A Study on Image Authentication and Recovery Techniques

N. Manonmani
M.Phil Scholar, Department of Computer Science
SNR Sons College, Coimbatore, Tamilnadu, India

Dr. Anna Saro Vijendran
Professor & Head, Department of Computer Application
SNR Sons College, Coimbatore, Tamilnadu, India

Abstract - Images transmitted electronically are vulnerable to unauthorized changes. The transmission does not guarantee that the receiver has received the original image. When the image integrity has been compromised it is necessary for the receiver to detect the attack and also recover the original image. In this paper a survey regarding the image authentication combined with recovery techniques has been conducted.

Keywords – Watermarking, Hashing, Authentication

I. INTRODUCTION

With the advent of Internet and growing number of users, millions of images are transmitted every day, the growing number also brought its own challenges. Attacks such as man-in- the- middle and other sophisticated attacks have also risen proportionally increasing the risk of unauthorized access to images. The images transmitted are susceptible to many interception attacks and with great number of tools available the ease of attack has increased. The unauthorized manipulation leads to the loss of integrity or authenticity of the images.

Traditionally "Watermarking" methods are used to verify the integrity. Watermarking is generally used to identify the ownership or copyright information of the image transmitted but there is only less provision to recover the original image. In the past many methods have been developed for authentication and recovery process. But only a modest amount of research has been conducted. Our motivation is to attempt a detailed study on image authentication and tamper recovery algorithms.

A digital image watermark is embedding a pattern of bits into the original image to prove its authenticity. There are different types of watermarking such as visible and invisible, robust and fragile. In order to protect images in public access visible watermark is used, on the other hand invisible watermark is used for authentication and copyright infringement.

A. Image Authentication and recovery

The customary approach used for image authentication and recovery is watermarking. It can be applied to both spatial domain and frequency domain. The general process flow for authentication and image recovery involves the following steps:

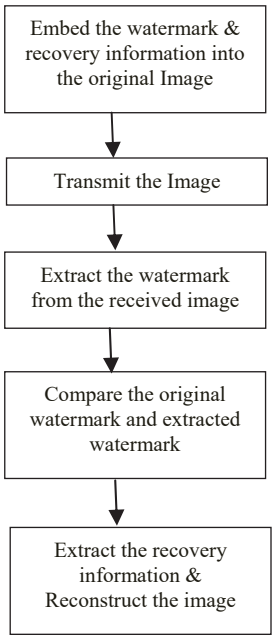

Figure 1. General process of authentication and recovery

B. Hash Based Authentication

Hash based authentication methods uses a set of features extracted from the image that represents the image, to construct the hash that is used for authentication. The hash value is then appended to the original image. Hash based methods have the following properties: Robustness, fragility and security.

Robustness:

The image hashing should be invariant to incidental modifications and common image processing operations including JPEG compression, small angle rotation, brightness adjustment, scaling, and noise contamination.

Fragility:

The image hashing should be able to distinguish the visually distinct images.

Security

Security is the degree to prevent the attacker from circumventing the authentication system with a maliciously tampered image.

The general method of hash based authentication involves the following steps:

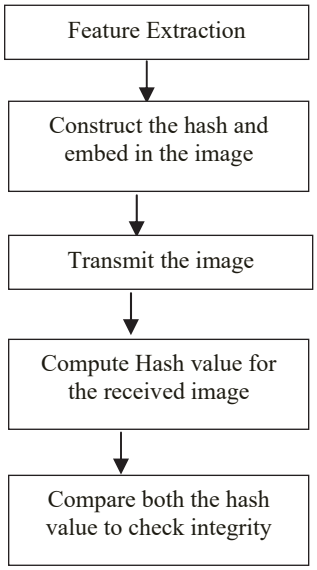

Figure 2. General method of hash based authentication

II. RELATED WORK

Watermark based methods:

Shamir's two-out-of-three threshold secret sharing scheme [9]

The image is divided into four parts of equal size. Out of this, two blocks are randomly picked and grouped and their average pixel values are calculated. This is used as recovery message. The recovery message is split into three shares and distributed separately. If the image is tampered the invalid blocks can be recovered if any of the two shares can be retrieved.

