International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Literature Survey on Tampering Detection Feature Extraction

D. Arputha Nancy[1], G. Athisha[2]
[1]*PG Student, Department of ECE, PSNA College of Engineering and Technology, Dindigul, India*
[2]*Professor and HOD, Department of ECE, PSNA College of Engineering and Technology, Dindigul, India*

***Abstract*: In this paper the comparative study of fragile watermarking feature extraction for the particular area to recover the original images. To protect the sensitive image, the fragile watermarking scheme is used for tamper localization and self-recover image .The watermarking feature extraction plays important in security and it addresses the requirements of both safety and non-safety in medical application. The watermarking methods improves the image authentication and provides a way to detect different attacked area of the image. Recently several research and techniques have been implemented for tamper localization accuracy and the Peak signal to noise ratio (PSNR) of self-recovered image. This paper discusses about the various algorithm and transformation proposed for the fragile tampered images.**

***Keywords*: Fragile watermarking, Tamper localization, Authentication, Image Security, Medical Image Security.**

1. Introduction

With the rapid growth of internet technology, illegal copy, transmission and distribution of digital multimedia become an important security issue. This issue motivates for developing a solution for image authentication and copyright protection. Digital watermarking considered as an alternative solution to prevent illegal copy has drawn wide spread attention. The watermark insertion and extraction may be done by the owner to ensure and verify its ownership and authenticity by using digital watermarking process. In general, watermarking can be done either in spatial domain in which watermarks are embedded in the image pixels directly or in frequency domain where the watermark is inserted in the frequencies obtained by frequency transformation of the image. Robustness in the spatial domain is a major issue as it is easy to identify the watermark inserted in the spatial domain. A digital watermarking consists of two steps embedding and extraction.
Several classifications of digital watermarking schemes are given in literature. Some ones classify it into robust, fragile and semi-fragile based on the resistance of the watermarking scheme against intentional or unintentional attacks. Robust watermarking methods generally are used for copyright protection and verification of ownership, because they resist most of image processing operations. Fragile watermarking methods are used for content authentication and integrity identification. Semi-fragile watermarking methods –which can be seen in allow non-malicious modifications, but they are fragile facing malicious attacks. Generally, the images may be manipulated by usual image processing operations, such as compression, which are considered non-malicious. In malicious attack, the meaning of multimedia content changes. A second classification for digital watermarking schemes is based on the requiring data to extract the watermark. It includes blind, semi-blind and non-blind watermarking methods. Non-blind watermarking schemes need the original image to extract the watermark. A semi blind watermarking uses some data or parameters of the embedding phase to extract the watermark. However, in a blind watermarking, the original image or any special data or parameters are not used for watermark extraction. A fragile mark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarks is in content authentication. Most of the work, as reported in the literature, in watermarking is in the area of robust techniques. Many important applications could benefit from the use of fragile watermarks.

2. Literature review

Maher et al. [1] propose an image authentication calculation in the DCT domain in view of neural networks. The watermark is built from the image to be watermarked. It comprises of the average value of each 8 × 8 block of the image. Each average value of a block is embedded in another supporting block sufficiently inaccessible from the ensured block to avoid simultaneous disintegration of the image and the recover data during local image tampering. Implanting is performed in the center frequency coefficients of the DCT transform. Moreover, a neural network is prepared and utilized later to recover tampered regions of the image. Thus we are able to conclude that the proposed method can produce high quality images. Also, it can successfully localize alteration and recover them. Yahya AL-Nabhani et al. [2] in this paper to develop an enhanced technique for producing watermarked images with high invisibility. Throughout extraction, watermarks can be successfully extracted without the necessity for the original image. We have got developed discrete wavelet transform with a Haar filter to embed a binary watermark image in chosen coefficient blocks. A probabilistic neural network is employed to extract the watermark image. To evaluate the efficiency of

the algorithm and also the quality of the extracted watermark images, we tend to used widely known image quality function measurements, such as Peak Signal-to-Noise Ratio (PSNR) and normalized cross correlation (NCC). Results indicate the excellent invisibility of the extracted watermark image (PSNR = 68.27 dB), still as exceptional watermark extraction (NCC = 0.9779). Experimental results reveal that the proposed watermarking algorithm yields watermarked images with superior imperceptibility and robustness to common attacks, such as JPEG compression, rotation, Gaussian noise, cropping, and median filter.

