DETECTION OF TAMPERING IN COLOR IMAGE

Manoj Nagar [1], Pinky Brahmbhatt [2], Dr. M. Sarada Devi [3]

[1] *PG Student, Department of ECE, L. D. College of Engineering, Ahmedabad, Gujarat, India*

[2] *Associate Professor, Department of ECE, L. D. College of Engineering, Ahmedabad, Gujarat, India*

[3] *Principal, Department of ECE, Narnarayan Shastri Institute of Technology, Jetalpur, Gujarat, India*

---***---

Abstract - *In the last few years there is a tremendous development in the area of high quality digital camera technology. So our life is full of the use of these digital images. However now a days there are lot of software (for example Photoshop, Photoscape, Photoplus and Picasa etc.) that can be used to modify these digital image. Therefore we cannot use these images as a proof or evidence. Therefore detection of tampering in image is important issue for forensic department. In this paper I have presented a method which is based on digital watermark for detection of tampering in image. In this method I have first embed a digital watermark in Least Significant Bit of pixel which is computed from digital content of image. My proposed algorithm consists of two parts. First is generation and embedding of digital watermark and second is detection of tampering and localization.*

Key Words: Digital watermarking, Spatial domain, Frequency domain, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT).

1. INTRODUCTION

Detection of tampering means showing the alteration which is not easily observable. In the last few years, malicious attackers generally try to alter meaningful information of an image so that meaning of image is changed. Watermarking methods are desirable because these methods protect the integrity of image and provide authentication. Therefore, watermarking method for detection of tampering has much attention.

In Digital watermarking method additional data is added into the digital content of image in such a way that distortion caused by embedding data remains imperceptible. The additional data which is embedded is called "Digital Watermark". Digital watermarking method is used for tamper detection and recovery. Embedding reference pattern (watermark) into image [1], the problem of integrity and authentication of image is solved and attracted the interest of researchers. Many watermarking methods can determine that image has been modified or not and some methods can localize the modified areas and some methods has capability to recover tampered areas [2-6]. Generally there are three types of question arises related to detection of tampering in image [8].

- Work altered in any way?
- Work altered significantly?
- Which parts of the Work altered?

There are many methods exists for giving the answer of above question for example first question can be answered by using cryptographic signature to the content of image. Even without using cryptographic signature tampering can be detected using detection modification to the images, identifying anomalies such as variation in the shadow, missing shadow, discontinuities in background and variation of lighting condition etc. But there are some potential benefits are using watermark for tampering detection. First, watermark does not need to store as a separate, associated metadata such as cryptographic signature. Second, watermark undergoes same transformation as the content of image in which watermark is embedded.

2. LITERATURE SURVEY

There are three level of tampering detection methods [9]. Low Level: This level method has no semantic information. This level method generally uses statistical property of image pixels for example DCT coefficients. Middle Level: This level method uses some semantic information. For example inconsistency of different lighting conditions and splicing etc. High Level: This level method has fully semantic information. For example image does not have semantic meaning in which toothbrush is used for hair setting.

The detection of tampering in image can be done using two techniques - blind techniques and non-blind techniques. Blind tampering[15-18] detection methods are based on the fact that they do not require original image or its representation for the purpose of tampering detection whereas Non-blind [10-14] tampering detection method requires original image or its representation for the purpose of the tampering detection techniques that do not require the original image for the purpose of tampering detection. Blind tampering detection methods are also called as "Passive" methods and non-blind tampering detection methods are also called as "Active" methods.

