Received: August 10, 2022. Revised: August 31, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Fragile Image Watermarking Based on Bidiagonal SVD-LSB for Tamper Detection and Localization

Nova Rijati[1]* **De Rosal Ignatius Moses Setiadi[1]** **Pulung Nurtantio Andono[1]**

[1]*Department of Informatics Engineering, Dian Nuswantoro University, Semarang 50131, Indonesia*
* Corresponding author's Email: nova.rijati@dsn.dinus.ac.id

Abstract: Tamper detection and localization are essential things in fragile image watermarking to carry out the authentication process. The tampering method continues to evolve from general and complex tampering. This study proposes a tamper detection and localization technique that can withstand a variety of standard and complex attacks with a combination of bidiagonal singular value decomposition, blockwise and group block for authentication. The least significant bit method is used in the embedding process to increase imperceptibility. By combining these methods, fragile image watermarking is produced that is robust against various common tampers such as type I and type II copy-paste, rotate, text addition, and noise addition, as well as various complex attacks such as vector quantization, collage, content only and constant feature. The tamper detection rate is more than 0.99, and the average PSNR value is 51.85 dB. This shows that the proposed method is robust against various tampers and has excellent imperceptibility.

Keywords: Tamper detection, Tamper localization, Fragile watermarking, Image authentication bidiagonal SVD.

1. Introduction

The rapid development of technology in information and communication technology has a positive impact on people's lives, namely sending text messages and even multimedia such as digital images[1]. Currently, there are many valuable applications for manipulating digital images, where this manipulation cannot be detected by the human visual system (HVS) [2]. Changing or falsifying digital image content can have a negative impact on the information sent. This can lead to misperceptions and hoax news. Even medical images can cause misdiagnosis, thus requiring protection during transmission[2, 3].

Image watermarking is one of the most popular methods widely used for copyright protection or authentication [2–5]. There are three watermarking models based on their use: fragile, semi-fragile and robust. These three methods have different approaches in securing digital images. In robust watermarking, watermarks are embedded robustly to withstand various image manipulations such as adding noise, blurring, cropping, rotation, and others [3–5]. Semi-fragile watermarking will be strong against accidental attacks but fragile against intentional attacks [6, 7]. Meanwhile, fragile watermarking is used for authentication because it is sensitive to minor manipulations [2]. The more sophisticated the technology, the more sophisticated the image manipulation, so the three watermarking models are equally important to develop.

In particular, how fragile image watermarking works is that it must be able to detect attacks or manipulations that occur in the image. The attack or manipulation may occur in a part of the image area or the entire image area, the location of a certain part of the image. The area of the image that is being manipulated must be known so that it can facilitate the authentication process. The authentication process must be strong and secure to accurately and precisely find the tamper's location [8, 9]. Some common tamper attacks are copy-paste attacks, removing content, adding text or adding noise. In a copy-paste attack, a part of the watermarked image is usually copied and pasted into another image or copy-pasted the other way around. There are also several complex attacks, these attacks are generally designed

to hide interference, some of these attacks include vector quantization attack (VQA), collage attack (CA), content only attack (COA), constant feature attack (CFA) [2, 10]. The ability of the fragile watermarking method to detect tampering can be determined by measuring tools such as the true positive rate (TPR) or often also called the tamper detection rate (TDR), true negative rate (TNR) or false positive rate (FPR), and precision (p), where when these three measuring instruments have a value close to 1, it means that the quality of tamper detection is getting better [2, 11, 12].

The imperceptibility aspect also determines the quality of fragile image watermarking. This aspect means that the watermark embedded in the image cannot be felt by the human senses, especially the visual system. The most widely used instruments to measure imperceptibility quality are PSNR and SSIM[13]. Fragile image watermarking can be designed in the spatial domain as in research [11, 14–16] or transformation domain [1, 17, 18] or these combination [2, 19, 20]. Determination of methods and domains can influence the results and advantages of the method in certain aspects. So this study aims to design a fragile watermarking method that can perform tamper detection and localization with accuracy and precision and has good imperceptibility. The strategy is to propose a combination of frequency and spatial domains. The bidiagonal singular value decomposition (BSVD) represents the frequency domain, while the spatial domain represents the least significant bit (LSB) method. The embedding technique uses block and group block methods so the watermark can be used for tamper detection. Further to understand the reasons, hypotheses, motivations and contributions of the proposed method are explained in section two. The total section in this paper is five, whereas in section three the stages of method testing are explained in detail. Section four on method implementation and analysis the results, and finally the research conclusions.

2. Motivation and contribution

Research is motivated by several related kinds of research. In research [16] LSB method is proposed to perform tamper detection and localization on fragile image watermarking. A watermark in the form of authentication bits is embedded in every two LSB of image pixels. This method's detection accuracy of damaged areas can reach 90%. In research [21] LSB method is also proposed. The LSB method is combined with the local binary pattern (LBP) operator. LBP determines rough and smooth image areas, embedding watermarks to be more adaptive. As a result, the proposed method can improve the imperceptibility aspect of the watermarked image.

