Journal of Engg. Research Vol. 9 No. (1) March 2021 pp. 168-175 https://doi.org/10.36909/jer.v9i1.8379

CLIFD: A novel image forgery detection technique using digital signatures

Sahib Khan* and Arslan Ali

Department Electronics and Telecommunications, Politecnico di Torino, 10129, Italy
**Corresponding Author: sahib.khan@polito.it*

Submitted: 30/06/2019
Revised: 19/10/2020
Accepted: 27/10/2020

ABSTRACT

The paper presents a new image forgery detection technique. The proposed technique uses digital signatures; it generates a digital signature for each column and embeds the signature in the least significant bits of each corresponding column's selected pixels. The message digest algorithm 5 (MD5) is used for digital signature generation, and the four-least-significant-bit substitution mechanism is used to embed the signature in the designated pixels. The embedding of the digital signature in the selected pixel remains completely innocent and undetectable for the human visual system. The proposed forgery detection technique has demonstrated significant results against different types of forgeries introduced to digital images and successfully detected and pointed out the forged columns.

Keywords: Forgery detection; digital signature; least significant bits (LSB) substitution; message digest 5 (MD5).

INTRODUCTION

Images are a prevalent source of preserving and sharing important events of life. Important information and documents are also saved in the form of images (Farid, 2009). These can become a solid proof of criminal activities and can be presented in the court of law as legal evidence. However, the contents of digital images can be manipulated, and the true sense of the image contents can be altered, with the help of readily available image modification tools and software, e.g., Photoshop (Redi et al., 2011). In such cases, in mind, it is important to know how much the contents can be trusted and how the modification can be detected. Issues like these are addressed in the field of image forgery detection by forensics experts (Wang et al., 2009).

Image forgery detection has emerged as a new active area of research in the last few decades. It has found various important signal processing applications, vision, investigation, and forensics (Farid, 2009). It has become very challenging to detect the image modifications, which cannot be detected by naked eye. There are various powerful and extremely sophisticated software tools that can modify a digital image, not to attract the human visual system (HVS) (Khan et al., 2016; Khan et al., 2015). The modification can be of different types, e.g., pixel modification, bit modification, image enhancement, image rotation, and truncation. The modification can be even worse; e.g., some image contents are placed in another image. So, it is essential to detect all types of possible modifications and forgeries introduced to digital images.

The digital image forgery detection techniques are broadly classified as active forgery detection techniques and passive forgery detection techniques (Khan et al., 2019). Active forgery detection techniques are deployed with the help of watermarks or signatures. Various techniques use a watermarking-based and signature-based approach to detect different types of forgeries in images. Details of these techniques are available in the literature (Wahid et al., 2018).

While the passive image forgery detection techniques use sensor noise of camera acquisition devices, the noise appears due to camera sensors' imperfection and is always unique (Birajdar et al., 2013). Each camera has its own and unique camera sensor noise, and due to its uniqueness, they are considered as the fingerprints of the cameras. Various passive image forgery detection techniques use sensor noise; the details are available in Agarwal et al. (2018) and Gautam et al. (2018).

This paper presents one such technique that uses hidden digital signatures to detect forgeries in images. The proposed technique can detect image forgery at the column level. That is why, it is termed as a column-level image forgery detection (CLIFD) technique.

The rest of the paper is organized in the sections of the proposed technique, experimental results, and analysis, comparison, and conclusion sections.

THE PROPOSED TECHNIQUE

The CLIFD technique comprises two processes: one is the signature calculation and hiding signature, and the second one is the signature recovery, signature regeneration, and comparison of the signatures.

The first process is performed by the sender or generation party. In the CLIFD technique, the image under consideration of size "NxM" is processed for signature calculation and embedding. The pixels of each column of the image are divided into two parts. One part is having "N-32" pixels and is used for the signature generation for the column, and another part of "32" pixels is used for signature embedding. The signature generation pixels are fed to the MD5 algorithm (Mahdian et al., 2009; Wang et al., 2010), which processes these pixels and generates a 128-bit digital signature. The 128-bit digital signature is then embedded in the 32 pixels of the same column. 4LSB substitution technique (Khan et al., 2013) is used for this purpose, and 4 bits per pixel are hidden. So, the 128-bit signature is completely accommodated in the 32 pixels.

Similarly, each column of the image is processed; a digital signature is calculated and embedded in the selected pixels. The final product of the whole process is an image with embedded digital signatures. The complete process is presented in Figure 1.