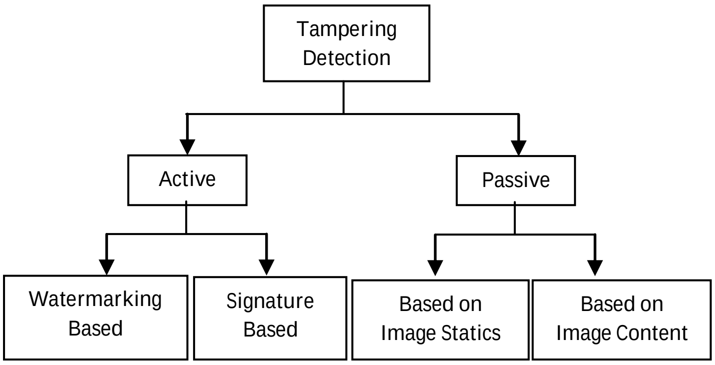


Fig -1: Different method of tampering detection

Active tampering detection methods are generally considered as watermarking methods. This method can be applied in two domains, spatial and frequency domain. In Spatial domain techniques we directly work with image pixels, these techniques are Least Significant Bit, Predictive coding techniques, Correlation based techniques and Patchwork techniques. In LSB technique watermark in embedded into LSB of pixels of image [19]. Predictive coding technique takes the advantage of correlation between adjacent pixels [20]. In correlation based technique random noise is added into image and at the receiver if correlation between image and noise is above threshold then image is considered as tampered image [21]. In Patchwork technique image is divided into two parts then a operation is applied into both parts in opposite direction and if image is tampered it will not satisfy operation on both parts [22]. In Frequency domain techniques we work with transform domain of image, these techniques are Discrete Cosine Transformation, Discrete Wavelet Transformation and Discrete Fourier Transformation. In all these techniques watermark is embedded into transformation domain [23-25].

Passive tampering detection methods are based on Detecting splicing by visual cues, Detection of inconsistencies in local noise, Cyclostationary Approach etc. In detection of splicing by cues method abnormality present at boundary of object is detected to detect tampering [26]. Detection of inconsistencies in local noise method various noise levels in image is used to detection tampering [27]. Image has hidden cyclostationary property which is transformed by scaling therefore cyclostationary properties can be used to detect tampering [28].

3. PROPOSED ALGORITHM

My proposed algorithm consists of two stages. First stage is Self Embedding Stage which consists of watermark generation and watermark embedding process. Second stage is authentication stage which consists of watermark extraction and authentication and localization using extracted watermark. In first stage watermark can be generated with the help of DCT or DFT coefficient and is embedded into LSB of image because change in only LSB of pixel doesn’t make significant change. In second stage same method watermark generation is used for watermark extraction and is compared with LSB to detect tampering in the image. General scheme of proposed algorithm is shown in fig. 2.

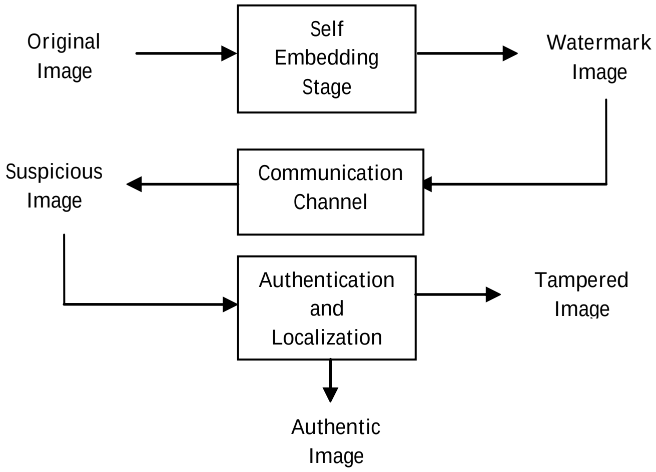


Fig -2: General Scheme of proposed algorithm

3.1 Self Embedding Stage:

Self embedding stage is shown in the figure. Following stages are taken for this stage as shown in the Fig. 3.

(1) Image is divided into three colour stacks of red, green and blue colours.
(2) Apply all below step to all three colour component.
(3) Divide image into blocks of 8X8 or 4X4 or 2X2.
(4) Take DCT or DFT without using LSB.
(5) Generate watermark based on following equation.
$W_k = 0$ if transformation coefficient is even
$W_k = 1$ if transformation coefficient is odd.
(6) Apply Special Lookup Table and Marking Key.
(7) Embedded watermark into LSB of pixels of image.
(8) Combine all the block and colour component to form complete image.

