Abstract — Information hiding is a technique of hiding information into an image and send to the receiver. The techniques is called watermarking and is mainly used for the security of secrete information over internet. Although there are various techniques implemented for the security and hiding of information, here in this paper a survey of all the techniques that are used for information hiding and retrieval are discussed here. So that by analyzing the various techniques implemented and by analyzing the issues in the technique new and efficient techniques is implemented in future.

Keywords— fragile watermarks, CDWM, QIM, CWE, WBS.

I. INTRODUCTION

Watermarking: A technology for the security of Multimedia in form of images, audio, video etc... Due to increase in internet popularity and so traffic use of multimedia files and data has also increased, sharing by it different communication means. Due to such situation a need aroused for the privacy and protection of such type of data and its sharing as it can contain confidential information or even personal data. Watermarking inserts hidden information or a watermark into the original media such as image or audio or video. For different purpose different type of watermarks can be used. Robust watermarks are used for ownership applications and data where as fragile watermarks can be used to authenticate data [1]. But if the authentication fails the entire image that has been attacked becomes unusable even on tampering a small part of it. This can overcome by using local authentication based watermarking. In local authentication based watermarking if tampered image does not authenticate, parts which do not get authentic can still be seen and can be put for further use. Local authentication based watermarking is used to detect and recover parts of tampered image.

Due to this development of multimedia technology various other security issues like copyright protection, traitor tracing etc. came into picture [2]. The need came to protect privacy of users in various multimedia applications. The security of data assures authentication of identity claiming the data, data confidentiality from unauthorized access data integrity for assurance that the data has not been changed or tampered by and any means [3].For such type of needs digital watermarking and fingerprinting protocol are being used with a variety of other watermarking protocols.

Various protocols allows the multimedia data provider to insert information about the owner of the file to preserve copyright and information about the one who is buying the media file or asking legally for its use to identify who violates copyright protection. Cryptography is another technique used for security of multimedia data it ensures that content of the data is secured by scrambling them making it impossible to understand. Another watermarking scheme is the fingerprinting scheme in which the sellers of multimedia data insert the buyer’s identity as the watermark into the content so that the seller can retrieve the buyer’s identity when seller gets a redistributed copy [4]. The aim of watermarking is to include imperceptible information in a multimedia document for securing it or just labeling the application. In comparison with Content dependent watermarking (CDWM) is the solution to overcome potential estimation attack used for recovering and removing the watermark from host signal. It is basically used for content authentication [5, 6]. In CWDM a decryption module is used before detecting watermark and only with correct decryption method watermark can be detected. With the help of integrity service it can be ensured that the sent and received multimedia data are identical.

![Figure 1. (a) Watermarking an Image (b) Extracting the watermark and detecting tampering.](image-url)
Watermarking can be defined as technique of digital pictures labeling by hiding secret information into the image. There are some key standards defined for watermarking technique they are [8]:

- **Imperceptibility**: The digital watermark should never be noticeable to the viewer.
- **Robustness**: The digital watermark should always be present in image even after attacks and can always be detected by the watermark detector.
- **Readability**: A watermark should always show as much as information possible.
- **Security**: A watermark should be secret and must be untraceable by an unauthorized user.

Another technique for watermarking is image authentication. A meaningful watermark with some other features is inserted invisibly in the image that can be stored in compressed form. The scheme can detect alterations of original image like tampering of images etc. Whereas many watermarking schemes also uses spread spectrum (SS) modulation technique used to insert the watermark with the multimedia data [9, 10]. With the help of Spread Spectrum Techniques a signal generated with a particular bandwidth is spread in frequency domain which widens the signal’s bandwidth and hence signal is transmitted on a bandwidth larger than frequency content of original information. Watermarking is applied on this transmitted signal in form of various digital watermarking techniques.