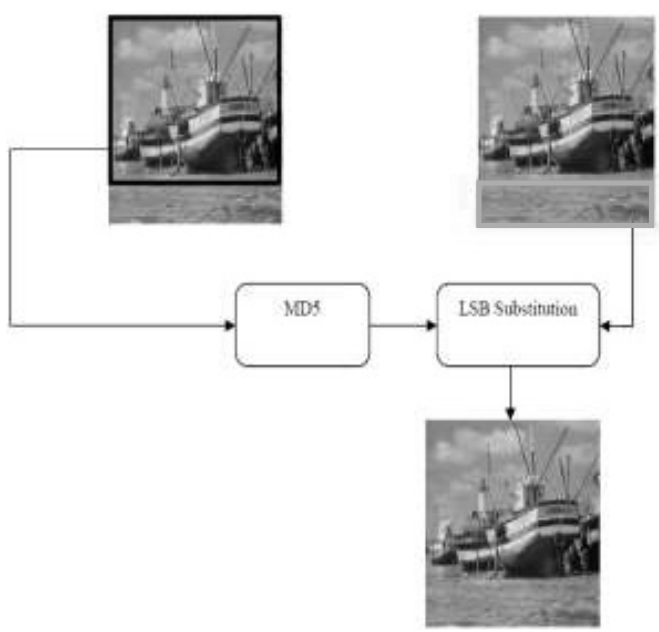


Figure 1. Implementation of CLIFD at source side.

If there is a need to check the image for possible forgery and detect the manipulation, the digital signature generation and signature retrieval are performed on the receiver side or any point. Checking and detecting any possible forgery in an image, each column of the image is divided into two parts similar to the process done on the sender side. One part is composed of "N-32" pixels, and the other part consists of those 32 pixels, having embedded digital signature inside. The "N-32" pixels of each column are fed to the MD5 algorithm to regenerate each column's digital signature. The signatures are stored and then used for forgery detection in a column or columns.

The 32 pixels are processed for signature retrieval, and 4LSB of each pixel is retrieved. So, the 128-bits signature is completely retrieved from 32 pixels. Each column's 32 bits are processed in the same way, and 128-bit digital signature is retrieved for each column. It is important to mention that MD5 algorithm always results in a 128-bit digital signature, and to embed the 128-bit digital signature in the selected pixels with 4LSB substitution technique, 32 pixels are needed.

It is also possible to use 3LSB, 2LSB, or 1LSB technique for 128-bit digital signature. However, in that case, a larger number of pixels per column will be required to completely embed the 128-bit digital signature. But, it is found from experimentation that 4LSB substitution is an efficient technique for signature embedding, and to check the authenticity of a column and detect any possible forgery, the regenerated and retrieved digital signatures of the corresponding columns are compared. If both of the signatures match with each other, the column is declared authentic. In case the match fails, the column is declared forged. Each column, which is modified is pointed out, and forgery at the column level is detected in the image. The process of signature regeneration, retrieval, and forgery detection is presented in Figure 2.

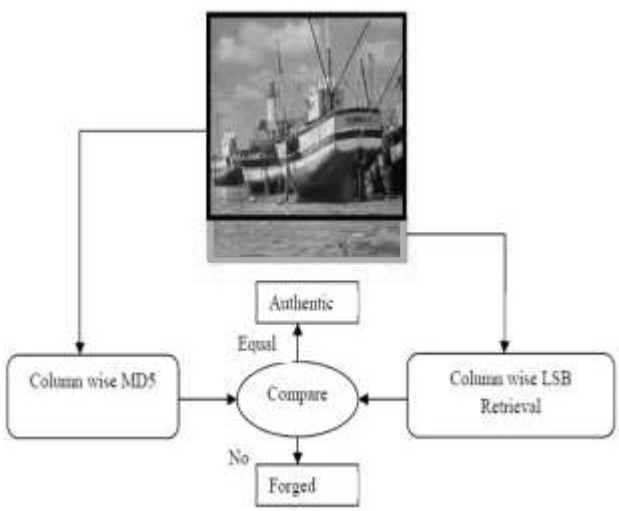


Figure 2. CLIFD forgery detection process.

EXPERIMENTAL RESULTS AND ANALYSIS

To check the performance and forgery detection capability of the CLIFD technique, it is tested against different types of forgeries. A digital image of Lena of size 512x512, as shown in Figure 3(a), is considered for the experimentation. CLIFD is applied to a digital image shown in Figure 3(a). Lena image is processed column by column, and each column of 512 pixel is divided into two parts. The one used for signature calculation has 480 pixels, and the rest of the 32 pixels of the column are placed in the second part, which is used for signature embedding.

