Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/74/20240428

Image authentication and tamper localization based on coupling between adjacent pixels

Qingyi Jiang

Shenzhen College Of International Education, Guangzhou, China

s21411.jiang@stu.scie.com.cn

Abstract. Digital image information has the advantages of easy storage and communication, especially with the continuous emergence of powerful image processing software, editing and modifying digital images has become extremely convenient. Subsequently, issues such as low security and easy tampering of digital images have emerged, and the integrity and authenticity of images have been questioned. Some important applications, such as news images, court evidence, medical diagnoses, etc., are not allowed to have their content modified. Passive authentication methods are often only suitable for specific images or situations, don't have the ability to locate the tamper areas. Active methods based on fragile watermarks often embed external information, making it inconvenient to perform blind authentication on the receiving end and resist malicious attacks that aim at bypassing tamper detection. In this paper, we propose to combine the advantages of passive authentication and active authentication. Firstly, an image is first divided into non-overlayed blocks, then generate check code for each pair of strongly coupled pixels within the same block. Fragile watermark technology is exploited to embed the check codes randomly based on a private key in the pixels of the image itself to achieve blind authentication for the receiver. Finally, we conduct the experiment in which a large number of images have been simulated for tampering and detected for authentication. The results show that compared with other similar methods, this paper not only has high detection accuracy, but also has high accuracy in locating the tampering location. In addition, the method proposed in this paper has other advantages in terms of computational cost and security.

Keywords: Image Authentication, Data hiding, Hash Value, Semi-fragile Watermarking, Tamper Detection.

1. Introduction

Many new forms of multimedia and their applications have emerged because of the rapid development of computer multimedia technology and the popularization of Internet applications. The development of digital imaging technology has made images an important carrier of information dissemination. Image processing and editing software that is readily available, such as Photoshop, are user-friendly and easy to operate, allowing non-professionals to perform various editing and processing of images. This reprocessing of images can make them clearer and more aesthetically pleasing, making it convenient for people's lives and work. But if such editing and processing are used to intentionally alter the authenticity of image content, it becomes image tampering or forgery. The tampered images, if used in some special fields, will bring some negative or even serious social impacts, such as news fraud incidents. In these

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/74/20240428

application areas [1], such as forensic photos presented at law enforcement sites and courts, and digital images in scientific research or medicine, authenticity verification of image content is required.

Therefore, digital images are like a double-edged sword that has different impacts, positive and negative. Real digital images faithfully record and reproduce on-site information, while fake digital images contain false information for different purposes. The *PS* (PhotoShop@) has become synonymous with tampering with digital images. When people see a digital image to obtain information, they do not believe the image they "see" with their eyes, but naturally have a question: is this image real or *PS*ed because 'seeing is no longer believing'?

Digital image forensics is to carry out the analysis, identification, and authentication of tampering or forgery of digital images to determine their origin, originality, integrity, and authenticity [2]. Conducting this research work has significant practical significance and academic research value for maintaining national security and stability, establishing public trust order, cracking down on criminal activities, ensuring judicial fairness, protecting intellectual property rights, and news integrity.

From the current research and practical application, there are two digital image forensics technology types [3-4]: passive forensics and active forensics. The research on passive digital image forensics is later than active digital image forensics, and it has received attention from scholars and experts both domestically and internationally in recent years.

By utilizing current image editing and processing techniques, it is often possible to achieve visually "traceless" tampering and produce a visually consistent appearance, making it difficult or impossible for even photographers or image experts to visually determine the authenticity of an image. However, since a natural digital image is based on imaging principles, imaging equipment, and natural scenes, it has inherent data statistical characteristics as well as special and inherent consistency between imaging equipment and natural images. The processing operations of editing and tampering with images can affect or disrupt the intrinsic statistical characteristics and consistency of the original image. What's more, it also introduces non-intrinsic characteristics that are manually operated but not possessed by the original image or imaging device itself. Passive forensics of digital images is based on the imaging principles of natural images, the inherent characteristics of natural images, and the impact of image editing and tampering on the original image [5-6].

In contrast to passive image authentication, active digital image forensics requires preprocessing of the image, "actively" embedding "extra information" like digital watermarks in the original natural image, or extracting abstract information or so-called digital signatures from the image as auxiliary information for future authentication [7-8]. During authentication, we determine whether the image has been tampered by comparing the additional information in the test image with known corresponding information. Active digital image forensics often achieves universality in authentication applications that do not rely on specific images or scenarios. In this paper, we research active digital image forensics based on digital watermarking.

2. Related works

Digital watermarking, as one of the information-hiding technologies, plays a crucial role in protecting image information from damage in image circulation. Embedding hidden information in the form of a watermark into the data carrier makes the watermark invisible in the original image data [9]. After receiving the image containing the watermark, the receiver obtains the watermark contained in the image through an extraction algorithm corresponding to the watermark embedding algorithm. In addition to invisibility, watermarks should also have requirements for fragility and robustness. Fragility and robustness are two mutually exclusive characteristics that can be emphasized according to different application environments. For example, copyright protection requires effective extraction of watermark information from the image, which requires strong robustness for watermarks. Image authentication requires verification of the integrity of the image [10], which requires watermarks to be sensitive to image tampering operations. In this case, watermarks need to have strong vulnerability.