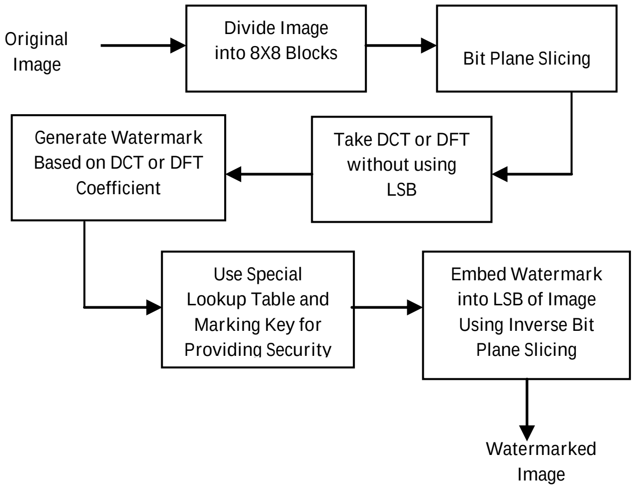

Original Image
Divide Image into 8X8 Blocks
Bit Plane Slicing
Generate Watermark Based on DCT or DFT Coefficient
Take DCT or DFT without using LSB
Use Special Lookup Table and Marking Key for Providing Security
Embed Watermark into LSB of Image Using Inverse Bit Plane Slicing
Watermarked Image

Fig -3: Flow graph of Self Embedding Stage

3.2 Authentication and Localization Stage:

Authentication and localization stage is shown in the figure. Following stages are taken for this stage as shown in the fig. 4.

(1) Image is divided into three colour stacks of red, green and blue colours.
(2) Apply all below step to all three colour component.
(3) Divide image into blocks of 8X8 or 4X4 or 2X2.
(4) Take DCT or DFT without using LSB.
(5) Extracted watermark based on following equation.
$W_k = 0$ if transformation coefficient is even
$W_k = 1$ if transformation coefficient is odd.
(6) Apply Special Lookup Table and Marking Key.
(7) Compare the extracted watermark with LSB of image.
(8) If both are equal then image is authentic and if both are unequal then image is unauthentic then highlight the tampered block.
(9) Combine all the blocks and colour component to form complete image.

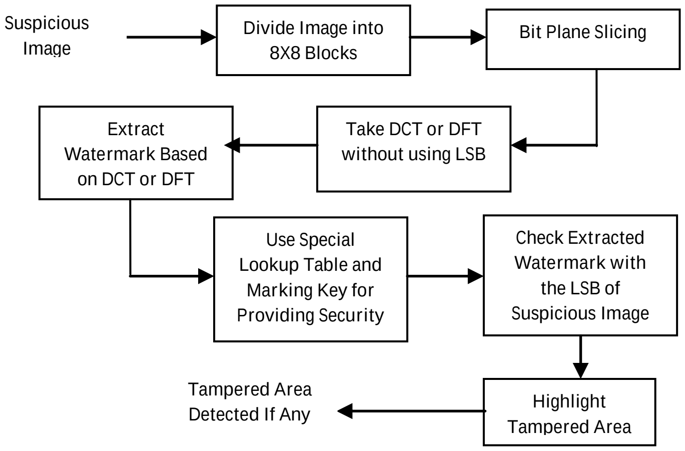
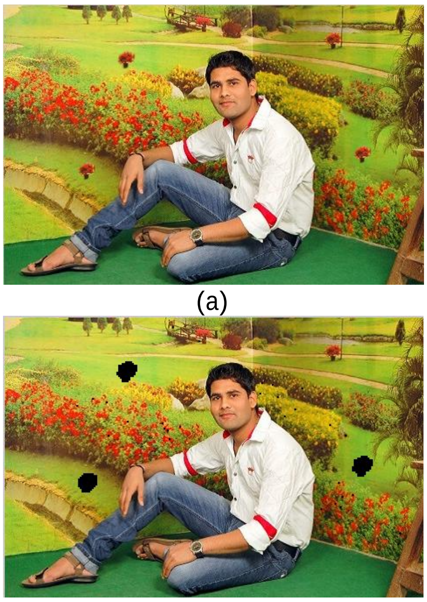

