Digital Image Watermarking Mechanism for Image Authentication, Image Forgery and Self Recovery

Hiral A. Patel[1], Dr. Dipti B. Shah[2]
[1] Sutex Bank College of Computer Applications & Science, Veer Narmad South Gujarat University, Surat, India
[2] G.H.Patel P.G. Department of Comp. Sc. and Technology, Sardar Patel University, VV Nagar, India

Abstract: Digital image modification is now the most common activity in present digital world. Because of the digital image manipulating software, the images are tampered quickly. This type of image forgery becomes common today. The paper briefs the techniques which are applied to modify the images to misguide others like cloning, splicing, retouching. The digital forensic active and passive approaches are also discussed. Moreover the framework for digital image watermarking system is demonstrated to solve tampering issue with the self recovery capability.

Keywords: Tampering Detection, Tampering Localization, Digital Watermarking, Image Authentication, Self Recovery.

Introduction:

Internet is the main source through which the digital documents can easily pass from one location to another. Because of fast data transmission rate, the demand of digital document increases day by day. In court, company, military etc. places also these documents are accepted as legal proof. On other hand, there are many image manipulated computerized software available in the market like Photoshop, Corel draw etc. using which the documents can be easily modified within few seconds. Image forgery means the process of modifying image for presenting as a legal document.

The images are modified for different purpose. Some users modify the image just for enjoyment. Some users intentionally modify the content of the image, this intentional modification is considered as malicious attacks like cloning, splicing, text editing etc. [1]. During digital data transmission, many operations are performed on image where the image is modified but the content or the meaning of the image will be as it is, are considered as non-malicious attacks like filtering, compression, enhancing, sharpening etc.

Because of the image forgery, the images are not considered as reliable source in news papers, magazines, journals, court etc. There is a need to verify the authenticity and integrity of these images. The researcher turned towards this direction and suggested many technologies through which the image is verified and if the image is not authentic then the tampered region can be identified. Many researchers have developed the systems through which the original image can be retrieved back from the tampered image. Digital forensics continuously works under this security issue and tries to develop latest technologies which may help to overcome this issue.

Types of image tampering techniques:

There are many image tampering techniques available:

1. Copy move or cloning: Here only one image is used. One part of the image is copied and it is pasted at one or many places within the same image.
2. Copy paste or copy create: Here the part of one image is copied and it is pasted within another image.
3. Splicing: Two or many images are required to create one new image. From different images different parts are copied and these parts are joined to make a new image. Totally a new story is generated using this technique.
4. Retouching: It is less destructive than other techniques. The feature of the image is modified to make the image more eye-catching. Normally the original face which is available within image is modified to look gorgeous.
5. Cropping: Part of the image is removed from the image which others cannot see.
6. Resizing: When the part of the image is copied and pasted at another location then sometime there is a need to modify the size of the copied part.
7. Blurring: With copy move and copy paste, when the part is pasted at another location then there is need to smooth the border of the object so human eye can’t observe the change. This smoothening effect is possible by applying blur effect to the border.

Digital Image Forensics:

As discussed earlier, the images are tampered therefore it cannot be used as a legal proof. There is a need to develop the electronic security mechanism so the originality of the image can be verified. Researchers started developing digital forensic systems to identify digital tampering. These systems are used for the authentication of digital documents and if the document is not authentic then tried to find out the region where the tampering is done. Even many systems are designed which try to retrieve the original content from the tampered one. There are two different types of protection approaches as shown in Figure.1 used by the researchers [2].

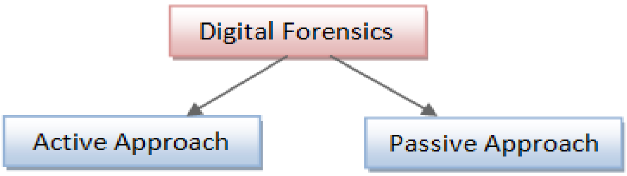

Figure. 1 Digital image forensic approach

1. **Active Protection Approach:**
   With active protection approach, verification code is embedded or attached with the original image so whenever there is a requirement for authentication then the verification code is used to check the originality of the image [3]. Digital watermarking and digital signature are the two active approaches use for digital forgery.
   Digital Signature is generated by encrypting some features of the original image using specific key. This signature always travels with the original image. When there is a need for authentication then digital signature is decrypted using the respective key. Because extra information in form of digital signature is passed with original image increase the size of the image.
   Digital watermarking hides the verification code within the original image means it embeds the watermark within the image using different image processing methods so it can't be observed by the human eye. When there is a need to test the authentication of this image then the embedded watermark is extracted from the image and it is matched with original watermark. If both are same then the image is considered as authentic otherwise it is considered as tampered. Watermark may include the information about the owner or the information about the feature of the image. This watermark can also be helpful to identify the tampered region as well as it helps to retrieve the original content back from the tampered image. The watermarking system can be helpful for authentication, tamper localization as well as for retrieving original content.

