Survey on Image Tampering Detection and Recovery Techniques

Maria Johnson
M.Tech Student,
ViswajyothiCollege of
Engineering and Technology

Resmi Cherian
Assistant Professor,
Viswajyothi College of
Engineering and Technology

ABSTRACT
The applications of digital images are increasing exponentially in the field of image processing. Many image editing tools and computer applications are available to manipulate the images. Hence image tampering has been increasingly easy to perform. It is very difficult to say whether an image is original or a manipulated version by just looking it. As a result of such modifications digital images have almost lost their reliability. Watermarking can be used to identify such modifications. Watermark can be hash values of the image, compressed content of the image etc. This paper discusses about various image tampering detection and recovery techniques.

Keywords
Image Tampering, Tampering Detection, Image Reconstruction, Watermarking.

1. INTRODUCTION
Today digital images are the most popular source of information in many of the applications like medical imaging, forensics etc. Digital images can be easily manipulated by image processing tools. One of the greatest challenge is to determine whether the image is genuine or faked. Attackers can replace some portion of digital image without any noticeable changes.

Recovering original image is a long standing problem for many image processing applications. Watermarking can be used to detect the tampering and to recover the original image. Watermark is the representation of content of the host image and it is embedded into the original image. The original content in the manipulated area can be restored after the extraction of watermark in the rest of the areas. Image reconstruction is one of the main features of digital image authentication schemes. Image hashes can be used as watermark for authentication, where hashes describe the original image content and hash value is used to describe the content, and it can be used to restore the tampered regions of the image. Sometimes the information used for reconstruction is a reduced quality version of the original image. This paper discusses about various image tampering detection and recovery techniques.

2. METHODS
In [1] Xinpeng Zhang and Shuozhong Wang proposed a fragile watermarking scheme capable of perfectly recovering the original image from its tampered version. The watermark data consist of two parts: reference-bits and check bits. Reference bits depends on the original host image, and check-bits are determined by the host content and the reference bits. Reference-bits and check-bits are embedded into all blocks of the host image using a DE algorithm. Sometimes an attacker may replace the content of a watermarked image with fake information. In such cases tampered blocks can be identified by comparing the extracted check-bits with the calculated check-bits at the receiver side. Inorder to recover the original content in the image, the reliable reference- bits from the rest of the blocks are extracted. This fragile watermarking scheme is applicable to color images. But fragile watermarking can be used to restore original image only if the modified area is not too extensive.

In [2] Hongjie He, Fan Chen .et.al proposed a performance analysis of block-neighborhood-based fragile watermarking scheme. This method consists of four steps: watermark embedding, watermark extraction, tamper detection, and recovery. The original image is partitioned into several blocks in the watermark embedding step. Each block consist of six most significant bit planes(MSB) and least significant bit planes(LSB). Then six recovery bits for each block is computed. The recovery and key bits for a block are concatenated in a bit vector. The 8 bit watermark vector is obtained by encrypting the feature with a secret key. Then for each block the watermark payload is inserted. All blocks in the test image are marked as either valid or invalid after tampering detection. The invalid blocks can be classified into two categories: feature-reserved and feature-destroyed invalid blocks. The recovery procedure for the invalid blocks consist of two steps. All feature-reserved invalid blocks are recovered using the extracted features from its mapping block, and the feature-destroyed invalid blocks are recovered by the average intensity of the neighboring valid pixels. Block neighborhood based fragile watermarking can be used to detect multiregion and multiattack tampering.

In [3] Xinpeng Zhang, Zhenxing Qian .et.al proposed a novel watermarking scheme with flexible self-recovery quality. The watermark data is calculated from the original discrete cosine transform (DCT) coefficients of host image. When the image is tampered, the watermark data can be extracted. Reconstruction depends on the amount of extracted data. If the amount of extracted data is large, reconstruction is done according to the constraints given by the extracted data. Otherwise, a compressive sensing technique is applied to retrieve the coefficients by exploiting the sparseness in the DCT domain. Compressive sensing and compositive reconstruction is applicable only if the tampering percentage is less than 45.