## II. LITERATURE SURVEY

In 2012 by Anamitra Makur, Nikhil Narayan S. “Tamper-Proof Image Watermarking using Self-Embedding “ Here propose a fragile watermarking with self-embedding for recovery of tampered image that does not use authentication bits. We use a robust spread spectrum based watermarking scheme using block based embedding, DCT based compression, and other improvements. Simulation results showing recovery performance are presented and find out the Conclusion we develop a novel algorithm for tamper detection and recovery of images using no authentication bit and robust watermarking. Here, the watermark is not only used for tamper detection, but it also carries enough information regarding the cover image so as to help in recovering the tampered parts of the received image. We have used a DCT based image compression scheme, spread spectrum image steganography to embed the watermark, several error correction schemes (both at the encoder and decoder) to enhance the watermark extraction, and careful selection of global and local MSE thresholds, to achieve up to 90% restoration of the tampered image [1].

Ming Li et.al. remarked the problem extraction of data blindly from a spectrum band in the domain of digital media in form of image, audio, video.

They developed a procedure to find and look to see hidden data in host which has been embedded in it by multicarrier spread spectrum. The procedure is named as “multicarrier iterative generalized least-squares (M-IGLS) core procedure”. They discovered that the algorithm can achieve recovery probability almost similar to the results obtained from embedding carriers and host autocorrelation matrix. They explained that while carrying out the experiments original host and embedding carriers were assumed to be absent. In accordance with the experimental result, the procedure they presented can be effective measure to conventional SS data hiding [10].

R. Sarkar et.al. explained the phenomenon of embedding watermark to a multimedia object in a way that it can be detected and extracted to make an assertion about the object later. They stated that the watermark embedded allow identifying the owner of hardware implementation even to audio and video files and needs to be digitally watermarked by embedding information to a digital signal that is irreversible. The research algorithm proposed by them stated easy implementation on hardware with low cost computation. The digital design proposed by them using FPGA is capable of secured communication and real time authentication [11].

Q. Liu et.al. explained seam carving defined as content aware scaling or image retargeting. They gave the idea of seams being used for reducing or increasing size of image for distortion free display on various devices. They provoked that Content-aware scaling can also be used to removing entire objects from photographs and hence can be used to tamper images which are now needed to be authenticated for legitimate purpose. They gave shift recompression based features for spatial domain and shift recompression based neighboring joint density for DCT domain. They used an ensemble classifier and steganalysis methods to identify forged images. They proposed shift recompression based features to detect seam carved forgery in images stored with same quantization matrix using fisher linear discriminate, LibSVM and ensemble classifier [12].

Gives the concept about Content-aware image resizing, also known as image retargeting, seam carving, content aware scaling, is originally proposed to automatically remove the paths of least importance, known as seams, to reduce image size or insert seams to extend it, in order to display images without distortion on various media especially on mobile devices, such as smartphones and PDAs. Contentaware scaling also allows removing entire objects from photographs without observed clues, and hence it has been used to tamper images. Due to the ubiquity of JPEG images on various mobile devices, it is increasingly necessary to authenticate these JPEG images for legitimate purposes.
To detect the content-aware-based forgery in JPEG images, in this paper, we merge shift-recompression-based characteristic features in spatial domain and shift recompression-based neighboring joint density in DCT domain together; an ensemble classifier is used to discriminate forged JPEG images from intact JPEG images. We also transfer other popular JPEG-based steganalysis methods to detecting the forgery. Experimental results show that steganalysis methods are effective in detecting context-aware-based JPEG forgery and our method is superior to other compared detection methods and find out the Conclusion propose a shift-recompression-based feature mining to detecting seam-carved forgery in JPEG images, which are stored with the same quantization matrix. The classifiers Fisher linear discriminant, LibSVM, and ensemble classifier are employed for the detection. We also adopt several recently welldeveloped steganography detectors to detect content-aware-based forgery in JPEG images. Experimental results show that steganography detectors can be used to detect content-aware-based forgery with satisfactory detection performance. Our approach outperforms other detectors in the comparison and achieves better detection accuracy with a much short number of features.

