Self-embedding and Variable Authentication Approach for Fragile Image Watermarking Using SVD and DCT

B. S. Kapre[1](✉), A. M. Rajurkar[1], and D. S. Guru[2]

[1] Department of Computer Science and Engineering, MGM's College of Engineering, Nanded, India
{kapre_bs,rajurkar_ab=m}@mgmcen.ac.in

[2] Department of Studies in Computer Science, University of Mysore, Manasagangotri, Mysore, India
dsg@compsci.uni-mysore.ac.in

Abstract. In this paper, we propose a self-embedding fragile image watermarking technique based on Singular Value Decomposition (SVD) and Discrete Cosine Transform (DCT). To improve security and robustness a novel block separation technique is presented in which an input image is divided into non-overlapping blocks and subsequently SVD is applied on each block. Entropy value of the resulting vector of singular values is measured. Mean of entropy of all blocks is considered as a threshold for deciding two sets of blocks. For the first set of blocks, Entropy measures of singular value based authentication codes are generated and for second set of blocks, DCT DC value based authentication codes are obtained for embedding information. To enhance visual quality of watermarked and recovery image DCT based watermark embedding technique is proposed. Experiments have been conducted on gray scale images and it is observed that proposed scheme gives peak signal to noise ratio (PSNR) of 58 dB which ensures high performance in terms of imperceptibility. Experimental results showed that 99% of watermarked blocks are correctly detected during recovery phase. The image tampering is precisely identified and tampered images are recovered with very good quality. To the best of our knowledge the presented fragile image watermarking scheme is superior to all existing scheme.

Keywords: Authentication code · Block separation · DCT · Entropy · SVD · Self-embedding · Fragile

1 Introduction

Advancement in the multimedia technologies has brought the whole world on one click. In every corner of the world, internet is being used as a means of communication for sharing files, images and videos. Considering widespread growth of internet, illegal usage of digital information and demand for strong data protection technology is greatly increased. Recently, due to the covid-19 pandemic, use of internet has increased drastically and because of social distancing and covid-19 restrictions, various types of human

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
D. S. Guru et al. (Eds.): ICCR 2021, CCIS 1697, pp. 366–379, 2022.
https://doi.org/10.1007/978-3-031-22405-8_29

activities such as learning, shopping, banking, meetings, working, and entertainment have shifted from offline to online mode. This has accelerated diffusion of emerging digital technology among ordinary people and most of our personal information is thus available online. Under these circumstances, integrity and authenticity verification of digital content has become an important research topic.

Based on authentication requirements in different domains, image authentication systems are classified into three types namely: robust watermarking [18–20], fragile watermarking [8, 14–17, 24–28], and semi fragile watermarking [22, 23]. Robust watermarking techniques are mainly used to prove ownership of the digital contents, wherein, watermark is successfully detected, even though watermarked images are distorted by common signal processing attacks. In Fragile image watermarking technique, watermark contents are highly sensitive to tampering and this technique can be used to detect and recover tampered area locations accurately. Semi-fragile watermarking techniques are combinations of robust and fragile watermarking system that are used to refuse reasonable content-preserving alteration and detect false modifications. In this paper, we have presented a novel self-embedding fragile watermarking scheme, with the intention to improve imperceptibility and robustness of the watermarked image as well as to achieve high level of tamper detection and recovery capability. To improve security level of proposed watermarking scheme a SVD based block separation technique is used to divide total non-overlapping blocks into two distant sets. Then, two authentication codes generation techniques are proposed using DCT and SVD. Recovery information is generated using DCT DC coefficients of each block, later the generated authentication codes are embedded into the cover image in DCT domain.

The rest of the paper is organized as follows. Section 2 highlights the related work; proposed watermarking embedding detection and recovery is illustrated in Sect. 3. Section 4 provides the experimental results. Finally, the paper is concluded in Sect. 5.

2 Related Work

Nowadays, image authentication has become an important research area. The aim of image authentication system is to detect the intentional and unintentional modification in multimedia content. Several watermarking schemes have been developed in the recent years [14–17] in spatial and frequency domain for authentication and recovering tampered area location in the digital image.

In this paper we focus on fragile image watermarking technique for tamper detection and localization in frequency domain. Fragile watermarking schemes are classified into two categories: pixel-based [1–5] and block-based [8, 14–28]. In pixel-based approach watermark is generated from the pixels of input image and is inserted into the input image and in the block-based fragile watermarking approach watermark information is generated form each block by dividing input image into non-overlapping blocks. Each block has watermark and each of them are protected by embedding watermark in it. If the watermarked image is tampered, the watermark information of a modified block is not successfully detected, and then that block is identified as a modified or tampered block.