In [4] Mehmet Utku Celik .et.al proposed a framework for lossless authentication watermarking. This framework enables zero-distortion reconstruction of the un-watermarked images upon verification. It also allows validation of the watermarked images before recovery of the original image. Therefore computational requirements can be reduced in situations when either the verification step fails. Integrity of the reconstructed image for verified images is ensured by the uniqueness of the reconstruction procedure. For efficient tamper localization it

provides a public key authentication. By using lossless authentication watermarking, computational efficiency and implementation flexibility can be achieved.

In [5] Shuozhong Wang, Zhenxing Qian .et.al proposed self-embedding watermarking scheme based upon a reference sharing mechanism. The original principal content in different regions in an image is taken as the watermark and shared by these regions for content restoration. To recover the principal content in the tampered area, the reference data and the original content in the reserved area are used. Reconstruction can be done in two ways. In first method the original data in five most significant bit layers of a cover image can be recovered and the original watermarked image can also be retrieved when the content replacement is not too extensive. In second method the host content is decomposed into three levels. Then employ a reference sharing method with different restoration capabilities to protect the data at different levels. By extracting the data from 5MSB the original image can be recovered only when the tampering rate is not more than 24%. Reference sharing with different restoration capabilities provides better restoration results.

In [6] Pawel Korus and Andrzej Dziech proposed a model of the content reconstruction problem in self-embedding systems, based on an erasure communication channel. To generate the reconstruction reference first image is divided into non-overlapping blocks. Bit substitution for data is used to embed the data in the 3 least significant bit-planes. The remaining 5 bit-planes are transformed into DCT domain for generating the reconstruction reference. This ensures that the embedded watermark does not interfere with the reconstruction reference generation basis. The 192 bits of watermark capacity are divided into two parts: 32 bits and 160 bits. Hashes are obtained by shortening the MD5 hashes using exclusive disjunction on neighboring bit pairs. 32bits are used for embedding the hash. The reconstruction reference is embedded in the remaining 160 bits. Quantization of the DCT coefficients are performed by using reconstruction reference generation function. This scheme provides high quality reconstruction of the image but quality of the restored image depends on some parameter values.

In [7] Paweł Korus, Jarosław Białas .et.al describe a design of practical self-recovery mechanism for lossy compressed JPEG images. At encoder side, the first step is to apply a standard JPEG compression with a quality factor. After JPEG compression, the resulting image is then used to generate the reconstruction reference. The watermark data is then generated from the reference data. The individual watermark symbols are scrambled and embed them into their corresponding macro-blocks. At decoder, watermark is extracted and hash is calculated. Then compare the calculated and extracted hashes to identify the tampered blocks. Image blocks to be restored can be identified from the tampering map and reconstruction can be achieved by using the watermark. This scheme guarantees a high and stable level of reconstruction quality.

In [8] Dekun Zou, Yun Q. Shi .et.al proposed a semi-fragile lossless digital watermarking scheme based on integer wavelet transform. The watermark is embedded in the integer wavelet coefficients of the image. The IWT coefficients can be derived from the image file through tier 2 decoding followed by tier1 decoding. Then encoding is applied to the changed coefficients to form the JPEG2000 file for transmission. At receiver, watermark is extracted that is the hidden data could be extracted from the marked JPEG2000 image file and all the modified coefficients can be inverted back to the original ones. The data hiding is carried out block by block. Inorder to achieve this selected high frequency subband is split into into non overlapping blocks. This scheme can be used for content based image authentication because the hidden data are robust to non-malicious attacks to a certain extend.

In [9] Adnan M. Alattar proposed a reversible watermarking algorithm with very high data-hiding capacity for color images. This reversible watermarking algorithm allows the watermarking process to be reversed, which restores the exact original image. It provide very high data hiding capacity for color images. The reversible watermarking hides several bits in the difference expansion of vectors of adjacent pixels. To avoid underflow and overflow the required general reversible integer transform and the necessary conditions are derived for any vector of arbitrary length. The potential payload size is determine and a feedback system for controlling this size is developed. Inorder to increase the amount of data that can be hidden into an image, the embedding algorithm is recursively applied across the color components of the image. In this method the amount of data embed into an image depends on the nature of the image.