C.H. FAN et.al. provided with the fact that due to increase in internet usage digital multimedia can easily be transmitted which thereby increased concern about intellectual property and copyright protection. They gave quantization index modulation (QIM) algorithm for watermarking based protection of media data. They came with an approach that resisted high JPEG compression ratios maintaining good image quality. The proposed mechanism stated that the robust embedding points and values of image in the JPEG compression are determined and then QIM algorithm is used to insert a watermark into the image and generating a secure key which thereby can be detected by this key. With the help of robust embedding points and values a watermark can be easily inserted. For the future work they stated when the size of the embedded watermark exceeds a specific boundary robust embedding points gets restricted resulting in generation of experimental result by the embedding capacity [13].

A. V. Subramanyam et.al. Depicted the problem faced by distributors while distributing digital media at multiple levels of distributors in an encrypted and compressed format. The problem generated of embedding watermark in compressed, encrypted domain for detection of copyright violation. They proposed a robust watermark embedding technique for JPEG2000 encrypted and compressed images preserving the confidentiality of content and maintaining image quality. The extraction of these watermarks is possible through encrypted or decrypted domain.

The implemented algorithm by them is simple because it does not require decrypting or decompression of the content compressed or encrypted.

They analyzed the relation between payload capacity and quality of image at different resolutions of the image resulting in higher resolutions carrying higher payload capacity without affecting the quality. They found that degradation in quality was more than caused by watermarking higher resolutions [14].

In this paper, we propose a robust watermark embedding technique for JPEG2000 compressed and encrypted images. While the proposed technique embeds watermark in the compressed encrypted domain, the extraction of watermark can be done either in decrypted domain or in encrypted domain and found out the Conclusion a technique to embed a robust watermark in the JPEG2000 compressed encrypted images. The algorithm is simple to implement as it is directly performed on the compressed-encrypted domain i.e it does not require decrypting or partial decompression of the content.

R. Schmitz et.al. proposed an approach of commutative watermarking-encryption (CWE). The approach proposed by them uses permutation cipher to encrypt the media data leaving its global statistics intact therefore with the help of non-localized watermarking scheme these global statistics can be attached to permutation cipher for forming a commutative watermarking encryption scheme. They explained concrete CWE scheme which was made by combining histogram watermarking scheme with permutation cipher which was based on 2-D chaotic map (discrete). They defined their future work as applying permutations without effecting efficiency of compression and to make the scheme more robust and if possible to revert CWE schemes [15].

In 2009 by Shiraz Ahmad1,a,b “Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants” gives the Many proposed image watermarking techniques are sensitive to geometric attacks, such as rotation, scaling, translation, or their composites. Even slight geometric distortions can also disable the watermark detector to reliably perform its function. In this paper, we utilize the robust invariant image features and discrete Hahn image moments to design a robust watermarking system that can withstand many geometric-distortions as well as survive a variety of common watermark attacks. Scale-invariant feature transform (SIFT) based bounding boxes and discrete orthogonal Hahn moment-invariants are used to embed watermark information into the selective image patches. Hahn moment-invariants are utilized for watermarking purpose because they are invariant to rotation, scaling, and translation.
Watermark detection is performed by synchronizing the SIFT points and then computing the RMS threshold value between the original and the watermarked images. Several tests are performed to check the robustness of the proposed method. Experimental results validate the effectiveness of the scheme as well as prove that the proposed method is robust to several geometric attacks and find out the Conclusion A new and effective feature-based image watermarking system employing discrete Hahn moments and Hahn moment-invariants is proposed and presented. The presented results validate that the proposed system is not only robust against geometric distortions but also effectively withstands many image processing attacks [16].

REFERENCES
[16] Shiraz Ahmad1,a,b, “Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants” a Dept. of Electronic and Information Engineering, HIT Shenzhen Graduate School (HTSGS), Shenzhen 518055, P. R. China. b Pakistan Atomic Energy Commission (PAEC), Islamabad 44000, Pakistan.acm-2009.