Initially, Fragile watermarking technique was proposed in 1995 [1], in which checksum were calculated using 7-MSBs of each image pixel and inserted into the LSB of pixel. Though, this method was simple, but it fails to detect tampered image. To overcome this drawback many researchers have presented improved techniques. In 2007 [2] authors have introduced a chaotic pattern and pixel pattern based fragile watermarking technique. In which binary watermark image was obtained by mapping the difference between host image and chaotic pattern image. Then the watermark image was embedded in LSB bits of host image. To localize tampered image content effectively an algorithm was proposed in [3] wherein, the watermark embedding was performed in two phases. In the first phase authentication code is generated from robust bits of each pixel and it is embedded into pixels of host image. In the second phase embedded and generated authentication codes were compared to detect tempered image. Authors of [3] have presented two more fragile watermarking methods [4] and [5]. In [4, 5] they have proposed fragile watermarking methods to detect tampered locations. In which authentication code was generated for each pixel by calculating hamming code from four MSBs and inserted into LSBs of same pixel. The proposed technique effectively detects tampered location even at pixel level. Usually, embedding watermark in LSBs leads to improve visual quality of watermarked image. In some research work, for improving performance fragile watermarking systems, encryption techniques [6–8] have been employed.

SHA-256 hash function based watermark generation method was proposed in [9]. In this block based fragile watermarking scheme original image was divided into blocks of size 32 × 32 and each block was further divided into 16 × 16 four sub-blocks. The 256-bit binary watermark was generated by applying SHA-256 hash function on first three sub-block and embedded into LSBs of fourth sub-block. Tamper detection was done by comparing extracted and generated watermark. But this method fails to recover watermark. In 2019 [10] authors have proposed image tampering and recovery based fragile watermarking method. DCT based authentication codes was generated and block-dependency based tamper detection technique was used that provides accurate tamper detection. Further, K-means clustering technique was used to generate recovery information. This presented technique provides effective tamper detection and recovering capability.

Two fragile watermarking techniques have been introduced by Singh D. et al. [11, 12]. First technique based on DCT was introduced in 2016, wherein two-bit authentication code and ten-bit recovery information was generated from each non-overlapping block. Generated authentication code was embedded into two LSBs of a block itself and recovery information was embedded into three LSBs of mapped blocks. This method has shown good detection and recovery capability. Second method was introduced in 2017, wherein 12-bit watermark information was generated from five MSB bits and embedded in three LSBs of mapped blocks. The technique performs well in terms of tamper localization and image recovery was achieved up to 50%. Fragile watermarking technique based on two different recovery codes has been proposed in [13]. In this scheme, three LSBs were removed before dividing image into non-overlapping sub-blocks of size 2 × 2. SVD was performed on each sub-block to obtain eigenvectors and those are converted into 9-bits sequence. Two bits authentication code for each sub-block was generated using 9-bits sequence for each block. Recovery code was generated after analyzing block textures. For the smooth blocks, recovery code was created by extracting five MSBs from the mean value of each block and for the textured block; DC and AC coefficients of DCT were used to create recovery information. Further, authentication code and recovery code were combined to get watermark for each block and finally, LSB technique was used for watermarked image generation. It is observed that the quality of recovered image was not acceptable in this method for blocks having complex texture.

In 2018 [14] watermark bit reduction based AMBTC technique was employed to divided watermark into two quantization values and, a bitmap. These watermark parts were embedded into LSBs of the input image. In this presented fragile watermarking technique tamper detection was done by comparing tampered image and decoded image. Recovery information which was extracted from watermark was used to recover tampered image. Tampering rate achieved in this technique was less than 50%. To improve the quality of watermarked image and recovered image the bit reduction based AMBTC technique was introduced in [15] to generate watermark of fewer bits. In which, fewer bit watermark was generated and embedded into the input image using turtle shell based technique. Two level tamper detection techniques were employed to improve the accuracy of tamper localization. The presented technique improves the quality of watermarked and recovered image compared to [14]. Furthermore, the tampered image can be perfectly recovered when the tampering rate is 50%.

Block-based fragile watermarking technique was proposed by Javier et al. [16]. Input image is divided into non overlapping block to generate watermark for recovery and authentication code. To increase the quality of watermarked image, watermark was embedded using bit adjustment method. Recovered image quality was increased by employing bilateral filtering and inpainting algorithm. In this technique tamper recovery rate was improved up to 80%. To improve tampered image quality, a self-embedding image authentication algorithm based on SVD is presented in [17], in which each non-overlapping block was divided into upper and bottom parts. After block separation, authentication codes were generated by applying SVD on both parts of each block and then they were concatenated to generate watermark. This algorithm provides good visual imperceptibility against a variety of attacks in addition to that used to detect tampered locations. It has high tampering ratio and very low PSNR 46 dB. Temper detection and self-recovery based watermarking technique was introduced in [16] wherein color image is partitioned into two non-overlapping block and embedding sequence was generated using permutation process. Watermark was embedded into different blocks using the generated sequence. This technique provides security and improves imperceptibility of watermarked image.

