ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 9, Issue 5 , May 2022

Comparative Analysis on Image Security Techniques

Dr. Senthil Vadivu M, Syeda Saniya Kayeenath

Assistant Professor, Department of MCA, Jyoti Nivas College, Bangalore, India
PG Student, Department of MCA, Jyoti Nivas College, Bangalore, India

ABSTRACT

Over the internet, the digital images are widely communicated. On shared communication channel the security of digital images is challenging and essential work to be done. By image security we can protect an image from revision, illegal access and other attacks. These days' multimedia data has been moved to the destinations broadly through the internet into various forms such as images, video, text and audio. Over the internet, everything is visible and accessible to every user in the digital communication. Confidentiality, integrity and availability are the three goals of a network and security. Confidentiality means that information is secure and not available to the unauthorized person. Integrity refers to the accuracy of information and availability means that information is in time access to authorized person. For reliable communication of information like text, audio, video and digital images network security is not sufficient. Various techniques are used to secure the digital image, the most popular ones are encryption and decryption and Image Steganography.

KEYWORDS: Image security, Steganography, Encryption

I. INTRODUCTION

Image security plays a significant role in different fields such as government sectors, military social media, forensic studies, etc. It is necessary to make the image private and secure before it is transmitted over the network [1]. Most important aspects to be looked into are confidentiality, integrity and authentication. To check whether the above mentioned aspects are satisfied we have to perform various checks. We have to compare the original image and the obtained image and check their consistencies respectively. This research paper also embarks on the study where two techniques such as image encryption and decryption and image steganography have been studied. The outputs obtained using various performance metrics, such as pixel count and the histogram evaluation will be helpful in successfully evaluating the techniques used in this research.

II. RELATED WORK

Gopal et al, suggested an approach of image encryption using Wavelet Transform, the Chaotic Mechanism, using the Hash function to be sent to the recipient along with the production of the image fingerprint. The suggested procedure, along with anonymity, often protects the image's encryption. [1]

Neena MK proposed that digital image encryption and mosaic image transmission are two approaches to secure image transmission [2]. Yasser and others proposed novel chaotic-based multimedia encryption schemes utilizing 2D alteration models for high secure data transmission [3].

Sahu et al, proposed an exhaustive scrutiny of various ISTs from the classical to various image steganographic metrics with recent developments in the spatial domain, with respect to mark an image by adding an invisible structure known as a digital watermark to the image. Techniques of incorporating such a watermark include transform-domain algorithms, spatial- domain techniques, and sub-band filtering approaches into the digital images [4]

Trivedi [6] and others proposed that the image is transformed into frequency domain where low and high frequencies are processed in a way that guarantees a reliable, secure and unbreakable. Guodong et al, proposed a new encryption algorithm based on magic rectangle. And also asymmetric image encryption algorithm based on RSA cryptosystem and a fractional-order chaotic system [7].

Jyotika Kapoor proposed that the secret image is divided into parts. The Encrypting Phase is the first phase, which deals with using the AES algorithm to convert secret message to cipher text. Embedding Phase is the second phase, the cipher text is embedded on part of secret image that is sent. Hiding Phase is the third phase, where steganography is to be performed [10] . Gao et al , proposed a multi-image encryption scheme based on the hyper chaotic system using fractional order [11].

III. METHODOLOGY

In this research paper two image security techniques have been used. Encryption and decryption process involves taking an

