International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 08 | Aug-2016 www.irjet.net p-ISSN: 2395-0072

A Review On Tamper Detection In Watermarked Image.

Revathy S[1], Gopu Darsan[2]

[1]Revathy S M-tech Research scholar, Department of computer science, Sree Buddha College of Engineering,kerala,India
[2]Gopu Darsan Assistant professor, Department of computer science, Sree Buddha Collegeof Engineering,kerala,India

---

Abstract - *Watermark is an invisible signature embedded inside an image to show authenticity or proof of ownership. Watermark technique have been widely applied in various fields to protect the image against tampering. Therefore watermark algorithm have been developed to discover the tampered area and recover the lost information. This survey include source coder, channel code parity bit and check bit. Watermark technique aim to accomplish the task of tamper localization and error concealment. To easy use and analysis on computers, analog images are transformed to digital file format by digital encoding techniques.*
Digital image watermarking is an information hiding technique that embeds watermark into the host image for copyright protection or integrity authentication. In general, digital image watermarking can be classified into different watermarking technics. Fragile watermarking is used for both authentication and localization of tampetered zone. An appropriate design of channel code can protect the reference bits against tampering. The technique work by dividing an image into blocks and watermarking each block with a transparent, robust watermark that sensitively depends on a secret key.

***Key Words*: Image watermarking, fragile watermarking , image tampering protection, self-recovery, SPIHT, RS channel codes, prime fields.**

1.INTRODUCTION *(Size 11 , cambria font)*

Image processing is a method to convert an image into digital form and perform some operations on it. Input is image, like video frame or photograph and output may be image or characteristics associated with that image. Image Processing forms core research area within engineering and computer science disciplines too. Image processing basically includes the following three steps.

1)Importing the image from any source

2)Analyzing the image which includes data compression and image enhancement

3)Output is the last stage in which result can be altered image. Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. Multimedia security address the problem of digital watermarking, data encryption, authentication and digital rights managements. Multimedia security provide content based protection. The authenticity and integrity of the digital images cannot be judged just by the human eyes. The digital image authentication watermarking technology, which is used to detect and locate of the tampered regions. Hash of the original image is used to protect it against malicious modifications. Then hash of the output is calculated and receiver declare it as the same if the obtained value and calculated value are the same. A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection. Modifications to an original work that clearly are noticeable. Also fragile watermark can used to locate tampered zone and protect against malicious modifications. Fragile watermark are designed for binary images, jpeg compressed images, colored images.

Self recovery in watermark is divided in to two : checkbit and reference bit. Check bit are used to localize the tampered block and reference bit are used to restore the original image in tampered area. Source coding and channel coding technique is used in this paper. The source coding technique is used to reduce the size of the information being transmitted and coserve the available bandwidth. It reduces redundancy. The channel coding technique is used to reduce the error during transmission of data along the channel from the source to destination and also add redundancy to data. SPIHT method provides good image quality, high PSNR. It is optimized for progressive image transmission and provide fast encoding and decoding. It provide efficient combination with error protection.

SPIHT is an image compression algorithm that aims exploit the inherent similarity across the sub bands in wavelet decomposition of an image. Wavelet transformation has become a most important and powerful tool of signal representation. Wavelet are used for image processing and compression because of low computational complexity of separable transforms. Application of wavelet transform are image compression , edge detection and noise removal. A parity bit or check bit is a bit added to the end of a string of binary code that indicate whether the number of bits in the

string with the value one is even or odd. Parity bit are used as one of the simpliest error correcting code. If parity bit is odd then any group of bit that arrive with an even number of ones must contain an error. All literature papers give information about different watermarking technique permutation along with source coder and channel coder is not specified. So the tamper detection become more complicated. SPIHT algorithm provide the image with more clarity Digital image tampering detection aims at verifying the authenticity of digital images without any a prior knowledge on the original images. Memory requirement is high and processing of robustness is less in previous techniques.

