Enhanced Secured Image Transfer over Internet

Kiran Gupta¹, Raunil Singh²

¹ Assistant Professor, CSE, SDDIET Barwala, Kurukshetra University Kurukshetra, India
² PG Scholar, CSE, SDDIET Barwala, Kurukshetra University, Kurukshetra, Haryana, India

Abstract—Steganography is the art of hiding the information through which the communication is taking place. With the advancement in hacking techniques the researchers are improvising their research in order to overcome the hacking technique by compression, encryption, steganography or their combinations. This paper describes the various researches done so far on image compression security. We are studying the different image compression techniques and analysing all these techniques. We can combine these techniques to design a stronger image security model and test the performance of image security system. In the end the goal to be achieved is image security.

Keywords—Steganography, Discrete Cosine Transform, Discrete Fourier Transform, Discrete Wavelet Transform, Fast Fourier Transform, Digital image processing, Advanced Encryption Standard, Data Encryption Standard

I. INTRODUCTION

An image may be defined as a two-dimension function, f(x,y) where x and y are spatial (plane co-ordinates, and the amplitude of f at any pair of co-ordinates (x,y) is called the intensity or gray level of the image at that point. When x,y and the intensity values of f are all finite, discrete quantities, we call the image a digital image.[1]

Fig 1: Basic fundamental elements of an image processing system

The field of DIP refers to processing digital images by means of a digital computer. A digital image is composed of a finite number of elements, each of which has a particular location and value. These elements are called picture elements, image elements, pels and pixels. Pixel is the term used most widely to denote the elements of a digital image. [1]

One of the first applications of digital images was in the newspaper industry, when pictures were first sent by submarine cable between London and New York.[1]

Fig 2: Fundamental steps in digital image processing

With the fast growing network, many people utilize the various applications to transfer digital image data. Most of people share their personal images with other users using the social application. Hacking attacks on these applications can cause great losses to the user security which can lower the number of active users and so the business popularity. Now-a-days users access these applications from their portable devices (smart phone, tablet, etc.). To prevent the hacking attacks on those web or mobile application architectures, there is various data security mechanism for image, video or text data. These existing security mechanisms are either using encryption or steganography, or their combinations. There is various securable and perfect system of image encryption that can be well protected from unauthorized access [13]. When it comes to the image transfers over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. To achieve the goal of image security, a number of image security and image processing algorithms are in use individually or in a combination to provide the effective image security. But these existing image security mechanisms fail to provide the best image security and sometimes proved to be breakable or hackable. Image compression is an additional function, which can be applied on the image to lower their memory size. The known and popular algorithms used for the data compression are DFT, DCT, DWT, etc. [13]. Popular and best compression algorithms are DFT, DCT or DWT. Steganography technique is used to hide digital data into another digital data (image into...
image, etc.). Popular steganography techniques are used to embed image (secret object) into image (cover object) are Spatial Domain and Transform domain methods. Mostly used compression schemes in existing security models, are DCT, DFT, FFT and DWT. DWT is the best because it is a robust compression scheme and outperforms the others. DCT and DFT provide less compression than DWT. For the portable devices with limited memory, using higher compression becomes better idea [13]. On battery running portable devices, lower computational count and higher speed lowers the CPU usage and hence result as longer battery life[13],[11] and [9]

Colour clustering based image steganography is used to hide the digital image data into image as a cover object on the basis of colour patterns. Hence colour clustering outperforms the existing steganography methods i.e. spatial domain method and transform domain method [10],[10]. Therefore the proposed study of image security includes the usage of DWT for compression with colour clustering based steganography for hides the data.

Image transfers over internet or intranet are prone to hacking. The image transferred over internet or intranet can be hacked by hackers using some attacks: [6].

1. Passive attacks: A passive attack attempts to learn or make use of information from the system but does not affect system resources. It is of two types: Release of message content, Traffic analysis.

2. Active attacks: Active attacks involve some modification of the data stream or the creation of a false stream. And subdivided into masquerade, replay, and modification of messages and denial of service.

End to end authentication can be also used to keep image transfer integrity intact, but end to end authentication is not possible in case of many image transfers, because many server based internet services like Facebook, Whatsapp, etc. does not let a user to save the content in secure formats, and does not allow the end-to-end authentication based protocols [6].

In order to guard the image transmission, the algorithms usually used for the Image security purpose are: Compression, Encryption and Steganography. The DWT technique used for compression is more complex. However DCT is simple to implement so data can be easily access by unauthorized user [13]. DCT is simple as the number of computations is less in it, because it computes cosines function at the different frequencies. DWT is complex than DCT because numbers of computations are more and it works with both, the frequency and time. For the numerical and functional analysis, DWT uses a number of options between the wavelets.

For the encryption of images, we use a variety of symmetric or asymmetric algorithms like Blowfish, AES, DES, etc. [14],[11] and [9]. Symmetric key encryption uses same key to encrypt and decrypt, whereas asymmetric key algorithms uses different keys for encryption and decryption [14], [11] and [9]. DES used to encrypt the block size 64-bit using 56-bit key size and having 16 rounds for encryption and decryption also. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), RSA (Rivest, Adi Shamir, and Leonard Adelman) uses 128-bit block size and variable key-length for encryption. AES used to encrypt the block size 128-bit using 128,192 and 256 bit key size and having 10, 12 and 14 rounds for encryption and decryption.

Steganography is a security mechanism which is used to hide the message into another object which may be a text, image, audio, video etc. The techniques used into the steganography are spatial domain method, Transform domain method [11] and [10], and Colour clustering based steganography [12]. Steganography comes into fashion to hide the text into text, image into image, text into image, text or image into audio, audio into audio, audio into video, etc. In spatial domain scheme, the secret messages are embedded directly. The transform domain Steg. Technique is used for hiding a large amount of data with high security, a good invisibility and no loss of secret message [11] and [9]. Colour clustering based steg. is exclusively used to hide image into image data based on the colour patterns or texture [12].