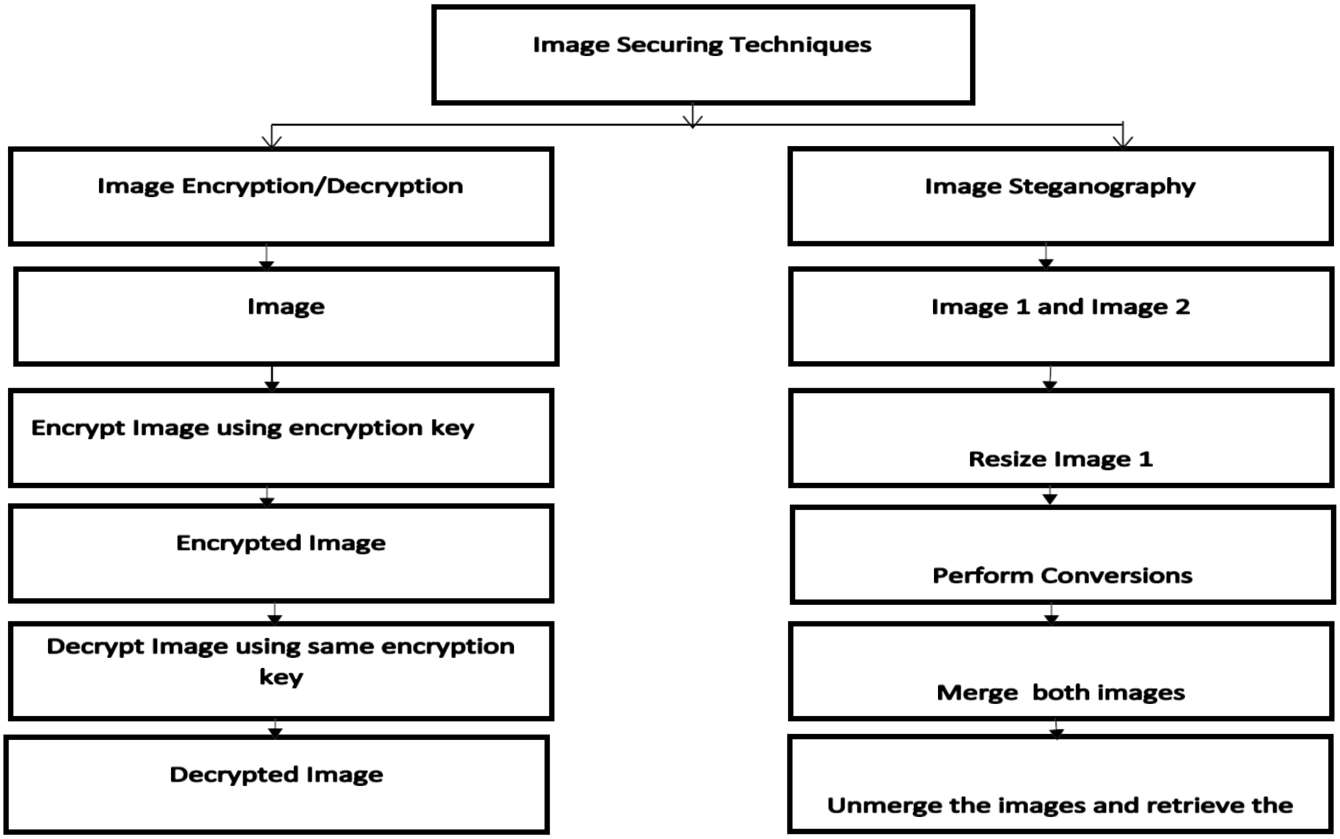


Image Securing Techniques
Image Encryption/Decryption
Image Steganography
Image
Image 1 and Image 2
Encrypt Image using encryption key
Resize Image 1
Encrypted Image
Perform Conversions
Decrypt Image using same encryption key
Merge both images
Decrypted Image
Unmerge the images and retrieve the

Fig 1: Shows the flow of entire process.

image encrypting it using asymmetric key. Once the image is encrypted it cannot be accessed unless in it decrypted using the same key. On the other hand, we make use of image steganography to hide one image inside another image to make the image more secure.

A. Image Encryption and Decryption Module: When a sender converts the original information to another form and transmits the result over the network, the process I referred as encryption. The process of encryption is also called as enciphering. When we perform the opposite task, that is the process of converting the enciphered data back to its original form the process is referred as decryption. Decryption is also called as deciphering [3].

Procedure:

Encryption: First, we will select an image, and then we will convert that image into a byte array due to which the image data will be totally converted into numeric form, and then we can easily apply the XOR operation on it. Now, the data will be changed whenever we will apply the XOR function on each value of the byte array due to which the data becomes unaccessible. But we should remember one thing that here our encryption key plays a very important role without that key we cannot decrypt our image. In order to decrypt it, it will act as a password. Hence by using a key our image is secure.

Decryption: Here the encrypted data is converted to readable form. Here in order to decrypt the image we will apply the same XOR operation. But one condition is that both encryption and decryption key should be the same.

Encryption

```
Step 1: Enter the path of image
Step 2: Enter the key for encryption of image.
Step 3: Print ‘path of file’
Step 4: Print ‘key for encryption’
Step 5: Open file for reading purpose
Step 6: Store image data in variable image
Step 7: Convert image into byte array
Step 8: Perform XOR operation on each value of byte array
Step 9: Open file for writing purpose
Step 10: Write encrypted data in image
Step 11: in case error: throw exception
```

Decryption:

```
Step 1: Take path of an image as input
Step 2: Print path of image file and decryption key that we are using
Step 3 : Open file for reading purpose
Step 4 : Store image data in variable image
Step 5: convert image into byte array to perform decryption
Step 6 : perform XOR operation on each value of byte array
Step 7 : open file for writing purpose
Step 8: write decryption data in image
Step 9: In case exception ‘throw error’
```

B. Image Steganography: The process of hiding a image within another image such that someone won’t know the contents or the presence of the hidden image is called as Image Steganography. The main purpose of Steganography is to maintain secret communication between sender and receiver. On the other hand cryptography, which conceals the contents of a secret message, steganography hides the very fact that a message is communicated [4].