2. LITERATURE REVIEW

Jiri Fridrich [1] has proposed a method of watermarking technique for tamper detection in digital images. By comparing correlation values from different portions of the image, the technique enables us to distinguish malicious changes, such as replacing / adding features from nonmalicious changes resulting from common image processing operation. The watermarking method is a frequency based spread spectrum technique. To achieve a continuous dependency on the image, we propose a special bit extraction procedure that extracts bits from each block by thresholding projections onto key dependent random smooth patterns. One of the first techniques used for detection of image tampering was based on inserting check-sums into the least significant bit (LSB) of image data. Walton proposes a technique that uses a key-dependent pseudorandom walk on the image. In this paper a technique is describe that uses a robust watermark in larger blocks. To prevent unauthorized removal or intentional distortion, the watermark must depend on a secret key S (camera's ID), block number B, and on the content of the block cameras has its own specifics. In one possible scenario, a special tamper-proof watermarking chip inside a digital camera will watermark the image data before it is stored on camera's memory. the total memory requirements are approximately determined by the number of pixels in two blocks plus the length of the spread spectrum signal. As the pixel increases memory requirement also increased.

Meng Chen, Yefeng Zheng, andMinWu [2] has proposed a set of classification-based block concealment schemes, including receiver-side classification, sender-side attachment, and sender-side embedding. The classification-based approach also helps us achieve a better tradeoff between the concealment quality and the computation complexity on the receiver side. The classification in the proposed new framework of error concealment can be done either on the receiver side or on the sender side. And determine which candidate concealment is better for corrupted block. support vector machine (SVM) classifiers, is adopted as they often exhibit good generalization performance. The linear SVM determines a linear discriminant function that gives the maximum separation margin between the two classes of training data. sender-driven perspective to provide perfect classification information to a receiver through attachment or embedding, and thus further enhance the error concealment performance. This paper take great effort in concealing corrupting the block but error concealing cannot be reduced. Sujoy Roy and Qibin Sun [3] has proposed an image hashing approach that is both robust and sensitive to not only detect but also localize tampering using a small signature. The amount of information in the hash about the original should be as large as possible. The goal of the hashing method is to verify the authenticity of the query. Only allowably modified images are declared authentic. Tampered or distinct images are declared non-authentic. Image hashing method consists of two steps:

(1) hash generation and

(2) verification.

For hash generation, a set of features is extracted from the image and a function maps them to a bit sequence. Lack of content information as part of the hash also leads to high false positive detection error. A clear disadvantage in using watermarking is the need for distorting the content. Search complexity and rate of noise is high. Min Vu and Bede Lui [4] propose a data embedding method for image authentication based on table look-up in frequency do-main. Simple features are embedded invisibly in the marked image, which can be stored in the compressed form. Fragile watermarking is a technique to insert a signature for image authentication. The signature will be altered when the host image is manipulated. An effective authentication scheme should have some features:

1. To be able to determine whether an image has been altered or not

2. To be able to locate any alteration made on the image

3.To be able to integrate authentication data with host image rather than as a separate data

4. The embedded authentication data be invisible under normal viewing conditions

5. To allowthe watermarked image be stored in lossy compression format.

A new authentication scheme by embedding a visually meaningful watermark and a set of simple features in the frequency domain of an image via table look-up. This scheme can be applied to compressed image using JPEG. The authentication data we embed in an image consists of a visually meaningful binary pattern and some content features. The scheme can detect tampering of the marked image and can locate where the tampering has occurred. Detect the tampering only in the marked area.

Chun-Shien Lu, Shih-Kun Huang, Chwen-Jye Sze, and Hong-Yuan Mark Liao[5] a novel image protection scheme called "cocktail watermarking" is proposed in this paper. Cocktail watermarking scheme is remarkably effective in resisting various attacks. A commonly suggested method is to insert watermarks into original information so that rightful ownership can be declared. This is the so-called

watermarking technique. The proposed cocktail watermarking scheme can embed watermarks firmly and make them hard to remove. This paper propose cocktail watermarking scheme, including encoding and decoding, watermark modulation is an operation that alters the values of selected transformed coefficients using every selected coefficient's corresponding watermark value. The values of the two watermarks are drawn from the same watermark sequence. The difference is that they are embedded using two different modulation rules: positive modulation and negative modulation. If a modulation operates by adding a negative quantity to a positive coefficient or by adding a positive quantity to a negative coefficient , then we call it "negative modulation." Otherwise, it is called "positive modulation". The proposed cocktail watermarking technique is that it can be applied to other types of media such as audio or video. The robustness issue of watermarking addressed in this paper, the rightful ownership deadlock problem the capacity problem and the public-key detection problem will be important issues.