Research [14] proposed a method based on least significant bit (LSB) and logistic map. The logistics map has a sensitivity feature that is used to generate watermarks. The logistic map's purpose is to create a more secure watermark for the authentication process. Before embedding the watermark, an XOR operation is performed with intermediate significant bits (ISB) and then embedded with the LSB method on the cover image. The results of the testing of this method get imperceptibility up to more than 51dB PSNR and have the efficiency in detecting and locating areas affected by tampering. The tamper detection trials were general tampering such as cropping, copy-pasting, adding noise and adding text.

Research [19] proposed a combination of LSB, singular value decomposition(SVD), and Arnold chaotic map (ACM) methods. The SVD process is carried out first, and then the embedding is carried out using the LSB method. Embedding is done by block to form 10-bit authentication and group block to form 6-bit group authentication. The ACM method is used to scramble blocks and improve watermark security. The combination of LSB and SVD methods for embedding watermarks in images can withstand general attacks and complex attacks such as VQA. Unfortunately, the evidence in this research is only the visual presentation of data without numerical data with TPR and TNR. Meanwhile, the imperceptibility level of the proposed method is also more than 51dB based on the PSNR value.

Study [20] also uses a method similar to research [19], namely LSB, SVD and ACM. The blocking technique is also carried out with the same size, namely 4×4. The difference is that this method can self-recover images with a 20-bits recovery, while the number of authentication bits used is 12-bits. This method is applied to medical images and obtains excellent FNR values for various general attack models and VQA. But the FPR value is around 0.31-0.89. Another measuring instrument NCC uses is the NCC value, which produces a value close to 1. For the imperceptibility aspect, PSNR is 51dB.

Research [2] proposed the SVD, LSB+MSB and logistic map methods focus more on tamper detection and localization processes. At the initial stage, the image is divided into small blocks measuring 2×2. While the 8-bits watermark is made with 6 MSB of pixel blocks, logistic maps and SVD. Watermark security is also enhanced with median value encryption. Embedding is done on 2-LSBs cover images. This method has advantages in tamper detection and localization with TPR value > 0.99, TNR and p = 1 for 100% tamper ratio. Tests were

carried out on various general and complex tamper such as VQA, CA, COA and CFA.

From the several state-of-the-art methods above, it appears that the use of SVD and LSB methods is one of the best combinations for designing fragile image watermarking. There is steganographic research [22] which uses the SVD diagonal. Bidiagonal SVD is claimed to be more secure than SVD to be applied to data hiding methods such as steganography and watermarking, so in this research the Bidiagonal SVD and LSB methods are proposed. A more detailed explanation of the research focus on tamper detection and localization, bidiagonal SVD and the proposed method is proposed in section 3.

3. Method

3.1 Tamper detection and localization

Tamper detection and localization is one of the most important processes in fragile image watermarking. The procedure for the tamper detection process is to identify and locate areas of the image that are suspected of having been tampered with or manipulated[1, 2, 18]. This is done by using an extracted watermark compared to the original. Generally, the shape of the tamper will form an area with a white or black color according to the area affected by the tamper. So the process of embedding the watermark must be done in such a way that it can form a pattern of the area affected by the tamper. The more similar the detected tamper area to the original one, the more reliable the method is. To do this, the embedding stage is generally added authentication bits. Generally by doing blocking techniques, in some research such as [2, 19, 20, 23] also uses the SVD method to generate authentication bits after blocking. Furthermore, to measure the accuracy of tamper detection can be used measuring instruments TPR, TNR and precision(p) which can be calculated with Eq. (1), Eq. (2) and Eq. (3) respectively.

$$TPR = \frac{TP}{TP+FN} \tag{1}$$

$$TNR = \frac{TN}{TN+FP} \tag{2}$$

$$p = \frac{TP}{TP+FP} \tag{3}$$

Where TP means the number of tampered blocks classified as tampered, FN means the number of tampered blocks classified as not tampered, TN means the number of untampered blocks classified as untampered, and FP means the number of untampered blocks classified as tampered. The perfect TPR, TNR and p values are 1.

3.2 Bidiagonal SVD

SVD is a tool that can transform a matrix (A) into three matrices, consisting of two orthogonal matrices (U and transpose V) and a diagonal/singular matrix (S). SVD can be calculated by Eq. (4), more detailed description of SVD can be seen in Eq. (5) [24].