Procedure:

First we will resize image1,then we will merge image 1 on image 2. After merging the images we perfom integer to binary conversion. Then we do the binary to integer conversion. Then we consider the first four digits and ignore the last four.

We then merge both the images. Hence image 1 is merged inside image 2. To get a clearer image we take MSBs from image 1 and 6 MSBs of image 2.
Step 1: Resize image1
Step 2: merge image 1 on image 2
Step 3: Integer to binary Conversion
Step 4: Binary to Integer Conversion
Step 5: Take first digits and ignore last four digits
Step 6: Merge both images
Step 7: image 1 is merged inside image 2
Step 8: take 2 MSBs from image 1 and add 6 MSBs of image2

IV. EXPERIMENTAL RESULTS

Image resolution is the procedure of calculating the number of pixels in the image. The higher the amount of pixels the higher will be the image quality.

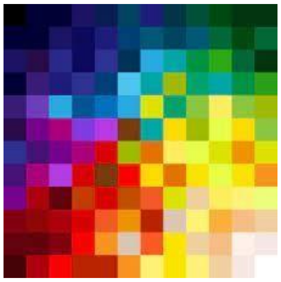


Fig 2: Image resolution

A) Histogram Evaluation

A color histogram is one which represents the distribution of colours in an image. It uses RGB values to carry out the analysis.

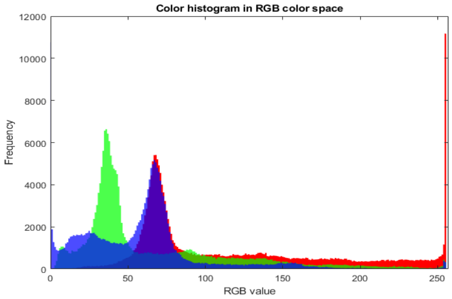


Fig 3: Histogram

Here asymmetric key is used in order to encrypt the image. The image is encrypted using the XOR function. We decrypt the image using the same key that is used for encryption. For image steganography, two images, one image that is hidden and another image that acts as a cover image in order to hide the first image. In this process we merge one image inside the other.