In literature on fragile watermarking schemes, it is observed that most of the existing techniques suffer from low quality of watermarked and recovered image. Major drawback of these schemes is use of same authentication code generation technique used for every block. To overcome these shortcomings, we presented a novel variable authentication generation approach to produce different authentication codes for different sets of blocks. A DCT based watermarking technique is used to improve imperceptibility and robustness.

3 Proposed Work

The proposed self-embedding fragile image watermarking scheme is described in two sections. In the first section block separation, authentication code generation, recovery information generation and embedding process are presented and in the second section tamper detection technique and recovery is described.

3.1 Watermarking System

In the proposed watermarking scheme, the first step is to calculate recovery information, in which the given original image is divided into non-overlapping sub-blocks of size 8 × 8 and DCT is employed on each sub-block to get DC coefficient. The DC coefficient of each sub-block is stored in matrix and the generated matrix is used as recovery information. Further, a block partitioning is done in second step, in which SVD is performed on each non-overlapping block of size 64 × 64 of original image to get U, D and V matrices. Then, k singular values are extracted from D diagonal matrix, where, k denotes the number which is 75% of total singular values in diagonal matrix of SVD. Entropy of those singular values is calculated by normalizing each singular value. Mean of entropies of all the blocks is decided as the threshold for getting two sets of blocks, Set1 and Set2. In the third step, authentication codes for each set of blocks are generated. For the Set1 authentication code is generated using entropy based singular value measures by employing SVD on each block and for Set2 authentication code is generated by applying DCT on each sub-block. However, DC coefficients of the two neighboring sub-blocks have certain correlation. By considering the relationship between two neighboring DC coefficients, we first scramble the position of block using a seed K1. Then DC coefficients of scrambled blocks are compared to get authentication code for Set2. In the fourth step, the generated authentication code is embedded in their respective block and respective Set using DCT transform. In this manner we obtain the watermarked image. Figure 1 shows the complete workflow of watermarking system and the related mathematics are explained in respective section.

The detailed steps of block selection, authentication code generation, recovery information generation and embedding are explained in the following section:

Step1: DC-Rmatrix: Original Image X is divided into non overlapping blocks of size 8 × 8. Then DCT is applied on each sub-block to get DC coefficient. Each DC coefficient is divided by 8 and stored into matrix to get DC- recovery matrix DC-Rmatrix.

Step2: Block Separation: Entropy based Block Separation technique is proposed to separate all non-overlapping blocks into two sets. In this step, the original image X is divided into non-overlapping block of size (64 × 64). Then SVD is applied on each sub-block (64 × 64) to get three matrices U, D and V [22]. Further, first k singular values $\boldsymbol{\sigma_k} = (\boldsymbol{\sigma_1}, \boldsymbol{\sigma_2}, \boldsymbol{\sigma_3} \ldots \boldsymbol{\sigma_k})$ are extracted from D matrix. Then each singular value is normalized σ_k as (1):

$$\boldsymbol{\sigma_k} = \frac{\boldsymbol{\sigma_k}}{\sum \boldsymbol{\sigma_i}} \tag{1}$$

Entropy value of all k singular values is calculated using following Eq. (2):

$$\boldsymbol{E_\sigma} = \sum \boldsymbol{\sigma_k} \, \boldsymbol{log}(\boldsymbol{\sigma}_{\boldsymbol{k}}) \tag{2}$$

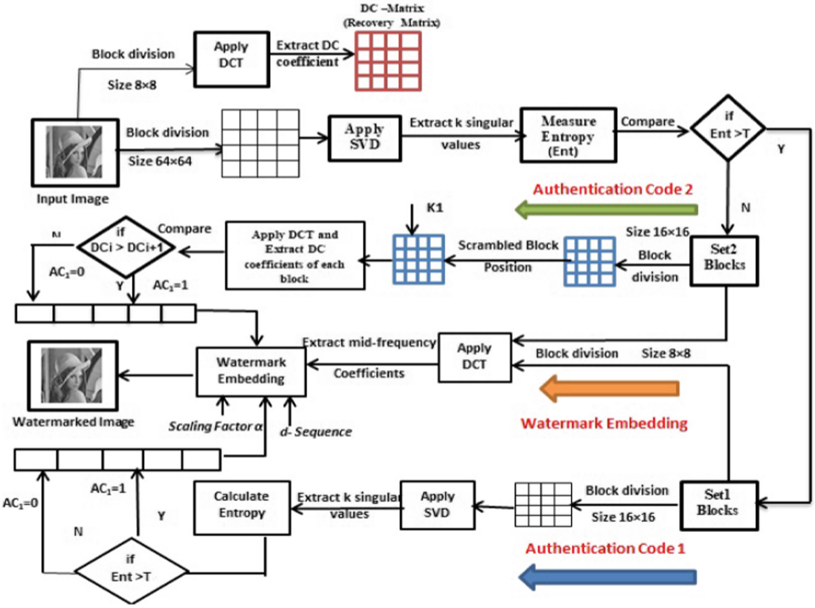

Fig. 1. Watermark embedding and authentication code generation

All entropy values are then compared with the threshold T to get two sets of block. Where, T is decided as a mean of all entropy values. Comparison equation is as follows (3):

$$\boldsymbol{Selected_{Block}} = \begin{cases} \boldsymbol{if\ E_\sigma \geq TSet1 = \{b_i, b_{i+1}\ldots\}} \\ \boldsymbol{elseSet2 = \{b_j, b_{j+1}\ldots\}} \end{cases} \tag{3}$$