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & & \\ \vdots & & \ddots & \\ a_{m,1} & & & a_{m,n} \end{bmatrix} = USV^T \tag{4}$$

$$\begin{aligned} U &= \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,m} \\ u_{2,1} & u_{2,2} & & \\ \vdots & & \ddots & \\ u_{m,1} & & & u_{m,n} \end{bmatrix} \\ S &= \begin{bmatrix} s_{1,1} & 0 & \ldots & 0 \\ 0 & a_{2,2} & & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & 0 & s_{m,n} \end{bmatrix} \\ V &= \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & a_{1,n} \\ v_{2,1} & v_{2,2} & & \\ \vdots & & \ddots & \\ v_{n,1} & & & v_{m,n} \end{bmatrix}^T \end{aligned} \tag{5}$$

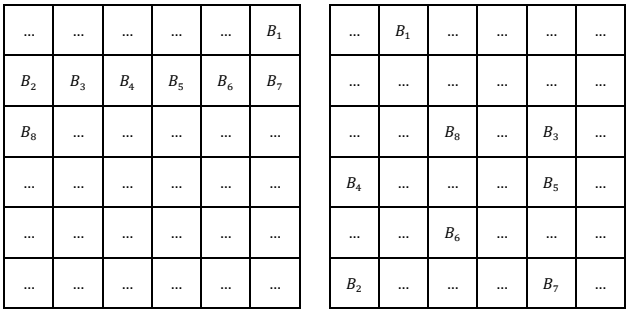
Where m,n is matrix size, $U^T U = I$ and $V^T V = I$, I is the identity matrix [25].

SVD has been widely used in image watermarking and steganography in data hiding science. The use of SVD in robust image watermarking is widely used because of its resistance to various geometric attacks, as well as superior stability [4, 26]. Meanwhile, the SVD method is widely applied in fragile image watermarking to generate authentication bits before the watermark embedding process [2, 19, 20, 23]. This proves that the use of SVD has an important role in various image watermarking methods.

The research [22] bidiagonal SVD (BSVD) method is proposed for image steganography. Steganography has something in common with watermarking, namely data embedding. BSVD is a derivative of SVD, which has similar values but a different approach. BSVD can be calculated by Eq. (6).

$$A = U_A B V_A^T \tag{6}$$

In BSVD U_A is an orthonormal matrix with size $m \times n$, V_A is a unitary matrix, and B is strictly an upper diagonal matrix. Bidiagonalization is the



(a) (b)

Figure 1. Block group in a scramble and after descramble image: (a) scramble blocks and (b) descramble blocks

decomposition of unitary matrices on dense, left and right unitary matrices. A series of Householder reflections achieve this process applied alternately from left and right, known as Golub - Kahan bidiagonalization. If the SVD is calculated by an iterative scheme to get a singular value, then the BSVD is obtained by calculating the finite operation. From Eq. (6) SVD of B can be calculated by Eq. (7). So the BSVD of A can be calculated by Eq. (8).

$$B = U_B B V_B^T \tag{7}$$

$$A = U_A U_B S V_B^T V_A^T \tag{8}$$

From the calculation example above, it can be concluded that the BSVD method logically produces better security for data hiding cases. Because to carry out the extraction process, more "keys" are needed. In particular, making authentication bits is more complex and secure for fragile image watermarking.

3.3 Proposed scheme

Based on the results of state-of-the-art identification in section 2, as well as analysis and hypotheses from sections 3.1 and 3.2, the study proposes the fragile image watermarking method by combining the 8×8 blocking method followed by the bidiagonal SVD and LSB to improve detection and localization for authentication performance. At the same time, they are increasing the imperceptibility of watermarked images. In detail, this method is described in two main processes, the first is embedding, and the second is extraction and tamper detection.

3.3.1 Embedding stage

The embedding stage requires input as a cover image and a watermark. The recommended watermark size is the same as the cover image size or the same as the block size. The difference is that the cover image has a depth of 8 bits and the watermark image has a depth of 1 bit or a binary image. So the embedding capacity in this method is 1 bit per byte. For this method to be strong from complex attacks such as VQA, CA, COA and CFA, the group block technique was adopted from [19]. In more detail, the embedding process is explained as follows:

1. The cover image that has been read is stored in the CI variable, then replaced with all LSBs on all pixels in the block to zero.
2. Next, the blockwise process is carried out with a size of 8×8 on the cover image with size $N \times N$, where $N = 512$, so 4096 blocks will be generated.
3. Do Arnold chaotic map for the scrambling block with Eq. (9)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \left(mod \sqrt{NB}\right) \tag{9}$$

Where x, y is block position, x', y' is block position after scrambling, a, b is a positive integer, NB is the number of blocks.

4. Perform BSVD on each block, then take each matrix S. Then trace with a map with a range of [0 65,536]. In this process, authentication bits will be obtained for each block ($AutB$) with a length of 16 bits, see Eq. (10).

$$AuthB_{xy} = \left\lfloor Trace_{xy}\ mod\ 65536 \right\rfloor \tag{10}$$

Where $Trace_{xy}(x, y \in [1, \frac{N}{8}]$

5. From all existing blocks, do grouping for every 8 blocks. Then descrambling the block so that the position of the block group becomes random, see Fig.1
6. Calculate the 16-bit $AutG$ value by calculating the absolute mean value of $AutB$ and then modulus 65,536, see Eq. (11).

$$AutG_{ij} = \left| \frac{\sum AutB_{xy}}{8} \right| mod\ 65536 \tag{11}$$

7. Extends AutG bit to 48bit with joint function like Eq.(12).

$$AutG_{ij} = joint(AutG_{ij}, \sim AutG_{ij}, AutG_{ij} \oplus AutG_{ij}) \tag{12}$$

Make a logistic sequence so that it produces a length of 64 sequences with adaptive parameters (pa) with a range of [3, 3.5], based on the mean value of block pixels, such as Eq. (13).