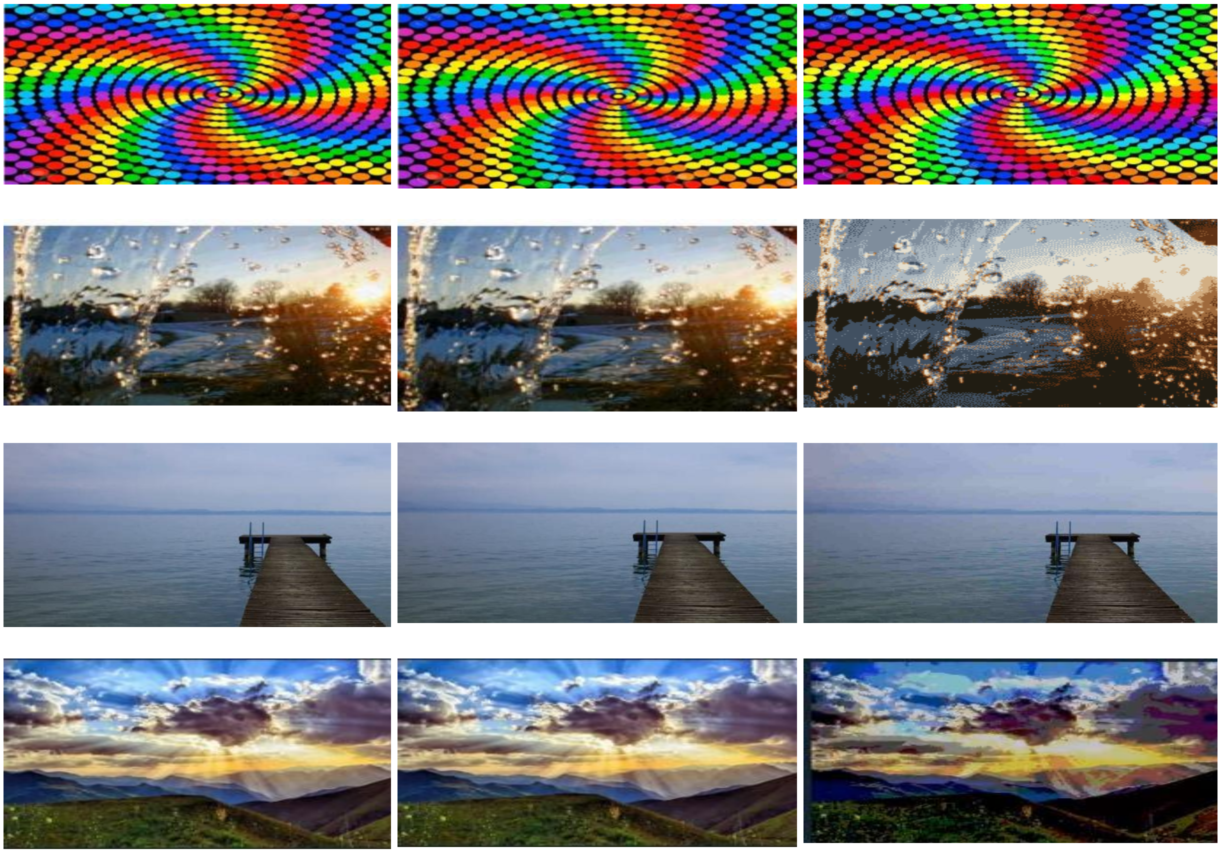


Fig 4: (a) Original image, (b) Image after decryption, (c) Image after steganography

V. PERFORMANCE EVALUATION

In order to check whether the original images and the retrieved images maintain data integrity two metrics that is pixel count to check the image resolution and histogram analysis to check the RGB values are used.

Pixel Count:

Table 1: This table shows the pixel count of different images to which image security techniques are applied.

Images	Original Resolution	After Decryption	After Steganography
Image 1	1300pixels x 1300pixels	1300pixels x 1300pixels	1280pixels x 1280pixels
Image 2	300pixels x 225pixels	300pixels x 225pixels	256pixels x 183 pixels
Image 3	800pixels x 400pixels	800pixels x 400pixels	716 pixels x 332 pixels
Image 4	300 pixels x 200 pixels	300 pixels x 200 pixels	283 pixels x 147 pixels

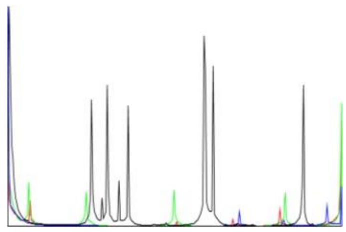
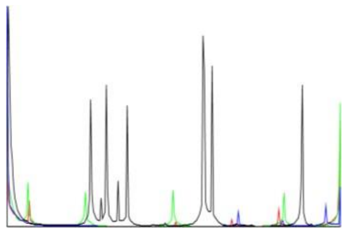
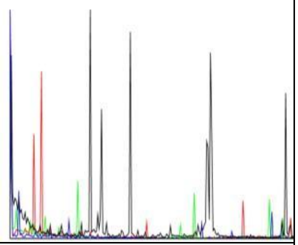
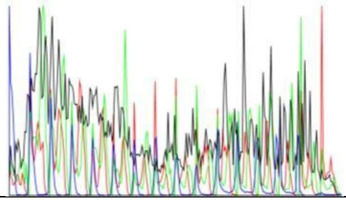
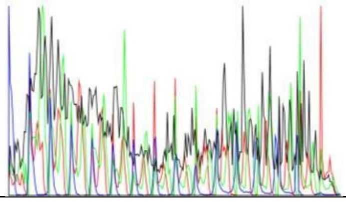
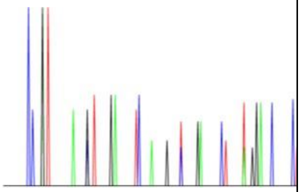
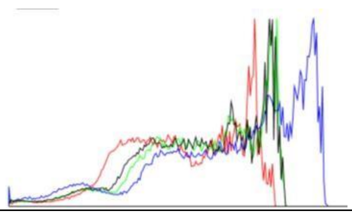
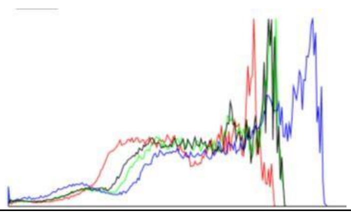
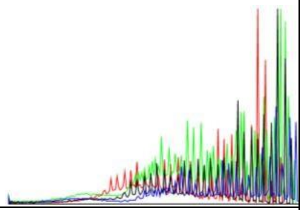
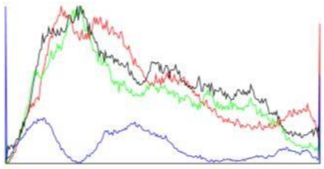
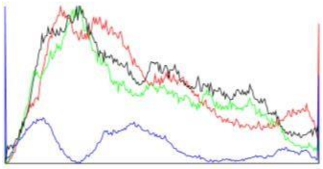
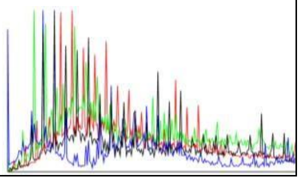
Images	Original Image	After decryption	After Steganography
Image 1			
Image 2			
Image 3			
Image 4			