The most successful spatial watermarking algorithm is the Least Significant Bits (LSB) algorithm. For an image with a pixel value of 8 bits and 256 levels, the watermark information is embedded into

DOI: 10.54254/2755-2721/74/20240428

the least significant bits of the pixels, which is the least sensitive bit compared to human vision. When the image is tampered with, the watermark information will also change. The LSB algorithm is a simple but widely used spatial watermarking algorithm. Various spatial watermarking algorithms are its extensions or variants.

Nguyen et al. proposed a checksum-based digital watermarking algorithm by a typical LSB algorithm [11]. This algorithm embeds the checksum of the pixel value in the image into the least significant bit, calculates the checksum of the pixel value in the image and compares it with the extracted checksum to extract the watermark and determine whether the image has been tampered with. Toyokawa et al. blocked the watermark and encrypted its embedding position and amplitude with a key, thereby preventing collusion attacks and improving the security of the watermark [12]. Qi et al. divided the original image into blocks with a size of 8x16 and performed hash verification on each image block [13]. This algorithm can resist vector attacks to a certain extent and locate tampered areas at the image block level. Otum et al. proposed the concept of layered watermarking, which synthesizes adjacent original image blocks to obtain higher-level image blocks [14]. As the watermark may be embedded in higher-level image blocks, it increases the concealment of the watermark information. Piper et al. suggested a spatial algorithm by statistical features, opening up a new direction for spatial algorithms [15]. This type of algorithm embeds watermark information by modifying the mean statistical features of pixels in the image. Sharma et al. adjusted the pixel values of the image accordingly, while embedding the watermark [16], keeping the average values of all pixels unchanged, making the watermark information more difficult to detect. Subsequently, spatial watermarking algorithms based on standard deviation statistical features and pixel histograms emerged one after another, becoming an important component of spatial watermarking algorithms.

In addition to embedding watermarks in the spatial domain, various mathematical transformation algorithms have been widely applied in the field of images, such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), etc. Based on these transformations, various image digital watermarking algorithms have been proposed. Compared to spatial watermarking, frequency-domain watermarking has poor vulnerability, low sensitivity to image tampering, and lacks the ability to locate tampered locations [17]. Fragile watermarks are suitable for achieving complete image authentication [18]. In recent years, people have different requirements for image authentication, one of which is to use watermark technology to distinguish malicious attacks from conventional image operations [19]. Based on such requirements, various semi-robust watermarking algorithms have been developed [20-27], and the image authentication operations completed by these watermarking algorithms are called semi-robust image authentication. Constructing a watermark by the characteristics of the image is a commonly used method in content-based image authentication. This method can retain the content of the image in the watermark and provide matching information for subsequent image authentication. Abdulqader et al. [28] represented the RGB image in the form of brightness and color difference, and extracted feature points on the brightness based on the SURF feature extraction. A description vector was constructed based on its main direction and decomposed into two sub-components. The watermark was constructed by comparing the angles between subcomponents and normal vectors, and is finally embedded into the pixel values of the image. The algorithm can effectively identify image tampering and resist salt and pepper noise, but its resistance to other noise is poor. Wang et al. [29] introduced the concept of sub-block groups, embedded watermarks in specific regions using the Slant transform DC quantization, and used a noise filtering strategy to distinguish between image tampering and noise interference during the authentication process, thus achieving tamper detection based on image content. This algorithm has good resistance to image compression, but its detection effect is poor in terms of noise interference similar to changing image contrast. Shi et al. [30] embed watermarks through multiple quantization coefficients, control the robustness of the watermark through DWT transformation, and finally use tamper detection functions for image authentication. This algorithm has good robustness for image compression, but poor robustness for other operations such as Gaussian noise and filtering, so its use has significant limitations. Al-Otum et al. [31] embedded watermarks into the wavelet domain subband coefficients of digital images, making them highly robust

DOI: 10.54254/2755-2721/74/20240428

to JPEG compression, but the algorithm makes it difficult to locate tampered areas. Shaik [32] utilizes the difference coefficients in the discrete cosine transform to extract watermarks, and utilizes BCH error correction codes to improve the watermark's resistance to noise interference. This algorithm has good robustness against general noise, but its recognition ability for tampering operations such as cropping and replacement is limited.

Through the comparison and analysis of various image digital watermarking algorithms mentioned above, it can be found that spatial domain image digital watermarking algorithms are generally relatively simple in algorithm, with low computational time complexity and relatively large watermark capacity. They are generally sensitive to data tampering. Frequency domain image digital watermarking algorithms are generally able to resist various noise interference and image compression operations, but the amount of computation required for watermark embedding is generally large, and the capacity of the watermark is limited, making it less sensitive to tampering and lacking accurate tampering localization.