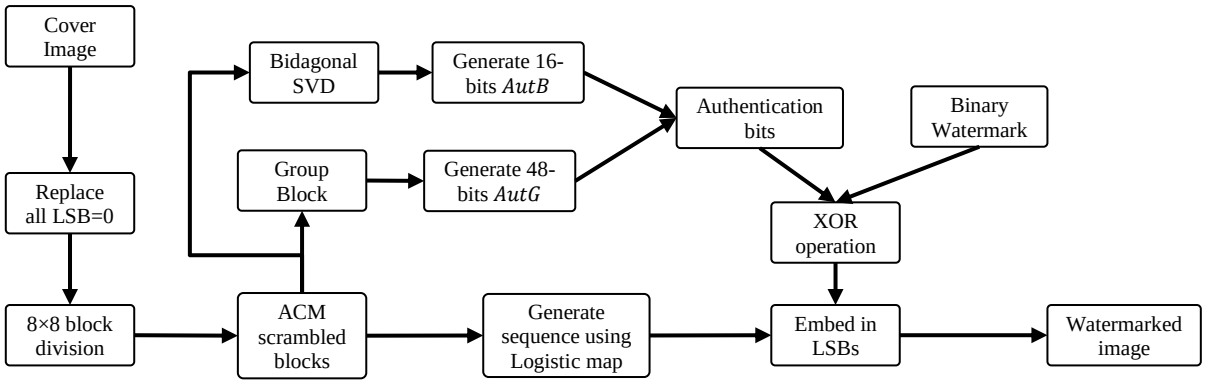


Figure. 2 Embedding scheme

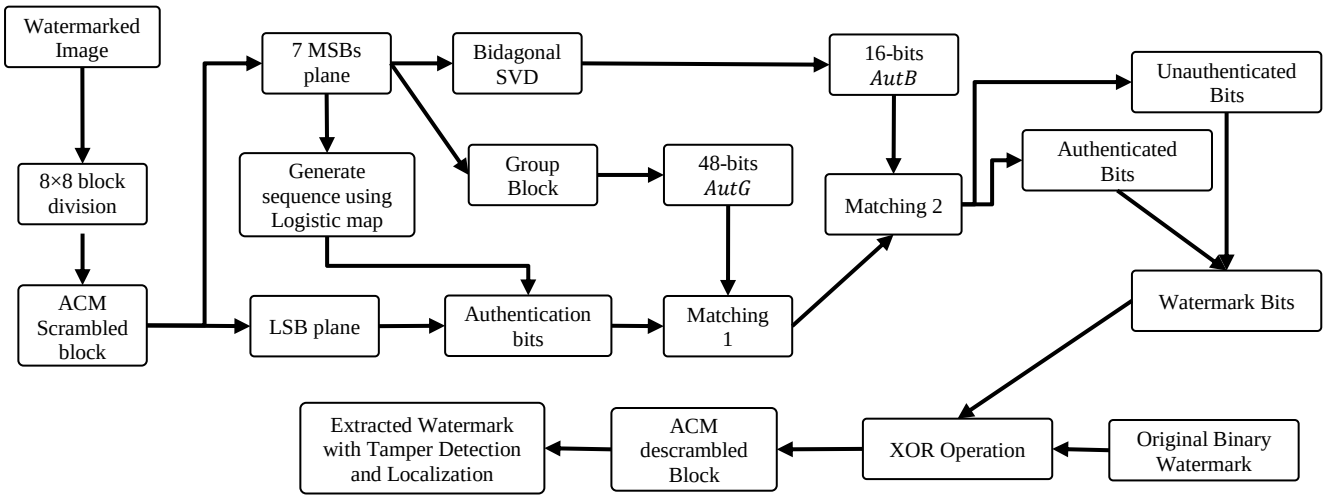


Figure. 3 Extraction scheme

$$pa = 3 + \left(\left(\frac{\sum px_{pq}}{64} - \left\lfloor \frac{\sum px_{pq}}{64} \right\rfloor \right) \times 0.5 \right) \quad (13)$$

8. Combine $AutB$ and $AutG$ so that 64-bit authentication is obtained, then XOR with a binary watermark image to produce an auth binary watermark image.
9. Embed the auth binary watermark image according to the high-order logistics sequence on the LSB pixel block.
10. Repeat step 9 until all blocks are embedded with an auth binary watermark so that a watermarked image with a size of $N \times N$ is obtained.
11. To measure the imperceptibility quality of the watermarked image, use the PSNR and SSIM measuring instruments, each with Eq. (14) and Eq. (15) [13].

$$psnr = 10log_{10}\left(\frac{max_{px}^2}{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(W_{ij} - O_{ij}\right)^2} \right) \quad (14)$$

$$ssim = \frac{(2\mu_O\mu_W + C_1)(2\sigma_{OW} + C_2)}{(\mu_O^2 + \mu_W^2 + C_1)(\sigma_O^2 + \sigma_W^2 + C_2)} \quad (15)$$

$$C_1 = (0.01 \times D)^2$$

$$C_2 = (0.03 \times D)^2$$

Where W for watermarked image, O for the original cover image, max_{px} for the largest pixel value of the cover image, μ for luminance mean intensity, σ for contrast standard deviation, and D for pixel value dynamic range. To illustrate the proposed embedding stages, see Fig. 3.