2. **Passive Detection Approach**
   In passive detection approach, there is not any requirement of pre-embedding process. Passive detection approach has mainly three categories: Image Acquisition, image storage and image editing. When the image is captured using device like camera then before storing image it performs some operations on it. If the forgery detection is based on this information then it is the part of the image acquisition. JPEG follows lossy compression which adds certain compression patters during image storage. By analyzing this compression pattern stored with image, it is possible to detect forgery. The forgery detection is based on the image editing. It is divided into inconsistency in light, local filtering trace, detection of copy move attack, re-sampling detection, image splicing detection [4, 5]. Researchers work under different image editing techniques. Lots of work is done under the copy-move detection, image splicing detection etc. But the forgery detection for copy move and image splicing etc. using one system is a difficult task in passive detection approach.

Active and passive both approaches have their own strengths and weaknesses. Researchers continuously work under both the approaches to develop the better and better solution to provide security to the digital image from the image forgery.

Digital image watermarking technique:

Digital image watermarking approach hides watermark within the original image which can be extracted whenever required. Using fragile as well as semi-fragile watermarking mechanism, these issues can be solved. The fragile systems don't allow a single bit modification within watermarked image [6]. The semi-fragile systems are designed for content authentication which gives protection to the system from malicious operations where as becomes robust for the non-malicious operations. These systems allow the content preserving operations and finds out the tampering applied on watermarked image.
The general framework for watermarking system is demonstrated in Figure.2.

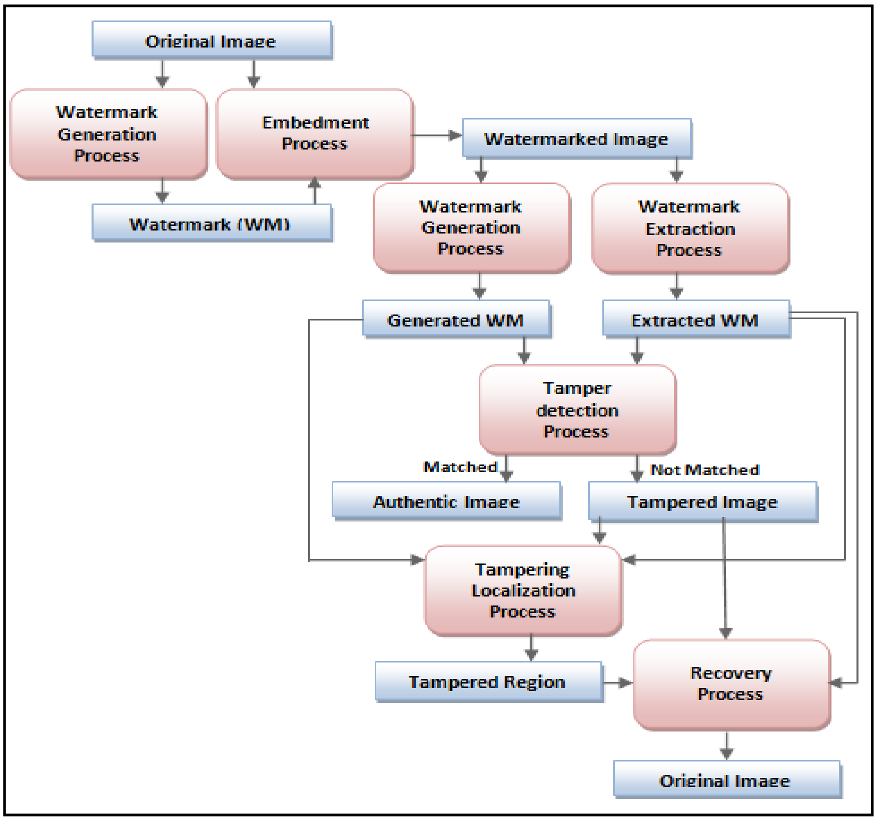

Figure. 2 Framework for watermarking system

The process of each component is discussed as below:

1. **Watermark Generation Process:** Watermark is the most important image for the watermarking system because using it the authentication and integrity issues can be identified. Some researchers use individual watermark image but it is difficult to retrieve original image from the tampered one [6-8]. Other researchers extract the feature of the original image and use it as a watermark which may help to retrieve and to find the tampered location [9-12]. Features can be extracted using methods like DCT, DWT, PCA, SVD, edge detection techniques.
2. **Embedment process:** The generated watermark is embedded within the original image using different image processing techniques in such a way that it can't be observed by the human eye. The watermark is embedded using spatial domain methods like LSB, MSB, SSM or frequency transform domain methods like DFT, DCT, DWT or the hybrid approach [13]of these methods. This watermarked image travels through insecure channel.
3. **Watermark Extraction Process:** The watermark extraction process is required when there is a need to verify the authenticity of the image. By applying the reverse process of embedding, the watermark is extracted from the watermarked image. Some researchers use original image to extract the watermark [14, 15] where as others blindly extract the watermark [3, 9, 11, 12, 13, 16, 17].
4. **Tamper Detection Process:** To test the tampering or authentication, the extracted watermark is used. Also the new watermark is generated from the watermarked image using the same watermark generation process. The extracted watermark and the generated watermark are compared and if both are same then the watermarked image is considered as authentic otherwise it is considered as tampered one.
5. **Tampering Localization Process:** Once the image is found to be tampered then by applying XOR operation, statistical operations, based threshold [7] or clustering of non-matched blocks in between generated and extracted watermark, the tampered region is identified.
6. **Recovery Process:** The extracted watermark is originally generated based on the features of the original image. So the information which is available from this extracted watermark assists to retrieve the original information from the tampered image. Some researchers have embedded another watermark which is used only when there is a need to retrieve the original content [9, 11, 12]. Some have developed system which divides the image into numbers of blocks and then invalid blocks are clustered. All invalid blocks are grouped and then the respective bits are replaced from the watermark [9].

Conclusion:

To solve the issue of image authentication and tampering, the electronic security mechanisms can be used. The image forensic systems can be designed based on active or passive approach. Digital image watermarking and digital signature are the active approaches which transmit extra detail of image. Digital signature can't be useful to retrieve the original data from tampered one. The passive techniques focus on different tampering techniques like either cloning or splicing or retouching etc. But the solution of multiple tampering techniques with one system is difficult with passive approach. The tampering with multiple techniques as well as original image recovery is possible using watermarking system. It is possible to embed one or multiple watermarks within the original image which can be extracted whenever required. Image authentication, tampering and self recovery is possible using digital forensic active watermarking approach. Using Digital Forensic Active approach, it is possible to do image authentication, Image forgery and Self Recovery.

References:

1. Sharma, Deepika, and Pawanesh Abrol. "Digital image tampering–A threat to security management." *International Journal of Advanced Research in Computer and Communication Engineering* 2.10 (2013): 4120-4123.
2. Mary Linda I, K. Shanmugapriya. "Digital Forensics and Image Forgery To Prevent Cyber Attack." International Journal of Pure and Applied Mathematics 116.8 (2017): 229:233.
3. Sathik M. M., and S. S. Sujatha. "Authentication of digital images by using a semi-fragile watermarking technique." International Journal of Advanced Research in Computer Science and Software Engineering 2.11 (2012): 39-44.
4. Lin, Xiang, et al. "Recent advances in passive digital image security forensics: A brief review." *Engineering* (2018).
5. Sadeghi, Somayeh, et al. "State of the art in passive digital image forgery detection: copy-move image forgery." *Pattern Analysis and Applications* 21.2 (2018): 291-306.
6. Gokhale U. M., and Y. V. Joshi. "A semi fragile watermarking algorithm based on SVD-IWT for image authentication." International Journal of Advanced Research in Computer and Communication Engineering 1.4 (2012).
7. Arathi Chitla. "A semi fragile image watermarking technique using block based SVD." International Journal of Computer Science and Information Technologies 3.2 (2012): 3644-3647.
8. Tiwari, Archana, and Manisha Sharma. "An Efficient Vector Quantization Based Watermarking Method for Image Integrity Authentication." Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Springer, Singapore, 2018. 215-225.
9. LV LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." Journal of Theoretical and Applied Information Technology 42.2 (2012): 287-2917.
10. Li Chunlei, et al. "Semi-fragile self-recoverable watermarking scheme for face image protection." Computers & Electrical Engineering on Elsevier (2016).
11. Molina-García, Javier, et al. "Watermarking algorithm for authentication and self-recovery of tampered images using DWT." Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 2016 9th International Kharkiv Symposium on. IEEE, (2016).
12. Chetan, K. R., and S. Nirmala. "Intelligent Multiple Watermarking Schemes for the Authentication and Tamper Recovery of Information in Document Image." Advanced Computing and Communication Technologies. Springer, Singapore, 2018. 183-193.
13. Madduma Buddhika, and Sheela Ramanna. "Content-based image authentication framework with semi-fragile hybrid watermark scheme." Man-Machine Interactions 2. Springer Berlin Heidelberg, 2011. 239-247.
14. Gadhiya, Tushar D., et al. "Use of discrete wavelet transform method for detection and localization of tampering in a digital medical image." IEEE Region 10 Symposium (TENSYMP), 2017. IEEE, 2017.
15. Wang, Na, and Chung-Hwa Kim. "Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD." Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on. IEEE, 2009.
16. Kommini Chaitanya, Kamalesh Ellanti, and E. Harshavardhan Chowdary. "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain."International Journal of Computer Applications 28.3 (2011): 42-46.
17. Ramos, Clara Cruz, et al. "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain." Discrete Wavelet Transforms-Algorithms and Applications. InTech, 2011.