3. Tampering authentication based on local image correlation

An active image authentication technique is proposed in the spatial domain. First of all, divide an image into small blocks, generate a checksum or checksum for each pair of interleaved pixels in the block, and LSB watermarking technology is used to hide each checksum in the spatial domain into a randomly assigned pixel. The advantages of the proposed technique are not only low computational cost, but also high sensitivity to any type of tampering, and high positioning accuracy. In addition, it also has a certain degree of resistance to intentionally bypassing identity verification.

3.1. Image blocking and local check codes

For an image, we divide it into equal-sized, non-overlapping chunks. Suppose the size of the image is MXN and the size of the block is kxk. Then the number of blocks we can obtain is as follows:

$$m=\lfloor M/\mathrm{k} \rfloor, n=\lfloor N/\mathrm{k} \rfloor \tag{1}$$

where $\lfloor . \rfloor$ is a rounding-down operation. In (1), m is the number of blocks in the row direction, and n is the number of blocks in the column direction. Here we take k=2, as shown in Figure 1. Thus in one block, there are 4 pixels, labeled as A, B, C, and D. We use them to establish four pairs of coupling relationships, such as B->A, D->C, A->D, and C->B.

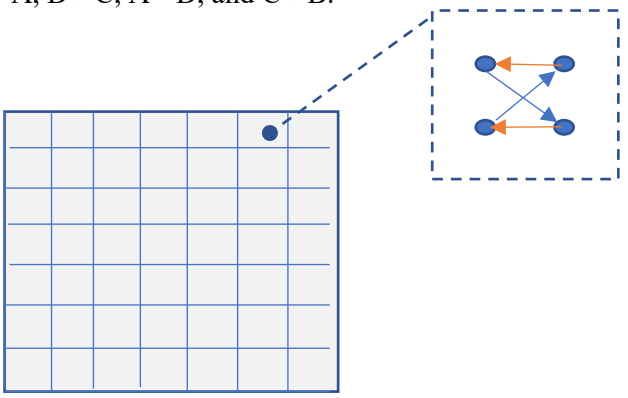

Figure 1. Coupling between adjacent pixels

DOI: 10.54254/2755-2721/74/20240428

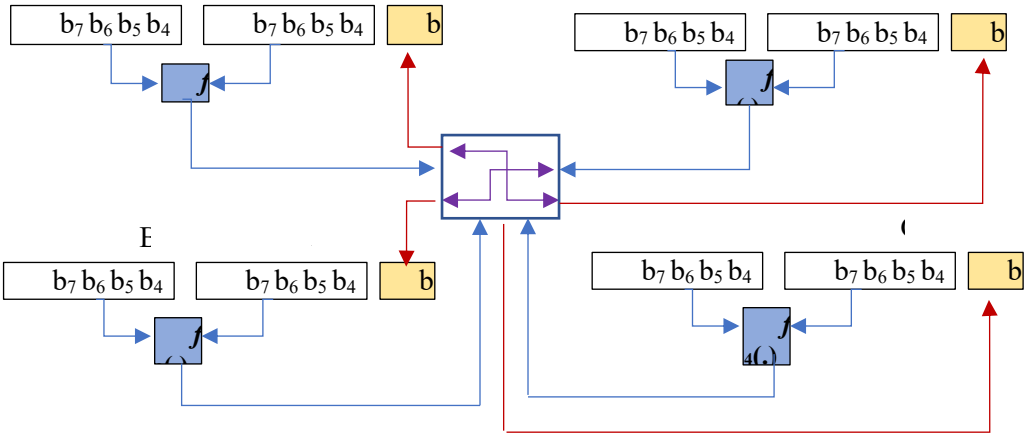

Figure 2. Generation and storage of local check codes

For a 256-scale gray image, the value of each pixel is one byte, or 8 bits (b7, b6, …, b1, b0 from high to low). The high 6 bits of a pair of pixels X and Y are used to generate a 2-bit checksum code C_{XY}:

$$C_{XY} = f_i(X_{b7\text{-}b2}, Y_{b7\text{-}b2}) \quad (2)$$

For example, the checksum code C_{BA} of pixels B and A is a function of bits b7, b6, …, b2 of both B and A. To enhance security, the functions used to generate each pair of pixel checksums can be different. For simplicity, the function used here is XOR operations, i.e.:

$$C_{XY} = (X_{b7\text{-}6} \oplus Y_{b7\text{-}6}) \oplus (X_{b5\text{-}4} \oplus Y_{b5\text{-}4}) \oplus (X_{b3\text{-}2} \oplus Y_{b3\text{-}2}), \text{ where } \oplus \text{ is an XOR operation} \quad (3)$$

Some pixel values (one byte) may have special circumstances. The checksum calculated using the first 6 bits of the pixel value may exactly match its last 2 bits. The image area covered by this pixel value will bypass tamper detection. To overcome this deficiency, we let $C_{AD} = C_{XY}$, $C_{DC} = C_{XY}$, while C_{BA} =NOT (C_{XY}), and C_{CB} =NOT (C_{XY}), where NOT(.) is a bit-wise invert operation.