Step 3: Generation of Authentication Codes AC1 and AC2 for Set1 and Set2 Respectively: Authentication code for each set of blocks is generated by dividing each block into non-overlapping blocks of size 16 × 16. To avoid false positive problem, authentication code $\boldsymbol{AC}1_{\boldsymbol{b}_i}$ for each block of Set1 is generated using the same procedure described above in Step-2. Entropies $\boldsymbol{E_{b\sigma}}$ of all blocks are calculated and authentication code $\boldsymbol{AC}1_{\boldsymbol{b}_i}$ is generated by comparing all entropy values with threshold (mean of entropy value) using following Eq. (4).

$$\boldsymbol{AC1_{Set1_b}} = \begin{cases} \boldsymbol{if\ E_{b\sigma} \geq TAC1_{b_i} = 1} \\ \boldsymbol{else\,AC1_{b_j} = 0} \end{cases} \tag{4}$$

Another authentication code $\mathrm{AC2_{b_i}}$ for each block of Set2 is generated by employing DCT on each 16 × 16 block. It is found that, magnitude relationship between DC coefficients of two neighboring blocks is changed because the neighboring blocks have certain correlation. So to improve the robustness of the $\mathrm{AC2_{b_i}}$, block positions are scrambled using seed K1. Then DC coefficients of scrambled blocks are compared to get authentication code $\mathrm{AC2}_{\mathrm{bj}}$ using Eq. (5)

$$.\mathbf{AC2}_{\boldsymbol{Set2_b}} = \begin{cases} \boldsymbol{if\, DC_{b(k)} \geq DC_{b(k+1)} AC2_{bj} = 1} \\ \boldsymbol{else\, AC2_{bj} = 0} \end{cases} \tag{5}$$

Step 4: Embedding: The generated authentication codes of respective block B is embedded in the same block using scaling factor '$\boldsymbol{\alpha}$' and decimal sequence '$\boldsymbol{d}$' which is generated using prime number. Each block of size 64 × 64 is partitioned into sub-blocks of size 8 × 8. DCT is applied on each sub-block. Generated authentication code is inserted into mid-frequency coefficient of DCT. Following Eq. (6) is used for embedding watermark in DCT domain.

$$\boldsymbol{I'_{mid}(i,j)} = \begin{cases} \boldsymbol{I_{mid}(i,j) + d} & \boldsymbol{if\ I_{mid}(i,j) > 1}\ \mathit{and}\ \boldsymbol{AC_n = 1} \\ \boldsymbol{I_{mid}(i,j) + \alpha * d} & \boldsymbol{if\ I_{mid}(i,j) \leq 1\ and\ AC_n = 1} \\ \boldsymbol{I_{mid}(i,j) - \alpha * d} & \boldsymbol{if\ AC_n = 0} \end{cases} \tag{6}$$

where, $I'_{mid}(i,j)$ is the watermarked DCT mid frequency coefficient, $I_{mid}(i,j) =$ is the DCT mid frequency coefficient, α is the scaling factor, d is decimal sequence AC_n is the authentication code.

3.2 Tamper Detection and Recovery

In tamper detection process, initially we apply the procedure explained in Sect. 3.1 to produce authentication codes $\boldsymbol{AC'_n}$ for each block $\boldsymbol{B_i}$ of watermarked image. The authentication code $\boldsymbol{AC''_n}$, is extracted, which was embedded using DCT transform. Then both the authentication codes are compared. If $\boldsymbol{AC'_n \neq AC''_n}$, it is concluded that the block B is tampered. Figure 2 shows the workflow of tamper detection and image recovery procedure. In the rest of this section proposed tamper detection and recovery technique and related mathematics are explained in each step.

Step1: The watermarked image X' is divided into non-overlapping block B of size 64 × 64. Watermarked blocks are extracted using same procedure as mentioned in step 2 of Sect. 3.1. Same procedure explained in step 3 of Sect. 3.1 is used to generate authentication code $\boldsymbol{AC'_n}$ for each block of image X' and embedded watermark $\boldsymbol{AC''_n}$ is extracted from the mid frequency coefficient by applying DCT using to Eq. (7).

$$\boldsymbol{AC''_n} = \begin{cases} \boldsymbol{0\ if\ I'_{mid}(i,j) \leq 0} \\ \boldsymbol{1\ if\ I'_{mid}(i,j) \geq 1} \end{cases} \tag{7}$$