3.3.2 Extraction and tampering detection stage

Tampering detection and localization are integrated with the extraction stage. Two inputs are also needed at this stage: the watermarked image and the original binary watermark. As an illustration of the proposed extraction process, see Fig. 3, and further explained as follows:

1. Read the watermark image and then break it into small blocks with a size of 8×8.
2. Do scrambling on watermarked image blocks.
3. Split the image into two parts, namely the LSB plane and the 7-MSBs plane

Figure. 4 Image dataset used: (a) baboon, (b) cameraman, (c) F16, (d) Lena, (e) Lake, (f) 5555.pgm, (g) 10000.pgm, and (h) binary watermark

Table 1. Imperceptibility measurement results

Image	PSNR (dB)	SSIM
Baboon	51.984	0.9983
Cameraman	51.632	0.9981
F16	51.983	0.9987
Lena	51.8311	0.9990
Lake	51.7267	0.9982
5555.pgm	51.9827	0.9998
10000.pgm	51.8709	0.9997
Avg 100 img	51.8501	0.9991
Avg all Image	51.8576	0.9989

4. Generate sequence using logistic map using the 7-MSBs plane, then generate authentication bits using LSB and the sequence.
5. On the image blocks on the 7-MSB plane do BSVD and then take the singular matrix to generate 16-bit $AutB$.
6. Generate 48-bit $AuthG$ by performing a group block process.
7. Use 48-bit $AutG$ and authentication bits for matching process on each block
8. Use 16-bit $AutB$ and authentication bits for the second stage of the matching process, the result will be two kinds of bits, namely bits with a value of 0 as authentication bits and bits with a value of 1 for unauthentication bits.
9. Combine authentication bits and unauthentication bits into one matrix of watermark bits.
10. Read the original binary watermark image then perform the XOR operation with the watermark bit
11. Perform ACM descramble block, then get extracted watermark image with tamper detection and localization
12. To measure the quality of tamper detection and localization, use the TPR, TNR and precision measuring instruments contained in Eqs. (1-3).

4. Implementation and analysis

The study was tested using several images on a standard dataset that can be downloaded at [27], and 100 sample images from BossBase 1.01 dataset [28]. All images used are 512×512 with 8-bit depth, while the watermark image uses images of the same size with 1-bit depth or binary images. In Fig. 4 is a sample dataset used in this research.

It should be noted that all image datasets are not preprocessed, such as cropping or resizing, and all images have the same size. It's just that the entire BossBase dataset is re-saved with the bitmap(BMP) extension. Similarly, all watermarked images are saved with the BMP extension after embedding. The entire testing process is carried out with the Matlab 2016a application. Implementation of the method, the watermarked image is saved with the extension bitmap (bmp). The results of the embedding process are presented in Table 1. While the sample results are presented in Fig. 5

Based on the data presented in Table 1, it can be seen that the proposed method has an average PSNR value of more than 52dB, as well as an SSIM value of more than 0.999. This value indicates that the imperceptibility quality of the proposed method is in the very good category both in terms of error rate and based on structure, luminance or image contrast. [13].

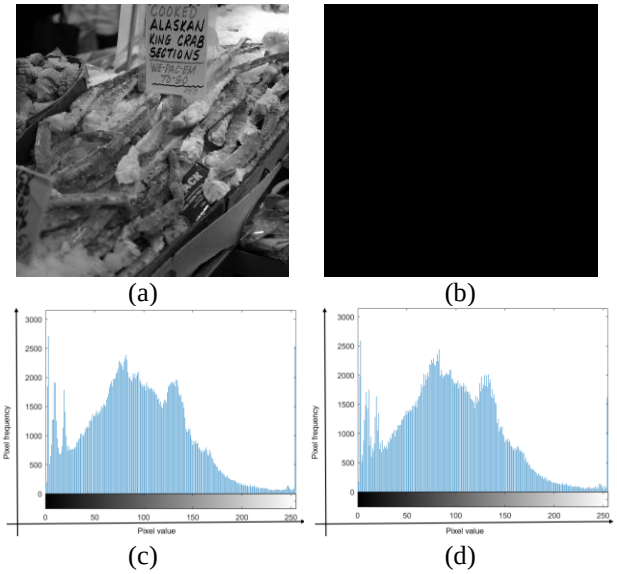


Figure. 5 Sample watermarked image results: (a) watermarked 10000.pgm.bmp, (b) tamper detection without attack, (c) original histogram and (d) watermarked histogram

Table 2. Average imperceptibility comparison

Method	PSNR (dB)	SSIM
Method [19]	51.14	-
Method [14]	51.14	0.9969
Method [10]	51.14	0.9978
Method [2]	44.16	-
Proposed	51.83	0.9985

Fig. 5 (a) also shows that visually the watermarked image has no visible difference, as well as in Fig. 5 (c) and (d), it appears that the histograms of the two images are very minimally different and appear identical. As a comparison of the average PSNR and SSIM results on the standard image dataset (without the Boss base dataset) is presented in Table 2. It can be seen the proposed method is superior in imperceptibility quality, both based on PSNR and SSIM values.