3.2. Self-embedding of check codes and the framework of the proposed technique

To achieve blind authentication, as well as not incur additional overhead of image transmission, we embed the check code directly in the image itself by using a data hiding technique in the spatial domain. For a 256-scale gray image, the value of each pixel is one byte or 8 bits. The change of LSB-1 and LSB-0 will not affect the pixel value too much, so the embedding of check code is implemented by directly storing check code (2 bits) in LSB-1 and LSB-0. To further enhance security, the generated check codes are interleaved and stored, as indicated with a router symbol in Figure 2. Then perform global random storage based on a *key*, which will be shared by the receiver.

The above scheme is based on grayscale images and can also be applied to color images.For an RGB image, each pixel consists of 3 components, namely R, G, and B, and the value of each component is one byte. The above scheme is employed in the R, G, and B planes respectively.

DOI: 10.54254/2755-2721/74/20240428

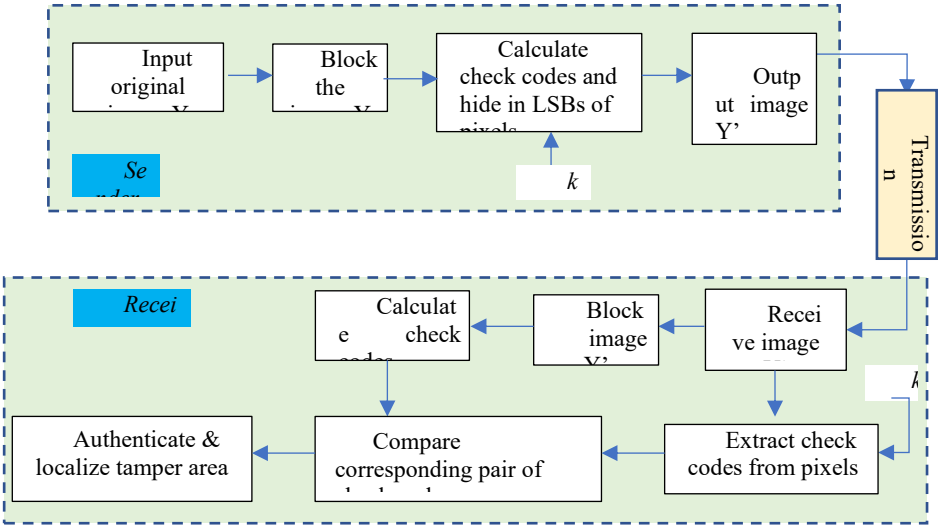

Figure 3. Framework of proposed image authentication and tamper detection

In figure 3, the framework of the proposed image authentication. On the sender side, for input, if it is a color image, generate and store check codes in the R/G/B plane respectively. The subsequent procedures are the same as done for a gray image. A *key* is used to generate a random matrix to determine the global storage location of check codes.

On the receiver side, firstly extract the check codes stored in the received image Y', and then use the matrix generated by the *key* to restore the positions of their corresponding pixel pairs. At the same time, use the same method as on the sender to generate check codes for image Y'. Image authentication and tamper localization are achieved by comparing the generated and extracted paired check codes. If such a pair of checksums is not equal, the corresponding pair of pixels is identified as tampered with. For color images, a pair of pixels has three check codes. If any checksum is not equal to the extracted one, then this pair of pixels is identified as tampered with. In other words, authentication of color images is more sensitive.

4. Results and analysis

In the following experiments, we evaluate the proposed authentication technique from three aspects. The first one is imperceptibility caused by image watermarking, using both the ratio of Peak Signal to Noise Ratio (PSNR) and Normalization Cross Correlation (NCC) metrics. The second one is tamper detection and localization for image authentication. The third one is the computational cost. Finally, we briefly analyze the security of the technique.

1000 images are randomly selected from the dataset CASIA [33] to test the proposed scheme and the state-of-the-art schemes with their empirically determined parameters. CASIA contains more than 8000 images divided into different categories based on content - animals, nature, textures, architecture, people, plants, objects, scenes, etc.

4.1. Fidelity test

Let the watermark embedding capacity equal the image payload. We compute the PSNR value to evaluate the influence on image fidelity by watermark embedding. Fig. 4 is a statistical distribution of the PSNR values of the 1000 test images. Figure 4 shows that our PSNR values range between 50 dB and 60 dB, and the average value is more than 55 dB. To achieve the same degree of tamper detection and localization capabilities, the PSNR value is much higher than any semi-fragile watermarking technology. This indicates that the fidelity of our processed image remains high.