Fig 5: Histogram (RGB values)

By performing the above experiments and after we obtained the results we checked if both the techniques satisfy the main properties necessary for securing an image. They are:

Confidentiality:

Confidentiality is the process of keeping the data private between the people who have authorized access to data.

Authentication:

It is an action or a process that involves the confirmation of the identity of the user.

Data Integrity:

It is the process of checking the consistency between the two images. We checked if both the images that is the original image and the obtained image are exactly the same without any compromise over the quality of the image.

And therefore the below mentioned table shows whether the techniques satisfied the properties or not:

Table 2: The properties satisfied by both the techniques.

Properties	Image Encryption	Image Steganography
Confidentiality	Yes	Yes
Authentication	Yes	Yes
Data Integrity	Yes	No

Here, image encryption satisfies all the three properties where as image steganography fails to satisfy the property of integrity.

VI.CONCLUSION

In this paper, different image securing techniques for making an image secure are discussed. Furthermore, compared results for these techniques are presented. From the obtained implementation and results it is concluded that image encryption and decryption is more efficient and reliable technique when compared to image steganography as it provides confidentiality, authentication and integrity of the image. Where as, image steganography on the other hand provides confidentiality and authentication but fails to provide integrity. Performance of these techniques was calculated using quantitative performance measures such as calculating the number of pixels and histogram evaluation (ie checking of RGB values). Since image encryption and decryption technique met all the requirements it is concluded that this technique is better and more preferable in order to make the image secure and thus avoiding it to be misused by unauthorized users while transferred over a network.

REFERENCES

[1] Gopal et al, “A Systematic Review on Image Encryption Techniques”, Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 3055-3059.

[2] Neena M K, “Image Transmission Techniques”, International Advanced Research Journal in Science, Engineering and Technology, vol 4, special issue 1, 2018.

[3] Yasser I, Mohamed MA, Samra AS, Khalifa F. “A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications”, Entropy (Basel). 2020 Nov 4; 22(11)

[4] Sahu, Aditya Kumar and Sahu, Monalisa, “Digital image steganography and steganalysis: A journey of the past three decades”, Open Computer Science, vol 10, no. 1, 2020, pp. 296-342.

[5] Li B., He, J., Huang J., Shi Y. Q., “A survey on image steganographyand steganalysis”, Journal of Information Hiding and MultimediaSignal Processing, 2011, 2(2), 142-172

[6] Trivedi M. C., Sharma S., Yadav V. K., “Analysis of several imagesteganography techniques in spatial domain: A survey”, In Proceedings of the Second International Conference on Informa-tion and Communication Technology for Competitive Strategies,2016, 84

[7] Guodong Ye, Kixin Gio , Huishan Wu, Chen Pan, “An Asymmetric Image Encryption Algorithm Based on a Fractional-Order Chaotic System and the RSA Public-Key Cryptosystem”, International Journal of Bifurcation and ChaosVol. 30, No. 15, 2050233 (2020).

[8] Naveen M-Acharya, “An Extensive Survey on Image Security Research Trends”, Institute of Technology-Volume 7 – No. 13, February 2018

[9] G. Nisha, R. Aarthy, N. Sasikaladevi, “An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security ‘Procedia Computer Science 115 (2017) 643– 650

[10] Jyotika Kapur, “Security using image processing”, International Journal of Managing Information Technology, (IJMIT) Vol.5, No.2, May 2013

[11] Gao, X., Yu, J., Banerjee, S. *et al.* “ A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion”. *Sci Rep* **11,** 15737 (2021).