Kaur Secure Data Hiding Technique Using Video Steganography and Watermarking - A Review (2014).

[12] N. Askari, H.M. Heys, and C.R. Moloney An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images (2013).

[13] Usha B.A1, N K Srinath2, N K Cauvery3 Analysis of Image Steganalysis Techniques to Defend Against Statistical Attacks – A Survey (2012).

[14] Gurpreet Kaur, Kamaljeet Kaur Digital Watermarking and Other Data Hiding Techniques (2013).

[15] Sandeep Katta Recursive Information Hiding in Visual cryptography (2010).