DOI: 10.54254/2755-2721/74/20240428

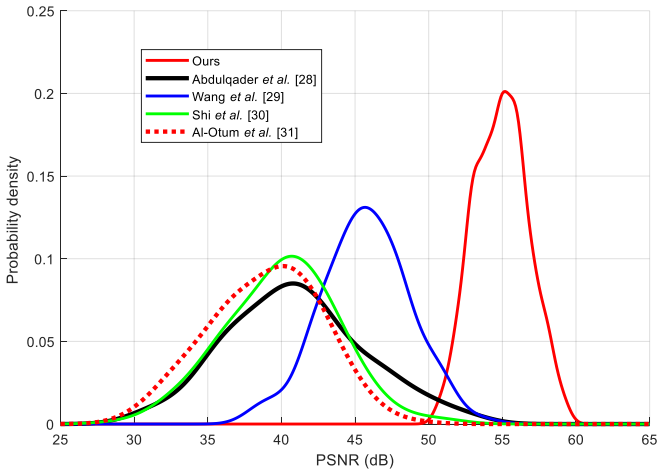

Figure 4. The probability distribution of PSNR values

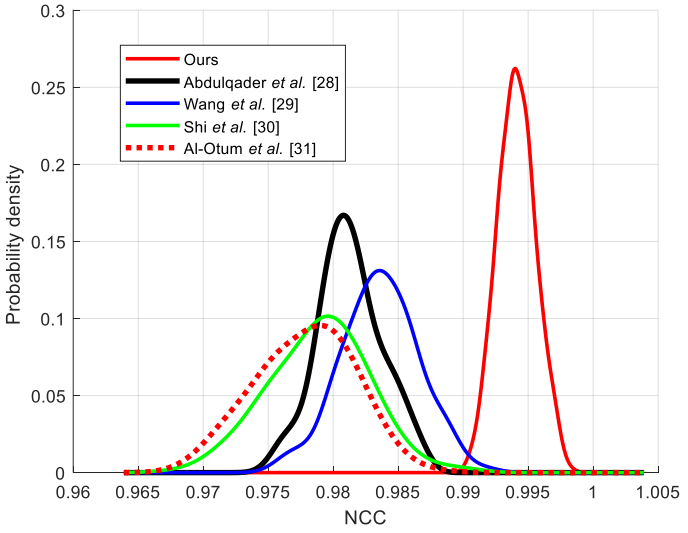

Figure 5. The probability distribution of NCC values

We also evaluate the image fidelity by NCC metrics, and the result is shown in Fig. 5, and the conclusion is the same.

4.2. Susceptibility to malicious manipulation and tampering with location

We discussed some purposeful tampering that causes semantic changes. The tampering below manipulates the original image into a new image with a different visual meaning. In Figures 6 to 8, the left is the original image, the right is the tampered image, and the white grid is located in the tampered area.

Type 1: object replacement, see Fig. 6. Modify and replace an object with a cutout to confuse the public with faked information.

Type 2: object removal, see Fig. 7. Erase an object to make the area a background to make some key information missing.

Type 3: object pasting, see Fig. 8. Paste an object which here is the thumbnail of the image itself to forge additional information.

DOI: 10.54254/2755-2721/74/20240428

Type 4: object addition, see Fig. 9. On the left, text annotation is added in the original image. On the right is the detected text, whose position corresponds to its position in the original image.

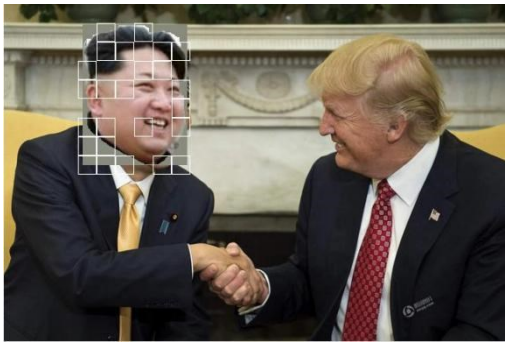

Figure 6. Left: original image

Right: the result of locating the replaced object

Figure 7. Left: original image

Right: the result of locating the removed object

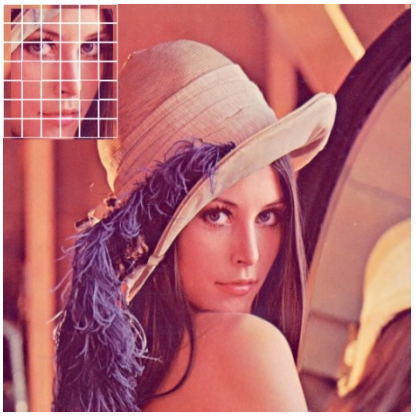

Figure 8. Left: original image

Right: the result of locating its own thumbnail pasted

DOI: 10.54254/2755-2721/74/20240428

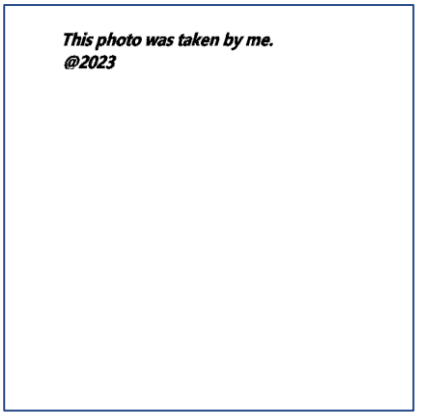

Figure 9. Left: addition of text annotation Right: highlighting of the detected result

The above four types of tampering are applied to 1000 images respectively. Evaluation indicators for model effectiveness are listed in Table 1, where we can find that our technology is better than others at tamper detection and localization. This is because our method achieves pixel-level accuracy in tampering with localization.