Step 2: *If any difference is found between* $\boldsymbol{AC'_n}$ *and* $\boldsymbol{AC''_n}$*, then the block is marked as tampered using Eq. (8).*

$$\begin{cases} \boldsymbol{if \left(AC1'_{b(i)} = AC2'_{b(i)}\right) Not\ tampered} \\ \boldsymbol{if\ AC1'_{b(i)} \neq AC2'_{b(i)}\ tampered} \end{cases} \tag{8}$$

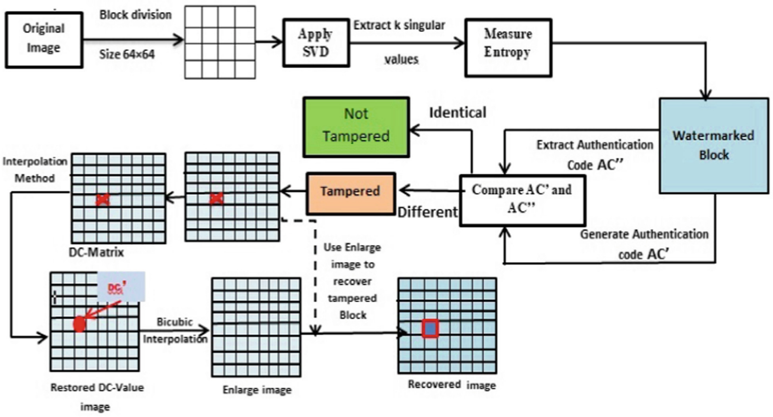

Fig. 2. Tamper detection and recovery

Step 3: If the block is tampered, image is reconstructed using the recovery information from each block. Tampered block is recovered using interpolation technique [10]. In this technique resized image is generated using recovery information DC-Rmatrix to the same size of original image X. When the image block is tampered, it is recovered by replacing it with a block which has the same block position in the resized image. Finally, the recovery image XR generated.

4 Experimental Results

In this section, we evaluate and analyze the performance of the proposed method in four aspects: correctness of block selection, watermark imperceptibility, tamper detection, and self-recovery ability. Eight standard test images such as Lena, Boat, Baboon, Couple, Barber, Airplane, Lake, and Pepper of sized 512 × 512 are used for experiments to demonstrate the effectiveness of the proposed scheme and are shown in Fig. 3.

Watermarked image quality determines the performance of watermark imperceptibility. The better the quality of watermarked image, the better is its invisibility [10–14]. A good PSNR value is obtained when the watermarked image and the original image are visually identical, which is calculated using following Eq. (9)

$$\mathrm{PSNR} = 10 \times \log \frac{255^2}{\frac{1}{\mathrm{m \times n}} \sum_{\mathrm{i=1}}^{\mathrm{m \times n}} ((\mathrm{X(i)} - \mathrm{T(i)})^2} \tag{9}$$

To measure the quality of image a standard tool Structure Similarity Index Measures (SSIM) is used that measures quality of image, which measures similarity between two images from three aspects: brightness, contrast and structure. If the two images are same from structural prospective then the value of SSIM is equal to 1.0. SSIM is calculated using following Eq. (10)

$$\mathrm{SSIM(O, W)} = \frac{(2\mu_{\mathrm{O}}\mu_{\mathrm{W}} + \mathrm{C1})(2\sigma_{\mathrm{OW}} + \mathrm{C2})}{\left(\mu_{\mathrm{O}}^2 + \mu_{\mathrm{W}}^2 + \mathrm{C1}\right)\left(\sigma_{\mathrm{O}}^2 + \sigma_{\mathrm{W}}^2 + \mathrm{C2}\right)} \tag{10}$$

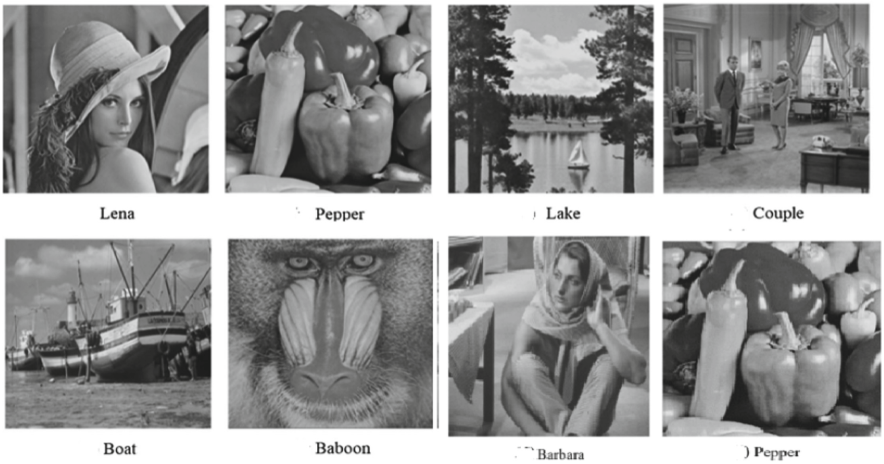

Fig. 3. Samples of grayscale images

where, O and W are the original and watermarked image respectively, μ_O is the mean of original image whereas μ_W is the mean of watermarked image, σ_O^2 and σ_W^2 are variance of original and watermarked image respectively, C1 and C2 are the constants.