Suspicious Image
Divide Image into 8X8 Blocks
Bit Plane Slicing
Take DCT or DFT without using LSB
Extract Watermark Based on DCT or DFT
Use Special Lookup Table and Marking Key for Providing Security
Check Extracted Watermark with the LSB of Suspicious Image
Highlight Tampered Area
Tampered Area Detected If Any

Fig -3: Flow graph of Authentication and Localization Stage

4. EXPERIMENTAL RESULT

In the experiment we have applied algorithm to 100 images to check its efficiency. we have applied different types of attack on the images. The first attack performed on image is collage attack. The collage attack is performed by copying one region and pasting that into another region of watermarked image. The second type of attack performed on image is deletion attack in which some part of image is deleted to hide information.

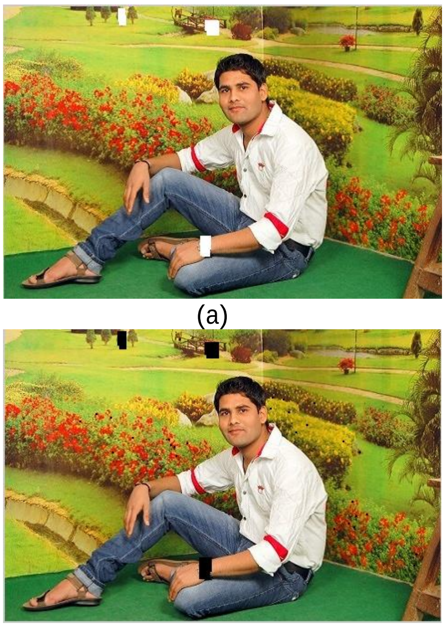
Collage Attack experimental result: Fig. 5 illustrating the collage attack on Colour image of me in which there is copy and paste of some part of the image inside the image. Figure illustrating proposed method exactly detects the tampered and localize areas.


(a)

(b)

Fig -4: Collage Attack (a) Tampered Image (b) Tampered area detected and localization

Deletion Attack experimental result: To check good experiment results, deletion attack is performed on different parts in different size on the same image. Fig.6 illustrates power of this algorithm to detect this type of tampering. Tampered part is detected and localize as shown in figure.


(a)

(b)

Fig -5: Deletion Attack (a) Tampered Image (b) Tampered area detected and localization

5. CONCLUSION

In this paper we presented an efficient method for detection of tampering. This algorithm has 3 level efficient check of each block because it checks each block for three colour component. We have performed different types of attack on the image to check efficiency of algorithm. The experiment result shows that proposed algorithm has high efficiency and accurately.

REFERENCES

[1] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[2] T.-Y. Lee, S.-D. Lin.: Dual Watermark for Image Tamper Detection and Recovery. In Pattern Recognition 41 pp. 3497--3506. (2008).

[3] Luis Rosales-Roldan, Manuel Cedillo-Hernández, Mariko Nakano-Miyatake, Héctor Pérez-Meana: Watermarking-based Tamper Detection and Recovery Algorithms for Official Documents. Electrical Engineering Computing Science and Automatic Control (CCE), 2011 8th International Conference on (2011).

[4] Song Qiang, Zhang Hongbin: Image Tamper Detection and Recovery Using Dual Watermark. Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on (2010).

[5] Surya Bhagavan Chaluvadi, Munaga V. N. K. Prasad: Efficient Image Tamper Detection and Recovery Technique using Dual Watermark. Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress (2010).

[6] P.-L. Lin, P.-W. Huang, A.-W. Peng.: A Fragile Watermarking Scheme for Image Authentication with Localization and Recovery. In IEEE Sixth International Symposium on Multimedia Software Engineering (2004).

[7] P.-L. Lin, C.-K. Hsieh, P.-W. Huang.: A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery. In: Pattern Recognition (2005).

[8] I.J. Cox, M.L. Miller, and J.A. Bloom Digital Watermarking, Morgan Kaufmann Publishers, 2002.

