ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 10, October 2015

Image Tampering Detection and Localization-Survey

W. Annie Felcia, T M. Babimol, X.M. Binisha

***Abstract*— Digital image usage has been increased rapidly for a few years due to its advancement in technologies. They can be altered very easily such that the tampering is unable to differentiate from the original image. Many number of software are used to alter the image, hence the integrity of the image has become doubtful. This has lead to the increase in security of the image. Image tampering detection and localization are used in different applications including forensics. Watermarking is mainly used to check the integrity and authenticity. In this paper, a survey of different types of existing tampering detection techniques like hierarchical watermarking, hashing, cryptographic signature, 3 LSB watermarking, self propagation, one parity section and 2 restoration section has been provided and their performance is also given. 3 LSB watermark has high PSNR value compared to others.**

***Index Terms*— Self recovery, Tampering detection, Tampering localization, Watermarking.**

I. INTRODUCTION

The first photographic image was taken by allowing light to fall on the surface. After the discovery of digital image, it has been used more often. Digital processing is easy and it requires less memory for storage. Digital image is acquired by taking photoshot of an object. The pixel are sampled and mapped accordingly as zeroes or ones. They are stored in computer and compressed by converting the bits into mathematical representation. Computer interprets the bits to display analog version. Photographs have been considered as an unchangeable form. Hence they were used in many application such as medical, military, forensics, research, crime detection etc.

But nowadays due to the advancement in digital image processing the image can be altered legally or illegally. Many software's like Photoshop, cropping, splicing, etc. Due to this reason we cannot say if the image is original or not [12]. If the images are tampered then the patients can change the image accordingly so that they can claim insurance and in case of crime scene image the criminal might become free of charges. In case of education the tampered image gives false information and students are also tampering images for their own benefit which is illegal [4]. Watermarking is a process in which digital information (data) is hided in the image [15]. It is used to prove authenticity. It is done by two steps embedding and extraction. The watermark is embedded in the image and if it appears to be leaked, the information is extracted from the watermark. It is divided into visible and invisible watermarking. Visible watermarking means the watermark appears visible to the eyes. It provides authenticity and does not affect the original image. It can also be used for advertisement. In Invisible watermarking the watermarking does not appear to human eyes but it provides authenticity [6]. Based on robustness it is divided into fragile, semi-fragile and robust watermarking. Fragile watermarking cannot tolerate all attacks hence all tampering can be detected. In Robust watermarking it withstands all malicious attacks. Semi-fragile watermarking is between fragile and robust watermarking [3]. It has two techniques for tampering detection block-wise and pixel-wise. In block- wise technique the image is divided into large number of blocks. In pixel-wise technique the image is processed based on pixels. Overall block diagram of image tampering detection and localization is given below in Figure 1.

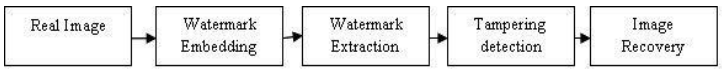

Figure 1: Block diagram of Tampering detection

The remaining of paper is organized as follows Section II describes the different methods for tampering detection and localisation, Section III deals with the result and discussion and Section IV concludes the paper.

II. METHODS OF TAMPERING DETECTION AND LOCALIZATION

A. Hierarchical Watermarking

In this technique watermark is embedded and extracted in a multilevel hierarchy. The lowest non overlapping partitioned block is the lowest level. Combination of various block constitute the upper level. We are assuming that 2×2 blocks are combined to form next level. Watermark is inserted by following 3 steps. First is the formation of block hierarchy, second the block signatures are computed and finally the watermark is inserted. When the hierarchical block X_{ij}^{l} is computed, a block similar to it $\tilde{X}_{ij}^{l}$ with the least significant bit as zero is produced. For these blocks the signatures are produced assuming it as a bit string. The top level consists of an indicator and in this step the hash is calculated.