Improvements can be made to this method as the image processing operations such as cropping, compression, and contrast adjust, etc., is recognized as a kind of attack.

Discrete wavelet transform method [7]

The 2D wavelet decomposition is performed for the host image. Two keys are used to generate a binary watermark and embedded into the image. The recovery data is extracted from the important visual information represented by the low-frequency components and this information is embedded into the multi-resolution sub-bands. In this method only the erroneous wavelet coefficients are recovered and other coefficients are left unchanged.

This method detects and localizes malicious attacks effectively yet tolerates mild modifications such as JPEG compression and channel additive white Gaussian noise AWGN. But some of the subtle distortion of the tampered image could not be detected is still an issue for detection efficiency and recovery capability.

Dual Watermark Technique [6]

In this method two watermarks are used. The first watermark is the digest image that is produced using DCT coefficients, then it is encoded using arithmetic coding and it is compressed. An Error Correcting Code (ECC) is encoded to the original image. The second watermarking contains the recovery information that is embedded in the second decomposition level of the Integer Wavelet Transform IWT using sub-band. The recovery is performed using Inverse Discrete Cosine Transform (IDCT). This method is able to resist large modification and is robust to noise insertion.

Block truncation coding compression technique [8]

In this method the authentication data and the recovery data is embedded into the least significant bit (LSB) and the second LSB of the spatial domain. Variance values for the Red, Green, and Blue components using only the six most significant bits (MSBs) of all pixels in the block is computed and this data is used as authentication watermark.

The recovery data is formed by block truncation code compression technique. The grayscale image block is decomposed to one binary bitmap image and two quantization levels that can be used for recovery.

Sharing block information method [5]

The image is separated into blocks and the block information is shared to two other blocks. All index of these blocks are marked in the original table. A Look up Table block is obtained that is separated into upper half and lower half. Then picking up one block from each part, and giving them a partner relationship, the top five bits of MSB are extracted from the block and its partner along with protection and verification code to form the watermark. The 12-bit watermark is embedded in the LSB of block and its partner block. The dilation algorithm is used for the invalid regions, and defines the result as a new invalid region. An invalid block can be recovered using the 12-bit watermark from the partner block or by using image inpainting. This method is used to detect large area tampering.

Adaptive encoding [2]

The image is divided into blocks of 2x2 pixels and the RGB color space is converted to YCbCr and the luminance and chromatic channels are used for better image analysis. Different encoding schemes are applied to the image blocks. The intensity and texture feature of four pixels are recorded using the codebook.

The four pixels are encoded using difference codebooks. For each Cb block, the mean of four Cb pixels is calculated. A binary map shows the position of the tampered blocks, after localizing the tampered blocks, their three channels, RGB, will be recovered by using the table lookup process in which the three YCbCr channels can be decoded for recovery. This technique is able to identify and localize image tampering, while preserving high quality for both watermarked and recovered images.

Hash based methods:

Rehashing Model [10]

This method takes two pixels per unit, and one pixel of the unit embeds hash indicator table information of itself and constructs and Hash address Table, it uses the locations of pixels as the keys of hash functions. The other pixel embeds recovery data of another unit. This method is used to check the authenticity of color and monochrome images. For a color image, convert the color image from RGB color space to YUV color space. In the image recovery phase, we must convert the color image from YUV color space to RGB color space. The proposed scheme uses average intensity as a feature and the least significant bit (LSB) plane for watermark embedding.

This method has good performance in tamper location and allows image recovery with an acceptable visual quality when there was up to 50% content tampering.

Robust Hashing Method using Zernike Moments [11]

This method is used to detect image forgery operations such as insertion, deletion of areas, replacement of objects, and abnormal color modifications. It uses global and local features to form the hash value. The global features represent the representing luminance and chrominance characteristics of the image based on Zernike moments. For local features the position and texture information of salient regions are used. For feature extraction and hash construction secret keys are used. The hash of a test image is compared with that of a reference image. This method locates forgery the forged area and finds the type of forgery by decomposing the hashes.