[9] Wei Wang, Jing Dong, and Tieniu Tan, A survey on passive-blind image forgery by doctor method detection, International Conference on Machine Learning and Cybernetics (2008).

[10] Pragya Jain , Anand S. Rajawat, Fragile Watermarking for Image Authentication: Survey, International Journal of Electronics and Computer Science Engineering (2012).

[11] Babak Mahdian and Stanislav Saic, Detection and Description of Geometrically Transformed Digital Images, Media Forensics and Security. Edited by Delp, Edward J., III; Dittmann, Jana; Memon, Nasir D.; Wong, Ping Wah. Proceedings of the SPIE (2009).

[12] Babak Mahdian and Stanislav Saic, Using noise inconsistencies for blind image forensics (2009).

[13] Babak Mahdian and Stanislav Saic, A Cyclostationarity AnalysisApplied to Scaled Images, Lecture Notes in Computer Science, 2009, Volume 5864/2009, 683-690, DOI: 10.1007/978-3-642- 10684-2_76.

[14] Zhenhua Qu, Guoping Qiu, and Jiwu Huang, Detect Digital Image Splicing with Visual Cues, Information Hiding: 11th International Workshop (2009).

[15] Mall, V. Shukla, S. ; Mitra, S.K. ; Roy, A.K.: Comprehensive Image Index and Detection of Tampering in a Digital Image. In IEEE Informatics, Electronics & Vision (ICIEV), International Conference (2013).

[16] J. Fridrich, "Robust hash functions for digital watermarking". In IEEE, Information Technology: Coding and Computing, International Conference on, vol. 0, p. 178, 2000.

[17] V. Mall, K. Bhatt, S. K. Mitra, and A. K. Roy, "Exposing structural tampering in digital images" in Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on, March 2012, pp. 1–6.

[18] Wang Jing, Zhang Hongbin: Exposing Digital Forgeries by Detecting Traces of Image Splicing. In IEEE, Signal Processing 8th International Conference (2006).

[19] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[20] K. Matsui and K. Tanaka, "Video-Steganography: How to Embed a Signature in a Picture", in Proceedings of IMA Intellectual Property, Jan. 1994, Vol. 1, No. 1, pp. 187-206.

[21] Chin-Feng Lee, Kuo-Nan Chen. Chin-Chen Chang and Meng-Cheng Tsai, "A Block Feature Correlation Based Image Watermarking for Tamper Detection using Linear Equation". In IEEE, Fifth International Conference on Information Assurance and Security (2009).

[22] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding". IBM systems journal, vol 35, nos 3&4, 1996.

[23] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[24] Preeti Parashar and Rajeev Kumar Singh, A Survey: Digital Image Watermarking Techniques, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 7, No. 6 (2014), pp. 111-124

[25] Vinita Gupta, Mr. Atul Barve, A Review on Image Watermarking and Its Techniques, International Journal of Advanced Research in Computer Science and Software Engineering (2014).

[26] Zhenhua Qu, Guoping Qiu, and Jiwu Huang, Detect Digital Image Splicing with Visual Cues, Information Hiding: 11th International Workshop (2009).

[27] Babak Mahdian and Stanislav Saic, Using noise inconsistencies for blind image forensics (2009).

[28] Babak Mahdian and Stanislav Saic, A Cyclostationarity AnalysisApplied to Scaled Images, Lecture Notes in Computer Science, 2009, Volume 5864/2009, 683-690, DOI: 10.1007/978-3-642- 10684-2_76.

BIOGRAPHIES

Manoj Nagar is Pursuing Master of Engineering from L. D. College of Engineering, Ahmedabad, India. His dissertation topic is DETECTION OF TAMPERING IN COLOUR IMAGE.

Prof. Pinky Brahmbhatt is Associate Professor at L. D. College of Engineering, Ahmedabad, India. She is Pursuing PhD. She has guided number of projects to under graduate and post graduate.

Dr. M. Sarada Devi is Principal of Narnarayan Shastri Institute of Technology, Jetalpur, Gujarat, India. She has guided number of projects to under graduate, post graduate and PhD student.