II. RELATED WORK

Sonja Grgic[2], In this paper they examined a set of wavelength functions for its implementation in a still image compression system and resulted in the benifits of this tranformation. A comparison with a discrete-cosine-tranformation-based compression system is also given.

Domenico Bloisi[3]. In this paper a method for integrating together cryptography and steganography through image processing has been described. They proposed a system which perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography. They presented a novel method for integrating in a uniform model cryptography and steganography. And concluded that ISC algorithm is an affective steganographic method as well as a theoretically unbreakable cryptographic (ISC is an image based one-time pad).

Xiangui Kang[4], This paper was related to the issue of watermarking. They first detected the template which has corrupted watermark image to obtain the parameters of an affine transformation and converted the image back to its original shape. Then translation registration was performed using the training sequence embedded in the DWT domain and finally the informative watermark was extracted.

Morkel[5], In this research paper, an overview of image steganography is given, its uses and the various techniques that can be used. They concluded that there exists a large selection of approaches to hide information in images. And also that Least significant bit (LSB) can be used in both BMP and GIF, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.
Mohammadi S[6]. In this article, existing methods for protection are examined and also authors have proposed an innovative solution, which considerably increases the security of Internet polls and the reliability of their results. The proposed solution has two phases: the construction phase in which the poll content and CAPTCHA test are created and the utilization phase, in which vote counting operation is done. The CAPTCHA that is used in the proposed method is an image-based CAPTCHA. For the aim of voting, an Internet user has to drag his or her desired poll option expressed in form of movable text object and drop it on to the picture of an object indicated by the CAPTCHA. The proposed method is fair, robust, and resistant. One of the main advantages of the method is that it can be used by all ages. Gary C.Kessler[7], This is an online article and it is continuously updated. This link is the best source for the information and study about the various encryption algorithms, their working flow, algorithmic structure, etc. This link proved to be the major source behind my encryption algorithm studies.

Verma O.P[8], In this research, the author have presented two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This paper provides a performance comparison between four of the most common encryption algorithms: DES, 3DES, Blowfish and AES (Rijndael). The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. Simulation has been conducted using C# language.

Ashwin S. [9], This paper presents a review of the literature on different types of contemporary steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image. In addition, research trends and challenges are identified and directions for future research are discussed.

Chanu Y. J[10], In this paper, the author has conducted a detailed survey on various steganography techniques. From this paper it is easy to understand and compare the steganography techniques. This paper is the major source behind my study on steganography.

MilindMathur[11], The authors have conducted a survey on the encryption algorithms. The detailed survey on encryption algorithms covers all of the popular and prominent algorithms. This survey shows that blowfish is the best encryption algorithm and outperformed all others. Blowfish takes least time and provides maximum throughput.

Chamkour [12], A novel steganography technique is proposed in this paper, which perform color based analysis on the image by using color clustering technique to hide the image data effectively into another image. This method is more secure than all other image steganography methods because it makes it difficult to detect the hidden image in the masking image. NavitaAgarwal[13], The authors have conducted a similar research, where they have applied compression, encryption and steganography on the digital image data. Pixel shuffling based symmetric encryption algorithm, DCT for compression, WinRAR to Image steganography are used to achieve the proposed model in this paper.

Gary C.Kessler[14], This is an old published paper on cryptography by Gary C. Kessler, and since then it was continuously updated till date. It was last updated in 2014. The author suggested the great source for the cryptography algorithms again. It is very important to understand the encryption algorithm structure before putting it in the use.

### III. Proposed System

On the social applications, most of its users share their personal data (images, etc.) using many applications. Hacks into these applications can cause great losses to the user security which can lower the number active user and so the business popularity. Now-a-days users access these applications from their portable devices (smart phone, tablet, etc.). To prevent the hacking attacks on those web or mobile application architectures, there is various data security mechanism for image, video or text data. These existing security mechanisms are either using encryption or steganography, or their combinations.

The major Problem of the existing systems is that, they are not well designed according to the portable devices running on batteries because of their limited memory, battery life and computational capability. The security models are not very energy efficient or computationally efficient, which affect the performance of portable devices (smart phones, tablet, etc.). This either affects the memory or battery or both. Compression is also being used to lower the file size, which saves the memory and easy to transport of internet. Compression algorithms are used to compress the digital data. In this research, we propose an effective and efficient Image security system for image sharing on online application. First step towards the research is the study of the existing algorithms for compression, cryptography and steganography. It will lead towards the development of an image security model for sharing the image over internet. This is also very important to get internet.

Through this we can get the information about the parameters and protocols. DWT and colour clustering based steganography. This can be implemented in the matlab simulator. A thorough performance and feature testing model would be formed and utilised to analyse the performance of the security model, to detect the flaws and to recover them.

#### A. Objectives

The main aim of the proposed study is to provide a secure system for the image sharing on online application by improving the existing techniques.
1. Study the image compression techniques (DWT, DCT, etc.).
2. To study the literature related to steg. (specifically color clustering and color clustering based steganography).
3. Implement and analyze all of the above three methods.
4. Combine the techniques to design a stronger image security model.
5. Test the performance of the image security system.

IV. CONCLUSION

The paper describes the various researches done so far on enhanced secured image transfer over internet. This can be done by cryptography, encryption and steganography or even the combination of all the above techniques and the algorithms discovered so far. Through this we can secure the image transfer on various networking sites.

ACKNOWLEDGMENT

Authors are grateful to the head of department of the institute for encouraging us and supervising us.

REFERENCES