In [10] Pawel Korus and Andrzej Dziech proposes an adaptive self embedding scheme. It differs from traditional schemes by using multiple reconstruction profiles. Multiple reconstruction profiles are used in adaptive self embedding schemes. The reconstruction profiles are used to describe and restore the content of individual image blocks. Block-based discrete cosine transform (DCT) spectrum is used to generate the reconstruction reference. A profile is defined by a set of quantization code-books, and the allocation of the precision of coefficient representation. Quality descriptor is referred as the mapping between image blocks and the reconstruction profiles. Quality descriptor needs to be reliably communicated to the decoder and the descriptor is separated from the reference information. For each block the information about the assigned profile could be placed in a header of the reference information.

In [11] Saeed Sarreshtedari and Mohammad Ali Akhaee proposed a source-channel coding approach to digital image protection and self-recovery. The method embed the watermark into the original image and the watermark is used to find the tampered areas of the received image, and recover the content of the original image in those zones. In order to embed the watermark keep most significant bits of each pixel unchanged, and use the remaining bits for the watermark embedding. Mainly the system consist of three phases watermarking embedding, tampering detection and image recovery. In watermark embedding phase, the original image is source coded and the output bit stream is protected using appropriate channel encoder. The original image is divided into several blocks and for each block hash value is calculated. Then the channel coded data and the hash data is embedded as the watermark. At receiver side the calculated and extracted hashes are compared to detecting the tampered blocks. After tampering detection erasure locations detected by check bits help channel erasure decoder to retrieve the original source encoded image. In source channel coding approach watermark image quality is achieved through spending less bit budget on watermark. But this method recovers the tampering up to 33%.

3. CONCLUSION

Recovering original image from tampering is one of the major issue in many image processing applications. Various systems

are available to recover the image from tampering. In fragile watermarking the original image can recover only if the modified area is not too extensive whereas, in DCT based watermarking original image can be retrieved if tampering is less than 45%. Computational efficiency can be achieved by using lossless authentication watermarking. In this survey several methods have been studied to recover the original image from tampering.

4. REFERENCES

[1]Xinpeng Zhang and Shuozhong Wang, "Fragile Watermarking With Error-Free Restoration Capability, " IEEE Transactions on multimedia, vol. 10, no.8, December 2008.

[2] Hongjie He, Fan Chen, Heng-Ming Tai, Ton Kalker and Jiashu Zhang, "Performance Analysis of a Block-Neighborhood- Based Self-Recovery Fragile Watermarking Scheme," IEEE Transcations on information forensics and security,VOL. 7, NO. 1, February 2012.

[3] Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng, "Watermarking With Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction," IEEE Transcations on information forensics and security, VOL. 6, NO. 4, December 2011.

[4] Mehmet Utku Celik, Gaurav Sharma, and A. Murat Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an Implementation," IEEE Transcations on image processing, vol. 15, NO. 4, April 2006.

[5] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng, "Reference Sharing Mechanism for Watermark Self-Embedding, " IEEE Transcationson image processing, vol. 20, no. 2, February 2011.

[6] Pawe Korus and Andrzej Dziech, "Efficient Method for Content Reconstruction With Self-Embedding, "IEEE Transcations on image processing, vol. 22, no. 3, March 2013.

[7] Pawe Korus, Jarosaw Biaas and Andrzej Dziech, "Towards Practical Self- Embedding for JPEG-Compressed Digital Images," IEEE Transactions on multimedia, vol. 17, no. 2, February 2015.

[8] Dekun Zou, Yun Q. Shi, Zhicheng Ni and Wei Su, "A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 10, October 2006.

[9] Adnan M. Alattar, "Reversible Watermark Using the Difference Expansion of Generalized Integer Transform, "IEEE Transcations on image processing, vol. 13, no. 8, August 2004.

[10] Pawel Korus and Andrzej Dziech, "Adaptive Self-Embedding Scheme With Controlled Reconstruction-Performance," IEEE Transcations on information forensics and security, vol. 9, no. 2, February 2014.

[11] Saeed Sarreshtedari and Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery, " IEEE Transcations on image processing, vol. 24, no. 7, July 2015.