In the extraction and tamper detection stages, the proposed method is tested with three tamper detection measuring instruments, namely TPR, TNR and precision. These three measuring tools have been discussed in section 3.1. Fig. 5 (b) shows that tamper detection results on watermarked images without attack can be carried out perfectly. The TPR, TNR and precision values are all 1. However, the tamper test needs to be carried out. Several samples of the tamper testing performed are shown in Table 3.

Based on the data shown in Table 3, the proposed method has very good results in various attacks, especially in various complex attacks and some general attacks, except for noise addition and

Table 3. Average imperceptibility comparison

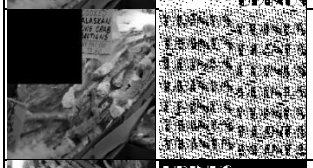
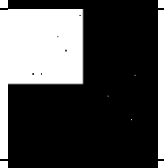
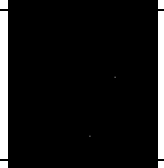
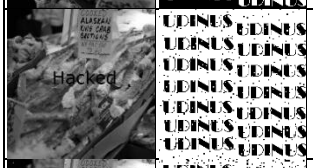
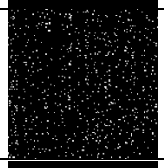
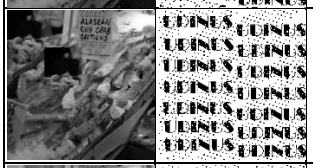
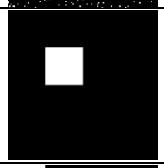
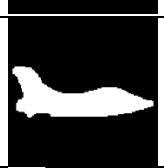
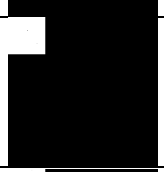
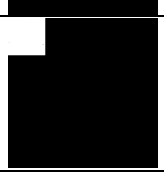
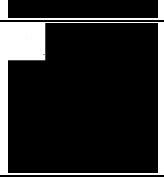
Attack Results	Extracted Watermark	Results	Attack Type Results
			Cropping 6.25% TPR=1 TNR=1 p=1
			Cropping 25% TPR=0.9907 TNR=0.9753 p=0.9853
			Rotate 90° TPR=0.9985 TNR=0.9957 p=0.9971
			Text Addition TPR=0.9931 TNR=0.9865 p=0.9850
			Noise Addition TPR=0.9873 TNR=0.9582 p=0.9598
			Copy Paste Type I TPR=1 TNR=1 p=1
			Copy Paste Type II TPR=0.9998 TNR=0.9997 p=0.9998
			VQA TPR=0.9935 TNR=0.9917 p=0.9898
			CA TPR=0.9997 TNR=0.9998 p=0.9998
			COA TPR=0.9998 TNR=0.9999 p=0.9998
			CFA TPR=0.9997 TNR=0.9997 p=0.9996
Average	TPR = 0.9964	TNR=0.9907	p=0.9916

Table 4. Average tamper detection comparison

Method	TPR	TNR	Precision	Attack types
Method [20]	0.9933	-	-	Copy-paste type I&II, content removal, text addition, VQA
Method [14]	0.9800	-	0.9755	Text addition, Noise addition, cropping attack
Method [10]	1.0000	-	-	Copy-paste type I&II, content removal, text addition, noise addition, VQA, CA, COA, CFA
Method [2]	0.9979	0.9999	0.9999	Copy-paste type I&II, content removal, text addition, noise addition, VQA, CA, COA, CFA
Proposed	0.9964	0.9907	0.9916	Cropping, Copy-paste type I &II, Rotate, Text addition, Noise addition VQA, CA, COA, CFA

cropping 25%. This method can only produce TPR, TNR and precision around 0.95, 0.98 and 0.95, respectively. The average value of TPR, TNR and precision of all attacks is around 9.99, compared with state-of-the-art methods in Table 4.

Based on the data presented in Table 4, it appears that the test results of the tamper detection method produce very good results, although they are not the most superior. For example, on [10], The test was carried out on TPR without TNR and precision. Actually, there are other measuring instruments used besides TNR, namely FPR. The value is the opposite of TNR, where the FPR value must be close to zero to get an excellent value. Although the TPR produces a perfect score, the FPR value in the study [10] is inconsistent, especially in the noise addition attack, the value of FPR = 27,588, which is the same as TNR = 72,412. The proposed method, on average, is not superior to the research [2], but the difference is not far. Compared to the imperceptibility side, the proposed method is superior to all state-of-the-art methods, see Table 2. This shows that the hypotheses described in sections one and two are proven. Using bidiagonal SVD can improve the authentication and imperceptibility process. But BSVD cannot be separated from its combination with blockwise and group block methods to ward off complex attacks.