First of all we analyzed the performance of presented entropy based block effect of block size(8 × 8, 16 × 16, 32 × 32 and 64 × 64) on precision and recall of entropy based block separation. It was observed that higher the block size better is the precision and recall. Hence, we have chosen block size of 64 × 64. To test resistance to different types of attacks the test images were distorted with different types of noise. Even then, it was observed that the precision and recall for block size 64 × 64 obtained was very good i.e. 99%. Figure 4 shows that the correctness of block separation using proposed approach is improved for fragile watermarking scheme.

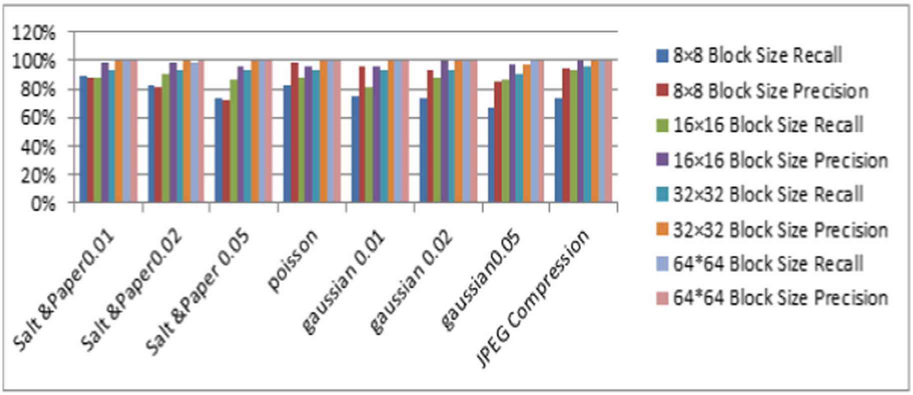

Fig. 4. Performance measure for correctness of block separation of proposed approach

From the experimentation it is revealed that our scheme provides high PSNR which is a measure of imperceptibility. Table 1 shows the PSNR and SSIM values of the proposed scheme on different test-images and it is observed that, PSNR value of all the images is above 57 dB and SSIM is in 0.99. Figure 5 shows the results of tamper detection and image recovery after removal of 10% to 50% content. It is observed that the PSNR of recovered image is ranging from 42 dB to 49 dB.

Table 1. Comparison of PSNR and SSIM using different test-images for proposed system

Image	PSNR	SSIM
Lena	59.2088	0.9999
Lake	59.1662	0.9999
Pepper	59..4618	0.9999
Boat	58.7956	0.9989
Baboon	57.0704	0.9979
Cameraman	63.5076	1.00
Average	**59.5497**	**0.9994**

Table 2. Comparison of quality of watermarked image between proposed and previous methods.

Image	Chin-Chen et al. [15]	Javier et al. [16]	Kim et al. [14]	Wang et al. [13]	Jau-ji [17]	Proposed
Lena	49.77	44.6	44.15	39.82	46.81	**59.2088**
Lake	49.76	--	44.15	38.91	46.82	**59.1662**
Pepper	49.76	44.54	44.13	40.63	46.93	**59..4618**
Boat	49.76	44.61	44.16	38.87	46.77	**58.7956**
Baboon	49.75	44.64	44.17	38.91	47.16	**57.0704**
Average	**49.76**	**44.59**	**44.15**	**39.42**	**46.89**	**58.56025**

In order to prove the effectiveness of the proposed scheme, we compared our scheme with five existing schemes such as: Chin-chan et al.'s [15], Javier et al.'s [16], Wang et al.'s [13], Kim et al.'s [14] and jau-ji et al.'s in [17]. Table 2 shows a comparison of our proposed method with existing methods [13–17] in terms of PSNR.. By using DCT the average PSNR value of watermarked image of proposed scheme has at least 10 dB improvements in comparison with other schemes. The average PSNR of proposed method is 58.56 dB and whereas for existing scheme it is less than 49.76 dB.

Table 3 presents a tamper tolerance and quality of watermarked image and recovered image between the proposed scheme and other reviewed techniques [13–17]. Our proposed methods provides good quality of recovered image, with an average PSNR of 45.51 dB, where tampering rate are set to from 5% to above 50%. However, it is observed

Table 3. Comparison of tamper tolerance and quality of watermarked image and recovered image

	PSNR (watermarked image)	PSNR (recovered image)	Tolerance
Chin Chen et al. [15]	49.76	32.30	<50%
Javier et al. [16]	44.59	26.00	<50%
Wang et al. [13]	39.42	32.05	<50%
Kim et al. [14]	44.15	31.89	<50%
Jau-ji [17]	46.89	35.65	<50%
Proposed	**58.56**	**45.51**	**>50%**

that the tolerable tampering rate of our method is above 50% and other methods are up to 50%. Even when tampering rate is greater than 50%, the image quality of recovered image is above 45 dM, which is greater than five existing methods [13–17] ranged from 26 dB to 35 dB.