By using the private key the hash is encrypted. The resulting signature is inserted in all LSBs. Thus the LSB will be same for all hierarchy level. Hence a partitioning algorithm is used that prevent collision. The higher level signatures are spreaded over the lower blocks and the payload is accumulated at the lowest hierarchy level by LSB modification. The signatures are partitioned into smaller

Manuscript received Oct 15, 2015.
***W.Annie Felcia**, ECE, Pet Engineering College, Vallioor, India.*
***T. M. Babi mol**, ECE, Pet Engineering College, Vallioor, India.*
***X.M. Binisha**, ECE, Pet Engineering College, Vallioor, India.*

number of strings where the number of partition depends on the number of levels. The lowest level payload of a block is formed by concatenating the units obtained from higher level blocks. By following these procedures the signature is kept localized and hence if there are manipulations on the pixel outside the block it does not affect the signature. LSB on the lowest plane is replaced by the payload bits. The verification process consists of formation of hierarchy block, extraction of block signatures and verification of them. From the LSB plane of the lowest block the payloads are extracted. Inversion is done for the partitioning algorithm so that the signatures can be obtained. Quantized version $\tilde{\hat{X}}_{ij}^{l}$ of block will appear for all block $\hat{X}_{ij}^{l}$ by setting LSB equal to zero. As mentioned above $\tilde{X}_{ij}^{l}$ will remain intact unless it's disturbed continually. Hence if the signature $\hat{S}_{ij}^{l}$ verifies the quantized $\tilde{\hat{X}}_{ij}^{l}$ it means authenticated. When cropping occurs hierarchical search can be used to re-obtain synchronization and also authenticate the untampered region. Sliding block window is used for search in higher levels. If quarter of an image is cropped it's a short coming for this method.

B. Cryptographic Signature And Block Identifier

Based on N_f the macro blocks are divided into 8 categories. They are done so as flippability condition will change mostly and N_f will also change. C_4, C_5, C_6, C_7 belongs to macro block which are named as qualified macro blocks (QMB). Distance between the previous QM B to the current QMB in vertical and horizontal directions is the horizontal distance D_x and vertical distance D_y. Index difference between the current and previous QMB in the horizontal direction is the sign S_x for D_x. D_x is larger and D_y is smaller when the image is processed in raster scan order. The image is divided into multiple macro blocks (MB) and N_f. Based on N_f MBs are classified and for each MB a block signature is generated. Calculations are done to find distance between two QMBs, the values of D_x and D_y are computed and they are represented as binary sequence of fixed length. For class C_i of the unqualified macro blocks, the number of MBs is calculated and they form a set N_u.

Binary features are generated by mapping binary bits for the minimum and maximum value. To prevent the swapping of C2, C3 the minimum, maximum, median, and mean of the block indexes are mapped as binary which are Xor-ed to generate F_{ub}. Block signature is obtained by mapping the binary bit of the feature code using lookup table. Embedding process is done by dividing the image into multiple MBs and they are divided into 8 categories to form block identifier (BI). BI is embedded on the flippable pixels on MB and Cryptographic Signature (CS) is embedded where more flippable pixels are present. The flippable locations are set to 0 to produce image which is given as feed to hash which produces the hash value. Encryption of hash and private key gives the CS. If the computed block signature (BS) is different from the extracted BS it means tampering is present. If the newly calculated S_{xw}, F_{ubw}, D_{xw}, D_{yw} are different from the extracted one it means multiple MBs tampered. CS_w is extracted from the flippable pixels and decryption is done by providing public key to get extracted hash. If the extracted hash is different from the one produced during embedding process it means user is unauthenticated. The Performance measure is shown in Table 2.

Table 2: Performance measure

Parameter	Value
Probability of miss detection	1.64%
Probability of false alarm	1.5%

C. Hash-Based Identification

Hash signature is produced by the content producer for the original image X. It passes through an untrusted network and the image obtained is $\overline{X}$. The original image is divided into small blocks. The average is taken and stored in a vector. Random projections are sampled from a Gaussian distribution using a random seed S. It is transmitted as part of the hash. It is quantized using uniform scalar quantizer. To reduce the number of bits lossy encoding is performed with side information at the decoder. Bits are encoded by transmitting syndrome bits which is produced by LDPC code. The syndrome bits are stored and they are transmitted when the feedback channel is available until the hash can be decoded. The image $\overline{X}$ is received by the content user and it requests the syndrome bits and the random seeds of the hash. The received image is divided into small blocks and their average is stored in a vector. Inverse geometric transformation is applied to match the original image.