5. Conclusions

The fragile image watermarking method is used to perform the image authentication process. This method is designed to be fragile against tampering but able to detect tamper and localize it. This study proposes a combination of BSVD, blockwise and block group methods to improve the authentication process. Using a larger sub-block size, the authentication bit size is enlarged and tends to be more secure. It has been proven that the proposed method has an excellent tamper detection rate with TPR = 0.9964, TNR = 0.9907 and precision = 0.9916 from the average of all types of standard and complex attacks. Another important aspect of fragile image watermarking is imperceptibility. Applying the LSB method for embedding combined with BSVD and ACM processes for processing watermarks before embedding succeeded in increasing imperceptibility with an average PSNR = 51.8576 and SSIM = 0.9989. It can be clearly concluded that the proposed method is strong against damage detection and imperceptible. In the future, this research needs to be improved to be able to recover image damage from various attacks.

Conflicts of interest

We wish to confirm no known conflicts of interest associated with this publication. There has been no significant financial support for this work that could have influenced its outcome. We also confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed.

Author contributions

Conceptualization, Nova Rijati; Methodology, Nova Rijati; Software, De Rosal Ignatius Moses Setiadi; Validation, De Rosal Ignatius Moses, and Nova Rijati; Formal analysis, Nova Rijati; Investigation, Nova Rijati; resources, Pulung Nurtantio Andono; data curation, Nova Rijati; writing—original draft preparation, Nova Rijati; writing—review and editing, Pulung Nurtantio Andono and De Rosal Ignatius Moses Setiadi;

visualization, Nova Rijati and De Rosal Ignatius Moses Setiadi; supervision, Nova Rijati; project administration, Nova Rijati.

Acknowledgments

The authors are grateful for the support for research funding in 2022 with numbers 158/E5/PG.02.00.PT/2022,158/E5/PG.02.00.PT/2022, 055/F9/UDN.09/VI/2022 provided by the Ministry of Research and Technology / National Research and Innovation Agency".

References

[1] M. Hussan, S. A. Parah, A. Jan, and G. J. Qureshi, "Hash-based image watermarking technique for tamper detection and localization", *Heal. Technol. 2022 122*, Vol. 12, No. 2, pp. 385–400, Jan. 2022, doi: 10.1007/S12553-021-00632-9.

[2] N. R. Neena and R. Shreelekshmi, "Fragile watermarking scheme for tamper localization in images using logistic map and singular value decomposition", *J. Vis. Commun. Image Represent.*, Vol. 85, p. 103500, 2022, doi: 10.1016/j.jvcir.2022.103500.

[3] A. A. Mohammed, M. A. M. Abdullah, F. S. Alghareb, and S. R. Awad, "A Novel FDCT-SVD Based Watermarking with Radon Transform for Telemedicine Applications", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 1, pp. 64–74, 2022, doi: 10.22266/IJIES2022.0228.07.

[4] A. Setyono and D. R. I. M. Setiadi, "Robust Video Watermarking using Tchebichef Transform and Singular Value Decomposition on the Selected Frame Based YCbCr Color Space", *Int. J. Intell. Eng. Syst.*, Vol. 13, No. 6, pp. 432–441, 2020, doi: 10.22266/ijies2020.1231.38.

[5] N. Rijati, P. N. Andono, and D. R. I. M. Setiadi, "Imperceptible Improvement using Edge Area Selection for Robust Video Watermarking Using Tchebichef - Singular Value Decomposition", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 2, pp. 298–306, 2022, doi: 10.22266/ijies2022.0430.27.

[6] H. M. A. Otum, "Colour Image Authentication and Recovery Using Wavelet Packets Watermarking", *Circuits, Syst. Signal Process.*, Vol. 41, No. 6, pp. 3222–3264, 2022, doi: 10.1007/s00034-021-01927-y.

[7] H. M. A. Otum, "Dual image watermarking using a multi-level thresholding and selective zone-quantization for copyright protection, authentication and recovery applications", *Multimed. Tools Appl.*, pp. 25787–25828, 2022, doi: 10.1007/s11042-022-11920-5.

[8] R. Sinhal and I. A. Ansari, "Multipurpose Image Watermarking: Ownership Check, Tamper Detection and Self-recovery", *Circuits, Syst. Signal Process.*, Vol. 41, No. 6, pp. 3199–3221, 2022, doi: 10.1007/s00034-021-01926-z.

[9] R. Munir and Harlili, "A Secure Fragile Video Watermarking Algorithm for Content Authentication Based on Arnold Cat Map", In: *Proc. of 2019 4th Int. Conf. Inf. Technol. Encompassing Intell. Technol. Innov. Towar. New Era Hum. Life, InCIT 2019*, pp. 32–37, Oct. 2019, doi: 10.1109/INCIT.2019.8912074.