Zahra Pakdaman et al. [3] explained the Reversible watermarking is a special kind of the lossless data hiding techniques. It allows lossless recovering of both the watermark image and the host image. In this method based on error prediction in Hadamard domain is presented. The original image is divided into blocks and transformed to Hadamard domain. If a block is in a smooth area, its AC coefficients will be predicted using a linear predictor function. Thus the value of error between the original and the predicted coefficient is computed. At last, a watermark bit will be embedded in the error. To reduce the error value, an Adeline neural network is used to determine coefficients of the predictor function. The Hadamard domain can achive higher capacity and quality of the water mark image. Nazeer Muhammad et al.[4] discussed a digital image watermarking algorithm using Partial Pivoting Lower and Upper Triangular (PPLU) decomposition is proposed. In this technique, a digital watermark image is factorized into lower triangular, upper triangular and permutation matrices by PPLU decomposition. The change lattice is utilized as the valid key matrix for authentication of the rightful ownership of the watermark image. The result of the lower and upper triangular matrices is inserted into specific sub-bands of a cover image that is decomposed by wavelet transform using the singular value decomposition. The weight age-based differential calculation is used to achieve the possible scaling factor for acquiring the maximum possible robustness against various image processing operations and pirate attacks. Thus the experiments show that the proposed algorithm is highly reliable with better imperceptibility of the implemented image and preserving the high-end security of watermarks, and exhibits fast computation. Assem et al. [5] the embedding strength parameters for per-block image watermarking in the Discrete Cosine Transform (DCT) domain are enhanced. A fitness function is proposed to best suit the optimization issue. The ideal arrangement is selected based on the quality and the robustness accomplished using that solution. For a given image block, the peak-signal-to-noise ratio (PSNR) is used as a quality metric to quantify the invisible for the watermarked block. However, the strength cannot be measured for a single watermark bit utilizing traditional metrics. The proposed method uses the PSNR quality metric to show the degree of robustness. Henceforth, optimum embedding as for as quality and robustness can be achieved. To demonstrate the viability of the proposed approach, a recent watermarking technique is modified, and then used as the embedding method to be optimized. The Bees algorithm is chosen as the calculation method and the proposed fitness function is applied. In this method provides enhanced imperceptibility and robustness under different attacks. The performance of the proposed fitness function was compared with that of the traditional fitness function. The results have shown that our strategy provides better compromise between imperceptibility and robustness.

Irshad et al.[6] during this work, the robustness and security problem of IWT(Integer Wavelet Transform) and SVD (Singular Value Decomposition) based watermarking is explored. Generally, SVD based watermarking techniques suffer with difficulty of false positive problem. This leads to even authenticating the incorrect owner. We have a novel solution to this false positive problem; that arises in SVD based approach. Firstly, IWT is utilized on the host image and then SVD is performed on this transformed host. The properties of IWT and SVD facilitate in achieving high value of robustness. Singular values are used for the watermark embedding. In order to further improve the quality of watermarking, the optimization of scaling factor (mixing ratio)is performed with the help of artificial bee colony (ABC) algorithm .A comparison with different Schemes is performed to show the superiority of proposed scheme. Rayachoti et al. [7] transmission of medical images among remote places is a general follow in telemedicine. Medical images may be changed intentionally or accidentally as the transmission of those could turn up through unsecure networks such as internet. Before making any diagnostic selections, the medical practitioner should verify the integrity of Region of Interest (ROI) in the received medical image as to avoid wrong diagnosis. Watermarking is used for checking the integrity of medical images. During this study, the authors propose a medical image watermarking method based on Integer Wavelet Transform (IWT). This proposal verifies the integrity of ROI, exactly identifies tampered blocks within ROI, provides robustness to the info embedded inside Region of Non-Interest (RONI) and recovers original ROI. In this method, the medical image is segmented into ROI and RONI regions. Hash value of ROI, recovery knowledge of ROI and data of patient are embedded into RONI using IWT. Experimental results show that the method provides robustness to the watermark data knowledge embedded within RONI and accurately detects and localizes tampered areas within ROI and recovers the original ROI.

Xiao-Long Liu, et al. [8] this paper presents a blind dual watermarking mechanism for digital color images in which invisible strong watermarks are embedded for copyright protection and fragile watermarks are embedded for image authentication. For the aim of copyright protection, the primary watermark is embedded by using the Discrete Tavelet transform (DWT) in YCbCr color area, and it can be extracted blindly while not access to the host image. However, fragile

watermarking is predicated on associate least significant bits (LSB) replacement approach in RGB components for image authentication. The authenticity and integrity of a suspicious image can be verified blindly while not the host image and the primary watermark. The mixer of robust and fragile watermarking makes the proposed mechanism appropriate for protecting valuable original images. The refined features indicated that the planned watermarking mechanism can withstand various processing attacks and accurately find the tampered space of an image.