Random projections are computed from the vector. The original image is obtained by using hash and side information. In the same way decoding of LDP is performed from the most significant bit. When the feedback channel is not available decoding does not happen if the distortion between the original and the tampered image is high than the tolerable distortion. Similarly if feedback channel is present decoding happens successfully. The problem is that small geometric transformations causes increase in MSE distortion between original and tampered image. This increases the number of syndrome bits. Hence it's advisable to limit the number of hash. When it fails for single value, it fails for all value hence unauthenticated. If it succeeds MSE distortion between original and tampered image is calculated. Estimate is obtained for the value. The chances are that reconstruction is either that the tampering is sparse or not sparse. After reconstruction we mostly choose the one which is sparsed. PSNR value is shown below.

Table 3: Performance measure

Parameter	Value
PSNR	31.5dB

D. 3LSB Watermarking

The tampering is detected by dividing the image into blocks of 2×2 and generating a 12 bit watermark from the MSB of the pixels. Tampering is detected by two steps 1) Comparing the last two bit of the LSB of the 12 bit watermark and the next step is 2) Comparing the other 10 bits of the 12 bit watermark. If they are same it means that tampering is not present otherwise tampering is present. Two steps are present such that if tampering is not detected in first step then it will be detected in next step. The flow chart is given in Figure 2.

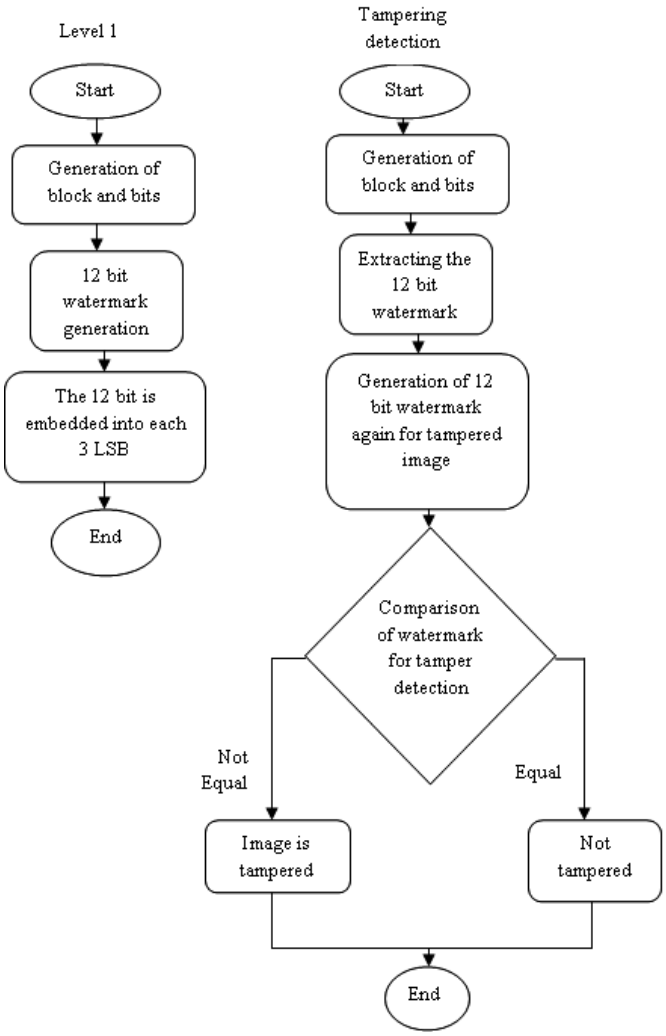

Figure 2: Flow chart of 3 LSB watermarking

The 12 bit watermark should be produced in such a way that they should be related to the pixels so that the tampering can be detected. A pixel is taken and their 5 MSB is the first 5 MSB of the 12 bit watermark. Another one pixel is taken and the 5 MSB of this pixel is the next 5 value of the 12 bit watermark. Thus the 10 bits are created for the 12 bit watermark. The pixel is padded by adding three zeroes to the LSB. Hence the value changes and the average intensity is taken for the four values and is parity checked with 1. It is placed as 11th bit in 12 bit watermark. It is denoted as C_r. The last bit is the average intensity of the entire bit and it is parity checked, it is denoted as r.

Table 4: Comparison of performance analysis for different methods

#	Attack-1	Attack-2
10% of Blocks selected in watermarking	1639	1639
Modified blocks in Watermark Image (%)	1458(1458/ 1639 = 88.96%	1639 (100%)
No of Detected blocks by system's proposed	81.41%	100%

The tampering is detected in such a way that the watermarked image is divided into blocks 2×2 and comparison is done for the average intensity and parity check of the new pixel to the LSB of the extracted image. If they are same no tampering otherwise tampering is present. In next step a bit by bit comparison is made for the remaining 10 bit of the watermark which is extracted. For different types of attacks the performance comparison is illustrated in Table 4.