The 480 pixels of each column are processed for signature generation using the MD5 algorithm. The 128-bit digital signature is then hidden in the LSBs of designated 32 pixels of the corresponding column, embedding 4 bits in individual pixel. The image has a total of 512 columns, so a total of 512 digital signatures are computed, each of 182 bits. The signatures are embedded in the designated 32 pixels of the respective columns. The final output image, with the entrenched digital signature obtained, is shown in Figure 3(b). The quality of the image with hidden digital signature,

i.e., Figure 3(b), is compared with the original image, i.e., Figure 3(a), by computing the PSNR. It has been found that the resulting image with hidden digital signature has a PSNR of 74 dB. It is further observed that part of the image that has hidden information, i.e., the selected 32 pixels of each column, has a PSNR of 40 dB. The results show that the proposed technique of hiding signature degrades neither the quality of the resulting image nor the selected pixels.

(a) (b)

Figure 3. Original and output images using CLIFD. (a) Original image. (b) Image with the hidden signatures.

The image with the hidden digital signature, shown in Figure 3(b), is subjected to various types of modifications. The resulting modified images are shown in Figure 4 (a, b, c, d, e, and f).

The different rows and columns of the image are manipulated first, and the manipulated image is shown in Figure 4 (a). The image with modified pixels in different rows of the single column is shown in Figure 4 (b). The image with modified pixels in different columns of a single row is shown in Figure 4 (c). Figure 4 (d) shows the truncated image, and Figure 4(e) shows the modified image, with multiple bits changes in single pixels. Figure 4(e) presents an image with only one LSB that is changed in one pixel. The image can be manipulated in many ways, e.g., rotation, scaling, contrast enhancement, blurring, and sharpening image details.

(a) (b)

(c)

(d)

(e)

(f)

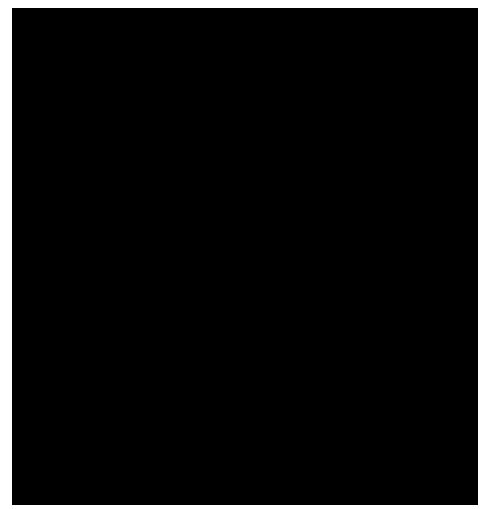
Figure 4. Images modified in various ways for the CLIFD. (a) Altered image with changes in various pixels of different rows and columns. (b) Modifying pixels in different rows. (c) Pixel manipulation in different columns. (d) Truncated image. (e) More than one bit forged in a single pixel. (f) One LSB changed in single pixel.

The manipulated images shown in Figure 4 are processed for forgery detection using CLIFD. The experimental results show that the CLIFD technique successfully detects the manipulation introduced in the images. Figure 5 shows that the CLIFD technique has detected the forgeries made to the image, and the forged columns are shown in complete black.

(a)

(b)

(c)



(d)

(e) (f)

Figure 5. Forgery detection in images using CLIFD. (a) Changes pointed out in multiple pixels in various rows. (b) Manipulation detection in pixels of different rows. (c) changes detected in pixels in multiple columns. (d) Truncation detection. (e) Various bits changes detection in one pixel. (f) Detection of one LSB changes in one pixel.

The proposed technique, i.e., CLIFD, is compared with the previous state-of-the-art techniques using the benchmark image Free-Form Copy-Move Forgery (FFCMF) dataset (Gürbüz et al., 2019). The images in the dataset are manipulated in various manners. The proposed technique and the techniques presented in Lyu et al. (2002), Shi et al. (2005), Zou et al. (2006), Rad et al. (2015), and Kashyap et al. (2016) are applied to the manipulated images.

The comparison is made using evaluation measures of true positive (TP), true negative (TN), and accuracy. The values calculated are listed in Table 1. The results demonstrate the comparison of the proposed techniques with the techniques presented in Lyu et al. (2002), Shi et al. (2005), Zou et al. (2006), Rad et al. (2015), and Kashyap et al. (2016).

The results show that, among all the previous techniques mentioned in Table 1, Kashyap et al. technique has the highest detection accuracy of 81.50%, while CLIFD techniques demonstrated a detection accuracy equal to 95%, which is even higher than that of Kashyap et al. Therefore, it can be concluded that the proposed method is more powerful and efficient than the previous techniques used for manipulation detection in digital images.

Table 1. Comparison of CLIFD with previous techniques.