Ashwin Swaminathan, Min Wu and K. J. Ray Liu[6] this paper introduces a new methodology for the forensic analysis of digital camera images. The proposed method is based on the observation that many processing operations, both inside and outside acquisition devices, leave distinct intrinsic traces on digital images, and these intrinsic fingerprints can be identified and employed to verify the integrity of digital data. The intrinsic fingerprints of the various in-camera processing operations can be estimated through a detailed imaging model and its component analysis. The presence or absence of watermarked image result in authenticity. Steganalysis methods have been proposed to identify the presence of hidden data in multimedia. Steganography is the art of secret communication where the hidden information is transmitted by embedding it on to the host multimedia. The proposed formulation is based on the observation that each in-camera and postcamera processing operation leaves some distinct intrinsic fingerprint traces on the final image. We characterize the properties of a direct camera output using a camera model, and estimate its component parameters and the intrinsic fingerprints Min Wu and Bede Liu [7] has proposed that images in which the pixels take value from only a few possibilities, hiding data without causing visible artifacts becomes more difficult. To assign flippability score manually according only to neighborhood patterns has the shortcomings that the storage of every pattern can be huge and that such a fixed assignment does not offer flexibility for binary images with different characteristics. The smoothness is measured by the horizontal, vertical, and diagonal transitions in a local window. Directly encoding the hidden information in flippable pixels may not allow the extraction of embedded data without the original image. Regarding the uneven embedding capacity in a binary image. A detector has to know exactly how many bits are embedded in each block. Any mistake in estimating the number of embedded bits is likely to cause errors in decoding the hidden data for the current block. The scores are used to determine which pixels to flip with high priority during the embedding process.

Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng [8], proposes two novel self-embedding watermarking schemes based upon a reference sharing mechanism, in which the watermark to be embedded is a reference derived from the original principal content in different regions and shared by these regions for content restoration. After identifying tampered blocks, both the reference data and the original content in the reserved area are used to recover the principal content in the tampered area. 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 the second scheme,the host content is decomposed into three levels, and the reference sharing methods with different restoration capabilities are employed to protect the data at different levels. One class of the fragile watermarking approaches is to divide a host image into small blocks, and embed the fragile watermark into these blocks. Since image tampering destroys matching between the content and the watermark in the corresponding blocks, the tampered blocks can be revealed. It is possible that data derived from the tampered pixels are the same as the watermark so that modification to these pixels is not directly detectable. After obtaining an estimate of the modification strength, distributions of the tampered and original pixels are used to accurately locate the tampered pixels. In some self-embedding watermarking schemes, the embedded watermark, or a part of it, is a representation of the host image content so that the original content in the tampered area can be restored. Data representing the principal content in a region are always hidden in a different region within the image. If both regions are tampered, restoration will fail. It is called *tampering coincidence* problem. On the other hand, when a part of data for image transmission is lost due to poor channel condition, the error concealment techniques capable of displaying acceptable images are desired. Some watermarking approaches with content restoration capability are free of the tampering coincidence problem. However, they do not work when the tampered area is too extensive. The tampered areas can still be located and the watermark data extracted from the reserved regions can be used to restore the host image without any error. A self-embedding scheme capable of restoring the watermarked image from a tampered version is proposed. The five MSB of all pixels in the host image are kept unchanged, while the three LSB of all pixels are replaced with reference data and hash data. A hierarchical self-embedding watermark scheme based upon the reference sharing mechanism is proposed. The reference sharing mechanism does not suffer from the tampering coincidence problem. Paper proposed two self-embedding watermarking schemes. The first scheme is capable of recovering all the original data in the 5MSB layers and retrieving the legitimate watermarked image when the tampering rate is no more than 24%. The second one uses the reference sharing methods with different restoration capabilities to protect the content data in different levels so

that a better restored result can be obtained from a tampered version with less fake content.

Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng [9], The embedded watermark data for content recovery are calculated from the original discrete cosine transform (DCT) coefficients of host image and do not contain any additional redundancy. When a part of a watermarked image is tampered, the watermark data in the area without any modification still can be extracted. If the amount of extracted data is large, we can reconstruct the original coefficients in the tampered area according to the constraints given by the extracted data. Two watermarks method are proposed from the wavelet coefficients of the approximation sub-band, the first mark used for tampered area localization and the second one for content recovery. To deal with the tampering /missing coincidence problem, a hierarchical mechanism combined with an exhaustive search method for retrieving the original most significant bits (MSB) is introduced. As long as the tampering is not too severe, the watermark data extracted from the reserved area can provide sufficient information to retrieve the principal content of the tampered areas. When the tampered area is small, a lot of watermark data can be extracted from the reserved area, but they do not result in a better recovery quality. When some tampered pixels cannot be recovered from the watermark data due to tampering/missing coincidence, the receiver may estimate their values according to the original or recovered neighbor pixels. Watermarking scheme with flexible recovery quality, which avoids both the tampering coincidence and the watermark-data waste problems. The tampered-block localization works well since any modification caused by image processing operations will result in a "tampered" decision.

Xinpeng Zhang and Shuozhong Wang[10], proposes a novel fragile watermarking scheme capable of perfectly recovering the original image from its tampered version. Content replacement may destroy a portion of the embedded watermark data, as long as the tampered area is not too extensive, the original image information can be restored without any error. While robust watermarks can be used for ownership verification, fragile watermarks are intended for checking integrity and authenticity of digital contents. If the image has been changed, the image content and the watermark corresponding to the tampered blocks cannot be matched so that the tampered blocks are detected. Block-wise fragile watermarking schemes can only identify tampered blocks, but not the tampered pixels. some watermarking approaches that can reconstruct the original content in the tampered areas have been proposed. As a special data-hiding technique, a number of lossless embedding methods can insert secret message into the host image in some invertible manner so that the original content can be perfectly restored after the hidden message is extracted. The original content in most reserved area can be directly recovered through an inverse DE operation. By folding the hash-bits as the check-bits, the amount of data to be embedded for tampered-block localization is saved, and the tampered blocks can be identified by introducing a statistical mechanism. One problem with the method is the relation between the watermark-induced distortion and the capability of image restoration.

3. CONCLUSIONS

We proposed a watermarking scheme to protect images against tampering. Watermarks are embedded once in the hiding process and it can be blindly useful for different applications in the detection process. Hash of the original image is calculated which protect against malicious modification. Different watermarking techniques are introduced to protect against tampering.

REFERENCES

[1] J. Fridrich, "Image watermarking for tamper Proc. Int. Conf. Image Process. (ICIP), vol. 2. Oct. 1998, pp. 404–408.

[2] M. Chen, Y. Zheng, and M. Wu, Classification–based spatial error concealment for visual communications, ppl. Signal Process., vol. 2006, pp. 1–17, Jan. 2006, Art. ID 13438.

[3] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," in Proc. IEEE Int. Conf. Image Process. (ICIP), vol. 6. Sep./Oct. 2007, pp. VI-117–VI-120.

[4]M. Tagliasacchi, G. Valenzise, and S. Tubaro, Hash-based identification of sparse image tampering, IEEE Trans. Image Process., vol. 18, no. 11, pp. 2491–2504, Nov. 2009.

[5] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," IEEE Trans. Multimedia, vol. 2, no. 4, pp. 209–224, Dec. 2000.

[6] A. Swaminathan, M. Wu, and K. J. R. Liu, Digital image forensics via intrinsic fingerprints, IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[7] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[8] X. Zhang, S. Wang, Z. Qian, and G. Feng, Reference sharing mechanism for watermark self-embedding," IEEE Trans. Image Process., vol. 20, no. 2, pp. 485–495, Feb. 2011.

[9] X. Zhang, Z. Qian, Y. Ren, and G. Feng, Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.

[10] X. Zhang and S.Wang, "Fragile watermarking with error-free restoration capability," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1490–1499, Dec. 2008.