Digital Image Watermarking Using Enhanced Fractal Technique

Bhavmeet Kaur
Dept. Of ECE University College of Engg. Punjabi University Patiala,India
bhavmeetkhivi@yahoo.com

Dipti Bansal
Dept. of ECE University College of Engg, Punjabi University Patiala, India
dipihi@gmail.com

Abstract—Image watermarking is the technology that is being used to provide secure communication between the sender and the receiver. The widespread use of internet has gained immense popularity and this has made the digital information and data such as images, audio and video clips available to audience. As the technology enhances, security becomes the important concern. Thus, watermarking helps in embedding the watermark image with the original image so that unauthorized user cannot access the data. In this technique signal is added to the host signal for privacy. In this paper, different techniques are discussed. This paper also concludes the proposed technique compare with the existing techniques. Compressing the data will reduce the length and increases the security of the system. So a key exchange algorithm is also used that will provide additional security to the data. Experiments have been performed with the proposed and existing technique and result shows the efficiency of the proposed method is better in terms of security.

Keywords- Diffie-Hellman Key Exchange; Watermarking; embedded; encoded; decoded.

I. INTRODUCTION

An image is a combination of number of pixels on the screen. It can be a 2Dimensional such as a photograph, screen display etc. or 3Dimensional image such as a statue or hologram. A digital image is a numeric representation. Normally binary representation of a two dimensional image is known as digital image. It can be detected or hacked by attacker. Thus, to secure the image from unauthorized user, it must be encrypted. Watermarking is a technique that is used for embedding with the host signal. This technique can be performed on the image, audio or video data. In this paper, image watermarking is used to provide security. Image watermarking encrypts the original image with the watermarked image and sends it to the receiver side. Sender can apply visible or non-visible marking to the image. Various techniques are used for watermarking. In this paper, the new technique is proposed for more efficiency as compared to existing techniques. In the proposed method, original image is taken, embedded it with watermarked image and the produced output transmit to the receiver. The basic idea behind using this technique is to retain the quality of the image. Watermarking includes various properties that are needed to be taken care before the process. Such as: - robustness, transparency, capacity etc. In this paper, the main focus is on the Diffie–Hellman key exchange technique.
Fig 1: Block diagram of the watermarking.
In this block, first the original image and watermarked image is taken and embedding is performed with the help of key technique and then output is produced or the watermarked image is obtained.

II. COMPRESSION
Compression is a technique which is used to compress the data without reducing the quality. Compression can be performed on different types of data i.e. Image, Video, Audio or Text. It is also helpful in reducing the storing number of bits. Compression is the method that reduces its original size without reduction in its quality. There are different techniques that are being used for compression. Different techniques have different advantages and disadvantages. The basic techniques used for compression are: - Run Length encoding, Fractal compression, Diffie-Hellman Key Exchange etc. These techniques are used for compression depending on the requirement of the data. Compression is done through removing the redundant data from the original data.

III. PROBLEM OF THE TRADITIONAL APPROACHES
Image watermarking is used to embed the original image with the watermarked image. In this technique, carrier signals embedded with the watermark image for obtaining watermark signal. Watermark can be an image, audio, video or text. Watermarking plays vital part in degrading the unauthorized access. The basic idea behind using watermarking is to retain the quality of the image which is done through the various techniques. The existing techniques of watermarking are not capable enough to provide security and efficiency. Watermark is embedded with the original image but it is observed that in the existing methods, the security of watermark image is not in consideration. Thus, the security of every part in the watermark is to be considered. Due to this reason, the proposed system is introduced.

IV. PROPOSED WORK
In this section of the paper, the main focus is on the proposed technique that is used to overcome the drawbacks of the existing method. Due to some security and efficiency issues, proposed technique is under considerations. Experiments have been performed and conclude that the proposed technique is better than the old techniques. In the proposed work, Diffie-Hellman Key Exchange technique is used for secure communication between the sender and the receiver. Thus this technique is helpful in exchanging data between them with the privacy.
Diffie-Hellman Key Exchange

This technique is used for cryptography for encryption as well as decryption. It is implemented in the public key exchange protocol. This key exchange method provides shared secret communication between the sender and the receiver. The secret key is known both to the sender as well as the receiver. This key will help in encryption as well as decryption. So the in between attacker will not be able to detect the key. Key is the main component in this technique. Communication between the both the parties are secure and protected due to the proposed method.

V. METHODOLOGY

In image watermarking the data is hided in the image, in the proposed work the Diffie–Hellman key exchange algorithm used for the secure transmission of the data. The proposed methodology consists of two parts one is encoding and other is decoding, the methodology of the work done is given below:

Encryption part

1) Initially an image is selected from the data set of the images, in which the data is to be embedded and is send to the receiver at the other end.

2) After selecting the image , next step is to convert the selected image into the lab color space for the further processing on the image

3) Select an watermarked image from the given set of the watermarked images, apply encoding on the selected watermarked image for the compression of the data. Finally the data is compressed.

4) Now embed the compressed data in the image that is converted into the lab color space after in step 2.

5) After embedding the data in the image , hide it into the image

6) Finally an Data embedded image is obtained and is send to the receiver at the receiver end

7) After obtaining the image the performance parameters are calculated.

Fig 2 flow diagram of proposed methodology

Selection of the original image

Selection of the watermarked image

Covert image into Lab color space

Apply encoding algorithm

Data embedding in the image

Finally Data embedded image is obtained

Performance parameters are calculated

Available online: http://internationaljournalofresearch.org/
Decryption part

At the decryption side, data is decoded to obtain the original image from the watermarking image. The whole process works in reverse order with the help of secure key that is send by the sender. Encrypted image is taken as input and decoding algorithm is applied to it and produces result is the original image.

VI. RESULTS AND DISCUSSION

In this section of the paper, results have obtained after applying encryption or watermarking to the original image. It also includes the comparison that has been performed on the proposed method with the existing method.

Fig. 3:- (A) Original image  (B) Watermark image  
(C) Watermarked image  
(D) Extracted watermark

The following figure represents the results obtained by applying proposed method the following parameters are calculated. The parameters like MSE, PSNR, and BER are calculated. A comparison graph on the basis of the PSNR value obtained is calculated for traditional and the proposed approach.
VII. CONCLUSION AND FUTURE SCOPE

Image watermarking is the technique that is being used to provide security to the system. In this process, image is hidden into another image (watermark image) for the security purpose. Watermark is embedded in the image. It can be visible or invisible depends on the type of technique. Image watermarking does not change the actual meaning of the data. It just hides the data into another data or image. In this paper, conclude that the proposed technique is much efficient than the techniques used before. In this method, first format of the image is changed. After this process, compression is applied to the image and the compressed image sends to the receiver. Thus, proposed work and the experiments applied on both the methods shows the efficiency of the techniques. It concludes that the proposed technique is more secure and efficient than the existing one.

There are numerous techniques that have been used in the watermarking process. But in this proposed method, first data is compressed before it embedded into the image. Thus, this method is more secure and efficient than the traditional methods. This technique can be enhanced with the help of other compression techniques. Security of the network can be enhancing with the combination of two or more techniques to prevent unauthorized access.

VIII. REFERENCES