[10] N. R. N. Raj and R. Shreelekshmi, "Blockwise Fragile Watermarking Schemes for Tamper Localization in Digital Images", In: *Proc. of 2018 Int. CET Conf. Control. Commun. Comput. IC4 2018*, pp. 441–446, 2018, doi: 10.1109/CETIC4.2018.8530950.

[11] L. Rakhmawati, T. Suryani, W. Wirawan, S. Suwadi, and E. Endroyono, "Exploiting self-embedding fragile watermarking method for image tamper detection and recovery", *Int. J. Intell. Eng. Syst.*, Vol. 12, No. 4, pp. 62–70, 2019, doi: 10.22266/ijies2019.0831.07.

[12] C. C. Lin, S. L. He, and C. C. Chang, "Pixel-based fragile image watermarking based on absolute moment block truncation coding", *Multimed. Tools Appl.*, Vol. 80, No. 19, pp. 29497–29518, 2021, doi: 10.1007/s11042-021-10598-5.

[13] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", *Multimed. Tools Appl.*, Vol. 80, No. 6, pp. 8423–8444, 2021, doi: 10.1007/s11042-020-10035-z.

[14] A. K. Sahu, "A logistic map based blind and fragile watermarking for tamper detection and localization in images", *J. Ambient Intell. Humaniz. Comput.*, No. 0123456789, 2021, doi: 10.1007/s12652-021-03365-9.

[15] R. Sinhal, I. A. Ansari, and C. W. Ahn, "Blind Image Watermarking for Localization and Restoration of Color Images", *IEEE Access*, Vol. 8, pp. 200157–200169, 2020, doi: 10.1109/ACCESS.2020.3035428.

[16] S. S. Bharti, S. Shivani, S. K. Pandey, and S. Agarwal, "An Efficient Blind Fragile Watermarking Scheme for Tamper Localization", *Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH*, Vol. 287, 2022, pp. 749–757.

[17] F. Nejati, H. Sajedi, and M. Mohammadi,

"Fragile Watermarking for Image Authentication Using QR factorization and Fourier Transform", In: *Proc. of 2019 5th Int. Conf. Web Res. ICWR 2019*, pp. 45–49, 2019, doi: 10.1109/ICWR.2019.8765292.

[18] S. K, M. K, and P. Kora, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine", *Biomed. Signal Process. Control*, Vol. 55, p. 101665, 2020, doi: 10.1016/j.bspc.2019.101665.

[19] Q. Kang, K. Li, and H. Chen, "An SVD-based fragile watermarking scheme with grouped blocks", In: *Proc. of 2nd Int. Conf. Inf. Technol. Electron. Commer. ICITEC 2014*, pp. 172–179, 2014, doi: 10.1109/ICITEC.2014.7105595.

[20] A. Shehab *et al.*, "Secure and robust fragile watermarking scheme for medical images", *IEEE Access*, Vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[21] Z. F. Makhrib and A. A. Karim, "Improved Fragile Watermarking Technique Using Modified LBP Operator", In: *Proc. of the 2nd 2022 International Conference on Computer Science and Software Engineering*, pp. 132–137, 2022, doi: 10.1109/CSASE51777.2022.9759647.

[22] M. S. Subhedar and V. H. Mankar, "Secure image steganography using framelet transform and bidiagonal SVD", *Multimed. Tools Appl.*, pp. 1–22, Nov. 2019, doi: 10.1007/s11042-019-08221-9.

[23] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, and S. Sadeghi, "An effective SVD-based image tampering detection and self-recovery using active watermarking", *Signal Process. Image Commun.*, Vol. 29, No. 10, pp. 1197–1210, Nov. 2014, doi: 10.1016/J.IMAGE.2014.09.001.

[24] M. Ali, C. W. Ahn, M. Pant, and P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony", *Inf. Sci. (Ny).*, 2015, doi: 10.1016/j.ins.2014.12.042.

[25] V. Santhi and A. Thangavelu, "DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition", *Int. J. Comput. Electr. Eng.*, Vol. 3, No. 1, pp. 8–16, 2011, Accessed: Sep. 02, 2019. [Online]. Available: http://www.ijcee.org/papers/285-E285.pdf.

[26] A. Setyono and D. R. I. M. Setiadi, "An Image Watermarking Method Using Discrete Tchebichef Transform and Singular Value Decomposition Based on Chaos Embedding", *Int. J. Intell. Eng. Syst.*, Vol. 13, No. 2, pp. 140–150, 2020, doi: 10.22266/ijies2020.0430.14.

[27] Ming Hsieh Department of Electrical Engineering USC Viterbi School of Engineering, *SIPI Image Database*, http://sipi.usc.edu/database/ (Accessed Mar. 27, 2019).

[28] P. Bas, T. Filler, and T. Pevný, " 'Break our steganographic system': The ins and outs of organizing BOSS", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 6958 LNCS, pp. 59–70, 2011, doi: 10.1007/978-3-642-24178-9_5.