E. Watermarking With Self- Propagation And Restoration Capabilities

Block-wise method is used to find the altered blocks and reference bits are also used to find set of potential restoration candidates. By using the set 5 MSBs of the tampered pixel can be found. Image is pseudo-randomly divided by a secret key k1 to generate subsets of m pixels. The MSB bits b4,..., b7are used to compute m-bit code. Bit b8 is not included as it's used to find potential restoration candidates. The reference bits produced are embedded in bit b3 of every subset. The same method is followed to generate another set of reference bits by using key k2. The reference bit produced is embedded in bit b2 of every subset. 64 bit description is created as I||n1||n2||p, where I is the image index, n1 and n2 is image size, p is the block index. Tampering can be detected and localised even if cropping is present. 64 bit hash code is generated from 7 MSBs of the block. Exclusive-or operation is done between 64 bit description and hash code. The resultant produced is the 64 bit authentication code. It is replaced by the LSB value. From the LSB 64 bit is decrypted to obtain authentication code. 64 bit hash code is produced from the 7 MSBs of each block.

By using Exclusive-or between authentication and hash code, description code is obtained which is denoted as A. In A the MSBs are identical to each other. If the image is watermarked |A| should be higher than threshold T_L .If $|A| \leq T_L$ it means that it is shifted. For shifted version the pixels are replaced by λ_i rows and λ_j columns. By using this authentication can be done when cropping is present. N1 and n2 are obtained from the description codes and it can restore the original shape. Potential restoration candidates are searched in every tampered pixel. Subsets with more than 3 tampering are associated to a set of potential restoration candidates which contains 5 bit values. From bit b3 reference bits are generated, they are compared with test codes from which 4 bits are identified. 4 bit values that have a match are extended to form 5 bit potential restoration candidates. From the potential restoration candidates unique restoration candidate is to be found. By using key k_2 reference bits are generated from bit b2 of every pixel. Test bit codes are computed which are compared with the reference code. The elements that do not match are discarded. By doing this process the single potential restoration candidate can be recovered. It is repeated until all the pixels can be recovered. The PSNR and restoration percentage of image is given in Table 5.

Table 5: PSNR and Restoration

Parameters	Value
PSNR	37.9
Restoration	24-28%

F. Fragile Watermark with One Parity Section And 2 Restoration Sections

It consists of a fragile watermark with one parity section and two restoration sections so that it can be restored easily if one

gets tampered. The blocks are divided into size of 3×3. The two LSBs are replaced so that they can be embedded. The watermark capacity is about 18 bits, the lat 2 LSBs are reset to 0. The remaining 6 bit is generated by applying XOR operation on 54 MSBs and 9×6 encrypt table which is created by secret key 1. The restoration section is generated by the average intensity of pixels. The 6 bit watermark section generated above is inserted as a payload of block i. As 2 restoration sections are needed, two copies are to be embedded. Hence two block mapping functions $\sigma 1$ and $\sigma 2$ are required. They are embedded into block σ_1 (i) and σ_2 (i). Tampering detection is done in 5 steps.

Step 1: The parity bits are generated again from MSBs of each block. Comparison is done between the extracted parity from LSB and the generated parity. If they are equal there is no tampering otherwise tampering is present.

Step 2: Tampering is detected based on block neighbourhood. If the m value is equal to 0 and the number of eight neighbouring blocks with m_1=1 is ≥4 tampering is present otherwise m_1, where m_1 is the index in step 1.

Step 3:The inter-block comparison pair is denoted as N. If m_2 =0 and the number of inconsistent pairs is more than N/2 the index value is 1 otherwise m_2.

Step 4: If the tamper ratio is high, there is a probability of false accept. To reduce this index is given by, if m_3=0 and $N_{m3=1} \geq \lambda_1$ =3 is 1otherwise m_3.

Step 5: The false reject can be modified by applying if m_4=1 and $m_2 \neq 1$ and $N_{m4=1} \geq \lambda_2$ =3 is 0, otherwise m_4. As 2 restoration sections are present if one block is invalid it can be restored by valid one. LSB is padded with two zeroes and the remaining six bit is replaced in the invalid block. The invalid blocks can be recovered without restoration watermark by taking the average intensity of the neighbour pixels. The PSNR and Probability of rejection is given in Table 6.