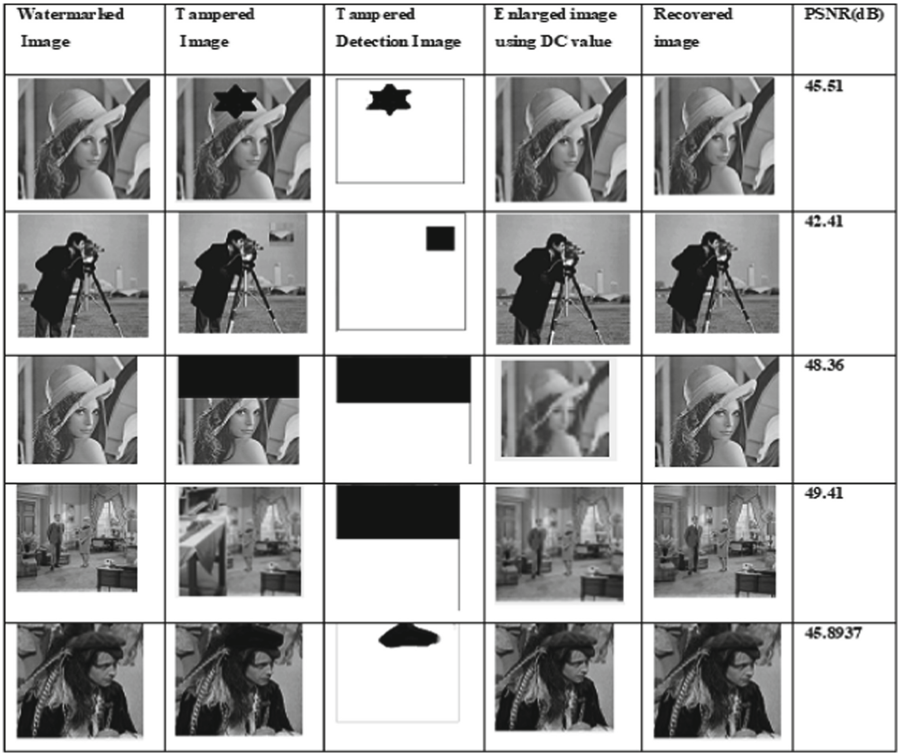

Fig. 5. Copy paste and collage attack on different images a) watermarked image b) tampered image c) tampered detection d) enlarged image e) recovered image. f) PSNR

5 Conclusion

In this paper, we have presented a self–recovery based fragile image authentication technique using DCT and SVD. It uses robust entropy based block separation technique to get two sets of blocks and the authentication code is generated for each set of block using two different methodologies. This variable authentication code generation approach improves the security level of proposed algorithm and the generated authentication code is embedded in DCT domain. In addition to this DC values of DCT are used in the proposed approach as recovery information which improves recovery ability.

To evaluate the performance of proposed scheme two measures precision and recall are used. Experiments are carried out on standard gray scale images. From the experimentation it is revealed that the proposed block separation technique is 99% accurate and it is shown that the quality of watermarked and recovered images is improved compared to existing approaches [13–17]. Proposed method also recovers tampered location back to its original place, without using original image. Simulation results show that PSNR and SSIM values of watermarked image are above 58 dB and 0.99 respectively and for recovered image PSNR is above 42 dB. In future, our research will focus on improving watermarked and recovered image quality as well as extend proposed method for video watermarking system.

References

1. Walton, S.: Image authentication for a slippery new age. Dr. Dobb's J. **20**(4), 18–22 (1995)
2. Liu, S.H., Yao, H.X., Gao, W., Liu, Y.L.: An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. Appl. Math. Comput. **185**(2), 869–882 (2007)
3. Prasad, S., Pal, A.K.: A tamper detection suitable fragile watermarking scheme based on novel payload embedding strategy. Multimed. Tools Appl. **79**(3–4), 1673–1705 (2019). https://doi.org/10.1007/s11042-019-08144-5
4. Prasad, S., Pal, A.K.: Hamming code and logistic-map based pixel-level active forgery detection scheme using fragile watermarking. Multimed. Tools Appl. **79**(29–30), 20897–20928 (2020). https://doi.org/10.1007/s11042-020-08715-x
5. Prasad, S., Pal, A.K.: A secure fragile watermarking scheme for protecting integrity of digital images. Iran. J. Sci. Technol. Trans. Electr. Eng. **44**(2), 703–727 (2019). https://doi.org/10.1007/s40998-019-00275-7
6. Dua, M., Suthar, A., Garg, A., Garg, V.: An ILM-cosine transform-based improved approach to image encryption. Complex Intell. Syst. **7**(1), 327–343 (2020). https://doi.org/10.1007/s40747-020-00201-z
7. Nancharla, B.K., Dua, M.: An image encryption using intertwining logistic map and enhanced logistic map. In: 2020 5th International Conference on Communication and Electronics Systems (ICCES), pp. 1309–1314. IEEE (2020)
8. Dua, M., Wesanekar, A., Gupta, V., Bhola, M., Dua, S.: Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. J. Ambient. Intell. Humaniz. Comput. **11**(9), 3771–3786 (2019). https://doi.org/10.1007/s12652-019-01580-z
9. Gul, E., Ozturk, S.: A novel hash function based fragile watermarking method for image integrity. Multimed. Tools Appl. **78**(13), 17701–17718 (2019). https://doi.org/10.1007/s11042-018-7084-0