Mohamed et al.[9] discussed a hardware implementation of an area cloud for storing, sharing and archiving patient's folders (health report and medical imaging) supported raspberry Pi card and an area cloud (hard disc) whereas exchanging alternative distant public cloud (google drive, azure cloud, …). Securing the medical knowledge is ensured by a proposed encrypting technique for the watermarked digital imaging and communications in medication imaging that contains the patient data (the watermark) and therefore the advanced encryption customary is employed to crypt the text files (health reports). The imaging encryption technique is based on the exoring of the ith block to be encrypted. The watermarking technique is based on the insertion of the watermark within the least significant bit. Finally, encryption and watermarking keys are encrypted and keep within the information. A real-time implementation on raspberry Pi and android smart phone is projected for the entire system using, severally, PHP and android studio. Thus the results demonstrate that the proposed security technique is robust against different types of attacks and can achieve high security with a decent performance.

Abdulaziz Shehab et al. [10] this method based on locates image tampering as well as recovers the original image. A number image is broken into 4×4 blocks. Singular Value Decomposition (SVD) is applied by inserting the traces of block wise SVD into the least significant bit (LSB) of the image pixels to work out the transformation within the original image. Two authentication bits particularly block authentication and self-recovery bits area unit wont to survive the vector quantization attack. The insertion of self-recovery bits is decided with Arnold transformation that recovers the original image even after a high tampering rate. SVD-based watermarking data improves the image authentication and provides some way to observe different attacked area of the watermarked image.

3. Conclusion

The comparative study of the fragile watermarking has been exhaustively used for detect tampering in an attacked image. A fragile watermarking system is useful in a variety of image authentication applications. This paper proposed the summary of different watermarking methods and algorithm proposed in literature. The watermarking methods were generate a tamper localization accuracy and PSNR of self-recover images. The future work of paper is mainly concentrate the developing a novel algorithm for highly reliable and is able to locate the attacked blocks efficiently. Improving the PSNR of the recovered host at a robust and satisfactory performance.

References

[1] Maher El'arbi, Chokri Ben Amar, "Image authenticatiom algorithm with recovery capabilities based on neural networks in the DCT domain," Journals of IET Image Process,.Vol. 8, Iss. 11, pp. 619–626, 2014.
[2] Yahya AL-Nabhani, Hamid A. Jalab , Ainuddin Wahid, Rafidah Md Noor,2015.ʻ Robust watermarking algorithm for digital images using discrete wavelet and probabilistic Network', Journal on Computer and Information Sciences.
[3] Zahra Pakdaman,Saeid Saryazdi, Hossein Nezamabadi-pour,2015.ʻ A prediction based Reversible image watermarking in Hadamard domain',Journal on Multimed Tools (springer) .
[4] Nazeer Muhammad, Nargis Bibi,2015.ʻ Digital image watermarking using partia pivoting lower and upper triangular decomposition into the wavelet domain',Journal of IET Image Process., Vol. 9, Iss. 9, pp. 795–803.
[5] Assem M. Abdelhakim, Hassan I. Saleh, Amin M. Nassar,2015.ʻ Quality metric-based fitness function for robust watermarking optimisation with Bees algorithm'. Journal on IET Image Process, pp. 1–6.
[6] Irshad Ahmad Ansari, Millie Pant, ChangWookAhn, 2016.ʻ Robust and false positive free watermarking in IWT domain using SVD and ABC. Journal on Engineering Applications of Artificial Intelligence.
[7] Rayachoti Eswaraiah , Edara Sreenivasa Reddy, 2015.ʻ Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest' . Journal on IET Image Process, 2015, Vol. 9, Iss. 8, pp. 615–625.
[8] Xiao-Long Liu, Chia-Chen Lin, Shyan-Ming Yuan, 2016.ʻ Blind dual watermarking for Colour images' authentication and copyright protection'.IEEE Transactions on Circuits and Systems for Video Technology.
[9] Mohamed Boussif, Noureddine Aloui, Adnene Cherif, 2018.ʻ Secured cloud computing for medical data based on watermarking and encryption'. Journal on IET Networks.
[10] Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou,2018.ʻ Secure and Robust Fragile Watermarking Schem for Medical Images'.