Table 6: PSNR and False Rejection

Parameter	Value
PSNR	44.33dB
Probability of false rejection	0.1

III. Results and Discussion

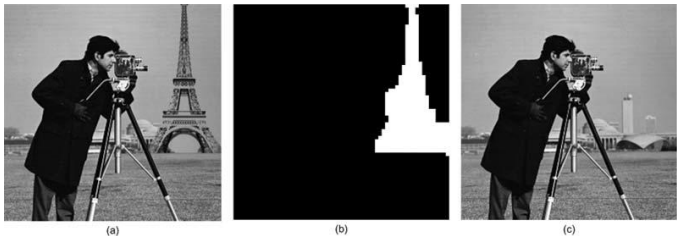

Figure 3: a) Tampered image b) Tampering detected c) Recovered image

Tampering detection and recovery is shown in Figure 3. The various survey results deals with the tampering detection, localization and recovery. PSNR, percentage of tamperings detected during attack, restoration percentage, probability of missing detection and probability of false detection are estimated for different grey scale images. By using the methods mentioned above tampering can be detected accurately, localised and even restored.

IV. Conclusion

The article describes the survey of different methods of tampering detection, localization and self recovery. The PSNR is estimated for the image, the probability of missing the tampering detection and false detection are also estimated. From the literature analysis it is inferred that the PSNR value is almost above 30 dB. . Concentration should be done on the PSNR value o that the loss of bits will be reduced and can be recovered easily.

REFERENCES

[1] S. Bravo-Solorio, C.-T. Li, A. K. Nandi, "Watermarking Method with Exact Self-Propagating Restoration Capabilities", WIFS 2012.

[2] Chao-Ming Wu, Yan-Shuo Shih, "A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections", Optics and Photonics Journal, 2013, 3, 103-107.

[3] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN 2009.

[4] Deepika Sharma, Pawanesh Abrol, "Digital Image Tampering – A Threat to Security Management", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.

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

[6] Gurpreet Kaur, Kamaljeet Kaur, "Digital Watermarking and Other Data Hiding Techniques", IJITEE ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[7] Huijuan Yang and Alex C. Kot, "Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature and Block Identifier", IEEE Signal Processing Letters, Vol. 13, No. 12, December 2006.

[8] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Comput. Sci. Softw. Eng., vol. 3. Dec. 2008, pp. 926–930.

[9] P. Korus and A. Dziech, "Efficient method for content reconstruction with self-embedding," IEEE Trans. Image Process., vol. 22, no. 3, pp. 1134–1147, Mar. 2013.

[10] Marco 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. [4] M. Wu and B. Liu, "Watermarking for image authentication," in Proc. Int. Conf. Image Process. (ICIP), vol. 2. 1998, pp. 437–441.

[11] Mehmet Utku Celik, Gaurav Sharma, Eli Saber, Ahmet Murat Tekalp, "Hierarchical Watermarking for Secure Image Authentication With Localization", IEEE Transactions On Image Processing, Vol. 11, No. 6, June 2002.

[12] Minati Mishra, Flt. Lt. Dr. M. C. Adhikary, "Digital Image Tamper Detection Techniques - A Comprehensive Study", International Journal of Computer Science and Business Informatics, Vol. 2, No. 1. June 2013, ISSN: 1694-2108.

[13] Saeed Sarreshtedari, Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery", IEEE Transactions On Image Processing, Vol. 24, No. 7, July 2015.

[14] Sajjad Dadkhah, Azizah Abd Manaf, Somayeh Sadeghi, "Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking", IJCSI Vol. 9, Issue 1, No 2, January 2012.

[15] Vinita Gupta, Atul Barve, " A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

Annie Felcia has done the B.Tech degree in Electronics and Communication Engineering in 2014 from Kalasalingam University and is pursuing M.e Communication Systems in Pet Engineering College.

T. M. Babi Mol is working as an assistant professor in Electronics and Communication Department, Pet Engineering Collgee. She completed her B.e and M.e in CSI Institute of Technology. Her Research area includes Image Processing and Antennas.

X. M. Binisha is working as an assistant professor in Electronics and Communication Department, Pet Engineering College. She completed her B.e in 2008 from CSI Institute of Technology and M.e in 2012 from Pet Engineering College. Her area of interest includes Embedded and signal processing.