Table 1. Precision and recall (%) of tamper detection and localization

Tamper type	Precision and recall	Ours	Abdulqader *et al.* [28]	Wang *et al.* [29]	Shi *et al.* [30]	Al-Otum *et al.* [31]	Shaik *et al.* [32]
Type 1	P_{1p} (%)	**99.184**	87.743	91.674	89.452	92.128	86.434
	P_{1r} (%)	**99.246**	88.456	91.664	88.234	91.514	85.093
	P_{2p} (%)	**96.358**	80.368	51.345	77.625	46.763	78.344
	P_{2r} (%)	**95.461**	79.341	35.917	74.578	38.783	77.918
Type 2	P_{1p} (%)	**99.166**	85.956	91.182	86.113	90.348	85.107
	P_{1r} (%)	**99.448**	84.287	90.228	85.467	89.551	83.096
	P_{2p} (%)	**94.156**	81.294	48.551	74.234	46.373	74.103
	P_{2r} (%)	**95.862**	74.811	47.723	73.168	38.291	71.935
Type 3	P_{1p} (%)	**99.114**	86.253	89.148	84.452	91.284	86.146
	P_{1r} (%)	**99.322**	85.122	88.196	82.234	90.103	85.007
	P_{2p} (%)	**94.256**	75.328	36.205	72.623	42.346	71.226
	P_{2r} (%)	**93.028**	74.004	40.313	71.882	41.724	70.204
Type 4	P_{1p} (%)	**98.216**	86.768	87.194	83.242	92.221	81.118
	P_{1r} (%)	**98.105**	86.095	89.884	85.224	90.534	80.102
	P_{2p} (%)	**95.773**	73.621	43.355	72.246	41.766	69.211
	P_{2r} (%)	**94.571**	73.225	40.872	71.012	38.719	58.027

P_{1p}: Precision of tamper detection, P_{1r}: Recall of tamper detection
P_{2p}: Precision of tamper localization, P_{2r}: Recall of tamper localization

4.3. Computational cost

We evaluate the complexity of the method by testing images of different sizes using a computer with an Intel Core i7 CPU (2.67 GHz) and 3GB RAM. Computational cost includes the calculating time spent on check code generation and embedding back in the image, T_g, and tampering detection and tampering localization, T_d. The reported average computational time is shown in Table 2. From Table 2, our method

DOI: 10.54254/2755-2721/74/20240428

takes a shorter time than most of the peer techniques, both in the generation of check code or hash value and in the tamper detection and localization.

Table 2. Average time spent on hash generation/watermark embedding T_g, and tamper detection and Tampering Localization T_d

	Image Size	256x256	384x384	512x512	832x832	976x976	1200x1200
Ours	***Tg*(s)**	**0.63**	**0.86**	**1.51**	**2.14**	**2.54**	**2.76**
	***Td*(s)**	**0.34**	**0.54**	**0.80**	**1.23**	**1.74**	**2.09**
Abdulqader *et al*. [28]	*Tg*(s)	1.14	1.39	2.32	3.92	5.63	7.36
	Td(s)	0.82	0.97	1.26	2.11	3.62	4.11
Wang *et al*. [29]	*Tg*(s)	1.26	1.98	2.98	3.74	5.02	7.95
	Td(s)	0.89	0.99	1.29	1.86	2.87	4.35
Shi et al. [30]	*Tg*(s)	1.91	2.11	3.27	4.84	6.77	8.58
	Td(s)	0.98	1.15	1.91	2.65	3.92	5.14
Al-Otum *et al.* [31]	*Tg*(s)	1.17	2.02	2.88	3.27	4.31	5.26
	Td(s)	0.61	0.89	1.05	1.24	2.55	3.21
Shaik *et al.* [32]	*Tg*(s)	0.68	0.97	1.14	1.25	2.99	4.25
	Td(s)	0.66	0.86	1.11	1.21	2.87	4.21

4.4. Security issue

The security mechanism of our authentication system has three layers:

This technique is secure if the attacker does not know the algorithm for checksum generation, as it is impossible for an attacker to manipulate the image to fool the authentication system without triggering an alarm.

This technique is still secure if the attacker does not know the *key* because attackers do not know the pairing relations between the generated and extracted check codes. Only people who share this private key know the correct pairing relationship between the generated and extracted check codes.