Sr. No.	Technique	TP(%)	TN(%)	Accuracy (%)
1	Lyu et al., 2002	78.20	69.39	73.75
2	Shi et al., 2005	75.55	76.02	75.78
3	Zou et al., 2006	77.40	75.07	76.21
4	Rad et al., 2015	80.11	77.61	78.80
5	Kashyaop et al., 2016	83.33	76.0	81.50
6	CLIFD	96.51	95.78	95.01

CONCLUSION

The proposed CLIFD technique is an efficient technique to detect forgeries in digital images with high accuracy. The technique detects manipulation at the column level and identifies the forged columns in one way or another. It is capable of detecting single or multiple rows and columns manipulations successfully. It has also been proven successful to detect single or multiple bits manipulation in a pixel or pixels. The experimental result demonstrated a true positive rate of 96.51%, while a true negative rate of 95.78% is recorded against different types of forgeries in various images. The proposed technique, when compared with the state-of-the-art technique, has presented better performance than others. In conclusion, the CLIFD technique is an efficient and powerful technique for image forgery detection and authentication.

REFERENCES

Agarwal, S. & Chand, S., 2018. Image Forgery Detection Using Co-occurrence-Based Texture Operator in Frequency Domain. In Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Springer, Singapore.: 117-122.

Birajdar, G.K. & Mankar, V.H. 2013. Digital image forgery detection using passive techniques: A survey. Digital Investigation. **10**(3): 226-245.

Farid, H. 2009. Image forgery detection. IEEE Signal Processing Magazine. **26**(2): 16-25.

Gautam, S. & Jalal, A.S., 2018. An Image Forgery Detection Approach Based on Camera's Intrinsic Noise Properties. International Journal of Computer Vision and Image Processing. **8**(1): 92-101.

Gürbüz, E., Ulutas, G. & Ulutas, M. 2019. Free-Form Copy-Move Forgery (FFCMF) Dataset, http://emregurbuz.tc/research/imagedatasets/ffcmf/ffcmf.html.

Kashyap, A., Parmar, R.S., Suresh, B., Agarwal, M. & Gupta, H. 2016. Detection of digital image forgery using wavelet decomposition and outline analysis. In International Conference on Signal Processing and Communication (ICSC).: 187-190.

Khan, S., Ahmad, N., Ismail, M., Minallah, N. & Khan, T. 2015. A secure true edge based 4 least significant bits steganography. In International Conference on Emerging Technologies (ICET), Peshawar, Pakistan.: 1-4. IEEE.

Khan, S. & Bianchi, T. 2019. Reduced Complexity Image Clustering Based on Camera Fingerprints. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP): Brighton, United Kingdom.: 2682-2688. IEEE.

Khan, S., Ismail, M., Khan, T. & Ahmad, N. 2016. Enhanced stego block chaining (ESBC) for low bandwidth channels. Security and Communication Networks. **9**(18): 6239-6247.

Khan, S., Khan, M.N. & Iqbal, S. 2013. Bit Position Based Qualitative and Quantitative Analysis of DCT and Spatial Domain Steganography. International Journal of Computer Science Issues (IJCSI). **10**(3): 169-173.

Lyu, S. & Farid, H. 2002. Detecting hidden messages using higher-order statistics and support vector machines. In Information Hiding: 340-354.

Mahdian, B. & Saic, S. 2009. Using noise inconsistencies for blind image forensics. Image and Vision Computing. **27**(10): 1497-1503.

Rad, R.M. & Wong, K. 2015. Digital image forgery detection by edge analysis. In IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW).: 19-20.

Redi, J.A., Taktak, W. & Dugelay, J.L. 2011. Digital image forensics: A booklet for beginners. Multimedia Tool Appl. **51**(1): 133-162.

Shi, Y.Q., Xuan, G., Zou, D., Gao, J. & Yang C. 2005. Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. In International Conference on Multimedia and Expo. Amsterdam.: 269-272.

Wang, J., Liu, G., Zhang, Z., Dai, Y., & Wang, Z. 2009. Fast and robust forensics for image region-duplication forgery. Acta Automatica Sinica. **35**(12): 1488-1495.

Wahid, M., Ahmad, N., Zafar, M.H. & Khan, S. 2018. On combining MD5 for image authentication using LSB substitution in selected pixels. In International Conference on Engineering and Emerging Technologies (ICEET). Lahore, Pakistan. :1-6. IEEE.

Wang, Y., Zhao, Q., Jiang, L. & Shao, Y. 2010. Ultra high throughput implementations for MD5 hash algorithm on FPGA. In High Performance Computing and Applications. Springer, Berlin, Heidelberg.: 433-441.

Zou, D., Shi, Y.Q., Su, W. & Xuan, G., 2006. Steganalysis based on Markov model of thresholded prediction-error image. In IEEE International Conference on Multimedia and Expo.: 1365-1368.