10. Abdelhakim, A., Saleh, H.I., Abdelhakim, M.: Fragile watermarking for image tamper detection and localization with effective recovery capability using K-means clustering. Multimed. Tools Appl. **78**(22), 32523–32563 (2019)
11. Singh, D., Singh, S.K.: Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. J. Vis. Commun. Image Represent. **38**, 775–789 (2016)
12. Singh, D., Singh, S.K.: DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimed. Tools Appl. **76**(1), 953–977 (2015). https://doi.org/10.1007/s11042-015-3010-x
13. Wang, C., Zhang, H., Zhou, X.: A self-recovery fragile image watermarking with variable watermark capacity. Appl. Sci. **8**(4), 548–568 (2018)
14. Kim, C., Shin, D., Yang, C.-N.: Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC. Pers. Ubiquit. Comput. **22**(1), 11–22 (2017). https://doi.org/10.1007/s00779-017-1061-x
15. Chang, C.-C., Lin, C.-C., Su, G.-D.: An effective image self-recovery based fragile watermarking using self-adaptive weight-based compressed AMBTC. Multimed. Tools Appl. **79**(33–34), 24795–24824 (2020). https://doi.org/10.1007/s11042-020-09132-w
16. Molina-Garcia, J., Garcia-Salgado, B.P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., Cruz-Ramos, C.: An effective fragile watermarking scheme for color image tampering detection and self-recovery. Signal Process.: Image Commun. **81**, 115725 (2020). https://doi.org/10.1016/j.image.2019.115725
17. Shen, J.-J., Lee, C.-F., Hsu, F.-W., Agrawal, S.: A self-embedding fragile image authentication based on singular value decomposition. Multimed. Tools Appl. **79**(35–36), 25969–25988 (2020). https://doi.org/10.1007/s11042-020-09254-1
18. Ahmadi, S.B.B., Zhang, G., Wei, S.: Robust and hybrid SVD-based image watermarking schemes. Multimed. Tools Appl. **79**(1), 1075–1117 (2020)
19. Singh, A.K.: Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed. Tools Appl. **76**(6), 8881–8900 (2016). https://doi.org/10.1007/s11042-016-3514-z
20. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed. Tools Appl. **77**(4), 4863–4882 (2016). https://doi.org/10.1007/s11042-016-3862-8
21. Qi, X., Xin, X.: A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J. Vis. Commun. Image Represent. **30**, 312–327 (2015). https://doi.org/10.1016/j.jvcir.2015.05.006
22. Li, C., Zhang, A., Liu, Z., Liao, L., Huang, D.: Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication. Multimed. Tools Appl. **74**(23), 10581–10604 (2014). https://doi.org/10.1007/s11042-014-2188-7
23. Klema, V., Laub, A.J.: The singular value decomposition: its computation and some applications. IEEE Trans. Autom. Control **25**(2), 164–176 (1980)
24. Botta, M., Cavagnino, D., Pomponiu, V.: Reversible fragile watermarking for multichannel images with high redundancy channels. Multimed. Tools Appl. **79**(35–36), 26427–26445 (2020). https://doi.org/10.1007/s11042-020-08986-4
25. Hemida, O., Huo, Y., He, H., Chen, F.: A restorable fragile watermarking scheme with superior localization for both natural and text images. Multimed. Tools Appl. **78**(9), 12373–12403 (2018). https://doi.org/10.1007/s11042-018-6664-3
26. Su, G.D., Chang, C.C., Lin, C.C.: Effective self-recovery and tampering localization fragile watermarking for medical images. IEEE Access **8**, 160840–160857 (2020). https://doi.org/10.1109/ACCESS.2020.301983216

27. AlShehri, L., Hussain, M., Aboalsamh, H., Wadood, A.: Fragile watermarking for image authentication using BRINT and ELM. Multimed. Tools Appl. **79**(39–40), 29199–29223 (2020). https://doi.org/10.1007/s11042-020-09441-0
28. Nejati, F., Sajedi, H., Zohourian, A.: Fragile watermarking based on QR decomposition and Fourier transform. Wirel. Pers. Commun. **122**(1), 211–227 (2021). https://doi.org/10.1007/s11277-021-08895-1