If an attacker knows the key, the technique may still be secure. Because the check codes in the block are closely related to each other, malicious tampering of the image while retaining all check codes is likely to result in artifacts in the image or disharmony and disunity in visual meaning. An attacker may try to develop special operations to defeat the proposed scheme, but it is difficult for an attacker to control the artifacts produced in the pixel domain.

Generally speaking, the idea of secure watermark technology for verifying images is whether the extracted watermark is consistent with the decrypted watermark. Knowing the watermark embedding method and the owner's claim to the embedded watermark, an attacker can keep the watermark intact by deliberately tampering with the image. Therefore, the security of watermark-based classical authentication techniques capable of both tamper detection and localization is no higher than ours.

5. Conclusions

The complete authentication of multimedia, especially digital images, has become an urgent practical problem that needs to be solved. Fragile watermarking technology takes advantage of the feature that watermark information is destroyed and not be fully detected after any changes occur in the image. It can be used to solve the authentication problem of digital images. In this paper, a fragile watermarking algorithm based on image blocks is proposed, combined with local coupling characteristics of pixels in the image and global position scrambling, which eliminates the independence between image blocks, and can effectively detect various types of malicious tampering. Specifically, based on the strong

DOI: 10.54254/2755-2721/74/20240428

coupling relationship of pixel values within the image block, a verification code is generated and embedded as an image feature watermark into the least significant bit and second least significant bit of each pixel in the image block. Thus, it effectively improves the ability to locate and tamper with positions and achieve accurate authentication of digital images. To further prevent tamperers from bypassing authentication, the embedding position of the verification code is globally random in the image. A large number of simulation experiments have confirmed the effectiveness of this proposed method, and it outperforms other similar methods in terms of image fidelity after preprocessing, detection accuracy, and time consumption.

References

[1] Rahul Thakur, Rajesh Rohilla, Recent advances in digital image manipulation detection techniques: A brief review, Forensic Science International, Volume 312, July 2020, https://doi.org/10.1016/j.forsciint.2020.110311

[2] B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When seeing isn't believing," IEEE Signal Processing Mag., vol. 21, no. 2, pp. 40–49, Mar. 2004

[3] Fatemeh Zare Mehrjardi, Ali Mohammad Latif, Mohsen Sardari Zarchi, Razieh Sheikhpour, A survey on deep learning-based image forgery detection, Pattern Recognition, Volume 144, December 2023, https://doi.org/10.1016/j.patcog.2023.109778

[4] Nhan Le, Florent Retraint, An Improved Algorithm for Digital Image Authentication and Forgery Localization Using Demosaicing Artifacts, IEEE Access, Volume 7, 2019, Page(s): 125038 - 125053, DOI: 10.1109/ACCESS.2019.2938467

[5] Zhiyong Su, Liang Yao, Jialin Mei, Lang Zhou, Weiqing Li, Learning to Hash for Personalized Image Authentication, IEEE Transactions on Circuits and Systems for Video Technology, Volume 31, Issue 4, April 2021, Page(s): 1648 - 1660, DOI: 10.1109/TCSVT.2020.30021

[6] H.T. Chang, C.H. Lin, and C. Y. Chen, "Image multiplexing and authentication based on double phase retrieval in fresnel transform domain", Optics Communications, vol. 389, issue 15, 2017, pp. 150-158

[7] Wien Hong, Jeanne Chen, Pei-Shih Chang, Jie Wu, et al., A Color Image Authentication Scheme With Grayscale Invariance, IEEE Access, Volume 9, 2020, Page(s): 6522 - 6535, DOI: 10.1109/ACCESS.2020.3047270

[8] Xiaofan Xia, Songsong Zhang, Kunshu Wang, Tiegang Gao, A novel color image tampering detection and self-recovery based on fragile watermarking, Journal of Information Security and Applications, Volume 78, November 2023, https://doi.org/10.1016/j.jisa.2023.103619

[9] Javier Molina-Garcia, Beatriz P. Garcia-Salgado, Volodymyr Ponomaryov, Rogelio Reyes-Reyes, et al., An effective fragile watermarking scheme for color image tampering detection and self-recovery, Signal Processing: Image Communication, Volume 81, February 2020, https://doi.org/10.1016/j.image.2019.115725

[10] K. Swaraja, K. Meenakshi, Padmavathi Kora, An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine, Biomedical Signal Processing and Control, Volume 55, January 2020, https://doi.org/10.1016/j.bspc.2019.101665

[11] T. S. Nguyen, C. C. Chang, and X. Q. Qian Yang, "A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain", International Journal of Electronics and Communications, vol. 70, issue 8, 2016, pp. 1055-1061

[12] K. Toyokawa, N. Morimoto, S. Tonegawa, K. Kamijo, and A. Koide, "Secure digital photograph handling with watermarking technique in insurance claim process," in Proc. SPIE, vol. 3971, 2000, pp. 438–445

[13] X. Qi, and X. Xin, "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization," Journal of Visual Communication and Image Representation, Volume 30, July 2015, pp. 312-327

DOI: 10.54254/2755-2721/74/20240428

[14] H. M. Al-Otum, "Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique," Journal of Visual Communication and Image Representation, Volume 25, Issue 5, July 2014, pp. 1064-1081.