Ring partition method [12]

This method incorporates a ring partition and invariant vector distance to image hashing algorithm for enhancing rotation robustness. The image hashing is done in a four-phase procedure. Input image is first pre-processed to generate a normalized image for stable feature extraction. The normalized image is divided into different rings which are kept unchanged after image rotation. Further, the statistical feature from the uniform color space, i.e., CIE L*a*b* color space are extracted from image rings. The Euclidean distance between vectors of these perceptual features that are invariant to commonly used digital operations of images such as JPEG compression, brightness/contrast adjustment and gamma correction helps in making image hash compact. This type of hashing method can resist commonly-used digital operations to images, including rotation with any angle, and be sensitive to visual content changes.

In this type of hashing based authentication system recovery feature is not implemented. So further research work can be taken create an optimized hash based recovery system.

III. CONCLUSION

In recent times, image authentication techniques gained great attention due to the large number of image transmissions and its importance for a large number of multimedia applications. To protect the authenticity of multimedia images, several approaches have been proposed. The aim of this paper is to present a survey of emerging techniques for authentication of images, detecting and locating the tampered areas, and reconstruction of images. Various watermarking and hashing techniques have been discussed that are robust against different desired image processing operations.

Research on image hashing is still under way. In future, studies can be conducted regarding the capability of tamper localization and content recovery using new techniques of image hashing and efficient hashing algorithms can be developed.

REFERENCES

[1] Che-Yen Wen, Kun-Ta Yang, Image authentication for digital image evidence, Forensic Science Journal 2006.

[2] Chun-Hung Chen, Yuan-Liang Tang, and Wen-Shyong Hsieh, Color Image Authentication and Recovery via Adaptive Encoding Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2014.

[3] Fridrich J, Goljan M, Protection of digital images using self-embedding. In: Proceedings of the symposium on content security and data hiding in digital media, 1999.

[4] Hai Tao, Li Chongmin, Jasni Mohamad Zain, Ahmed N. Abdalla, Robust Image Watermarking Theories and Techniques: A Review Journal of Applied Research and Technology Volume 12, Issue 1, February 2014.

[5] Hao-Chun Wang, Wei-Ming Chen, Ping-Yi Lee, Image Tamper Detection and Recovery based on Dilation and Chaotic Mixing, Computer Science and Information Technology 3(4): 127-132, 2015.

[6] Jose Antonio Mendoza Noriega, Brian M. Kurkoski, Mariko Nakano Miyatake, and Hector Perez Meana, Image Authentication and Recovery Using BCH Error-Correcting Codes, International Journal Of Computers, Issue 1, Volume 5, 2011.

[7] Min-Jen Tsai, Chih-Cheng Chien, Authentication and recovery for wavelet-based semifragile watermarking, Optical Engineering 476, 067005 June 2008.

[8] Shu-Chien Huang and Ching-Fen Jiang, A color image authentication and recovery method using block truncation code embedding, Journal of Marine Science and Technology, Vol. 20, No. 1, pp. 49-55 (2012).

[9] Shu-Fen Tu, Ching-Sheng Hsu & Fu-HsingWang, Application of Threshold Secret Sharing to Image Authentication and Recovery, The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 4, September-October 2013.

[10] Wan-Li Lyu, Chin-Chen Chang, Feng Wang, Image Authentication and Self-Recovery Scheme Based on The Rehashing Model, Journal of Information Hiding and Multimedia Signal Processing, Volume 7, Number 3, May 2016.

[11] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Robust Hashing for Image Authentication Using Zernike Moments and Local Features, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[12] Zhenjun Tang, Xianquan Zhang, Xianxian Li, and Shichao Zhang, Robust Image Hashing With Ring Partition and Invariant Vector Distance, IEEE Transactions on Information Forensics And Security, Vol. 11, No. 1, January 2016.