[15] A. Piper, R. Safavi-Naini, "Scalable fragile watermarking for image authentication," IET Information security, 2013, Vol. 7, Issue 4, pp. 300–311

[16] Suchita Sharma, Shivendra Shivani, Nitin Saxena, An efficient fragile watermarking scheme for tamper localization in satellite images, Computers and Electrical Engineering, Volume 109, Part B, August 2023, https://doi.org/10.1016/j.compeleceng.2023.108783

[17] R. O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain," Measurement, Vol. 46, Issue 1, January 2013, pp. 367-373

[18] Anuja Dixit, Soumen Bag, A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks, Expert Systems with Applications, Volume 182, 15 November 2021, https://doi.org/10.1016/j.eswa.2021.115282

[19] Xiaofeng Wang, Qian Zhang, Chuntao Jiang, Jianru Xue, erceptual hash-based coarse-to-fine grained image tampering forensics method, Journal of Visual Communication and Image Representation, Volume 78, July 2021, https://doi.org/10.1016/j.jvcir.2021.103124

[20] Mianjie Li, Chihui Liu, Chun Shan, Houbing Song, Zhihan Lv, A dual-embedded tamper detection framework based on block truncation coding for intelligent multimedia systems, Information Sciences, Volume 649, November 2023, https://doi.org/10.1016/j.ins.2023.119362

[21] Neena Raj N.R., Shreelekshmi R., Fragile watermarking scheme for tamper localization in images using logistic map and singular value decomposition, Journal of Visual Communication and Image Representation, Volume 85, May 2022, https://doi.org/10.1016/j.jvcir.2022.103500

[22] Pascal Lefèvre, Philippe Carré, Caroline Fontaine, Philippe Gaborit, Jiwu Huang, Efficient image tampering localization using semi-fragile watermarking and error control codes, Signal Processing, Volume 190, January 2022, https://doi.org/10.1016/j.sigpro.2021.108342

[23] Edgar González Fernández, Ana Lucila Sandoval Orozco, Luis Javier García Villalba, A multi-channel approach for detecting tampering in colour filter images, Expert Systems with Applications, Volume 230, 15 November 2023, https://doi.org/10.1016/j.eswa.2023.120498

[24] Chuchu He, Yunshu Chen, Jie Pan, Yue Huang, et al., Enhanced features in image manipulation detection, Signal Processing: Image Communication, Volume 116, August 2023, https://doi.org/10.1016/j.image.2023.116983

[25] Shahad Lateef abdulwahid, The detection of copy move forgery image methodologies, Measurement: Sensors, Volume 26, April 2023, https://doi.org/10.1016/j.measen.2023.100683

[26] Xiangyang Wang, Wencong Chen, Panpan Niu, Hongying Yang, Image copy-move forgery detection based on dynamic threshold with dense points, Journal of Visual Communication and Image Representation, Volume 89, November 2022, https://doi.org/10.1016/j.jvcir.2022.103658

[27] Esteban Alejandro Armas Vega, Edgar González Fernández, Ana Lucila Sandoval Orozco, et al., Image tampering detection by estimating interpolation patterns, Future Generation Computer Systems, Volume 107, June 2020, Pages 229-237,https://doi.org/10.1016/j.future.2020.01.016

[28] Mohammed Fakhrulddin Abdulqader, Adnan Yousif Dawod, Ann Zeki Ablahd, Detection of tamper forgery image in security digital image, Measurement: Sensors, Volume 27, June 2023, https://doi.org/10.1016/j.measen.2023.100746

[29] Kunshu Wang, Xiaofan Xia, Zehui Zhang, Tiegang Gao, Hashing-based remote sensing image tamper detection system, Digital Signal Processing, Volume 140, August 2023, https://doi.org/10.1016/j.dsp.2023.104101

DOI: 10.54254/2755-2721/74/20240428

[30] H. Shi, M. C. Li, C. Guo, and R. Tan, "A region-adaptive semi-fragile dual watermarking scheme," Multimedia Tools and Applications, 2016, vol. 75, issue 1, pp. 465–495
[31] Hazem Munawer Al-Otum, Arwa Abdelnaser Ali Ellubani, Secure and effective color image tampering detection and self restoration using a dual watermarking approach, Optik, Volume 262, July 2022, https://doi.org/10.1016/j.ijleo.2022.169280
[32] S. Abdul Shaik, K. Ram Karsh, Mohiul Islam, Shubhashish Bhakta, Content Authentication and Tampered Localization Using Ring Partition and CSLBP-Based Image Hashing, IEEE Access, Volume 11, 2023, Page(s): 126791 - 126802, DOI: 10.1109/ACCESS.2023.3330969
[33] CASIA, accessed on Nov. 25, 2023. [Online]. Available: http://forensics.idealtest.org/