IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 13, 2017, accepted January 14, 2018, date of publication February 6, 2018, date of current version March 15, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2799240

Secure and Robust Fragile Watermarking Scheme for Medical Images

ABDULAZIZ SHEHAB[1], MOHAMED ELHOSENY[1], KHAN MUHAMMAD[2], ARUN KUMAR SANGAIAH[3], PO YANG[4], HAOJUN HUANG[5], AND GUOLIN HOU[6]

[1]Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[2]Intelligent Media Laboratory, Digital Contents Research Institute, Sejong University, Seoul 143-747, South Korea
[3]School of Computing Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
[4]Department of Computer Science, Liverpool John Moores University, Liverpool L3 5UA, U.K.
[5]Department of Computer science, College of Computer, China University of Geosciences, Wuhan 430074, China
[6]Science and Technology on Near-surface Detection Laboratory, Wuxi, China

Corresponding Author: Guolin Hou (honeyline@126.com)

This work was supported by the National Natural Science Foundation of China under 61402343.

ABSTRACT Due to the advances in computer-based communication and health services over the past decade, the need for image security becomes urgent to address the requirements of both safety and non-safety in medical applications. This paper proposes a new fragile watermarking-based scheme for image authentication and self-recovery for medical applications. The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block wise SVD into the least significant bit of the image pixels to figure out the transformation in the original image. Two authentication bits namely block authentication and self-recovery bits are used to survive the vector quantization attack. The insertion of self-recovery bits is determined with Arnold transformation, which recovers the original image even after a high tampering rate. SVD-based watermarking information improves the image authentication and provides a way to detect different attacked area of the watermarked image. The proposed scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared with the state-of-the art methods, the proposed scheme greatly improves both tamper localization accuracy and the peak signal to noise ratio of self-recovered image.

INDEX TERMS Medical image security, tamper localization, singular value decomposition, fragile watermarking, arnold transformation, image security, authentication.

I. INTRODUCTION

With the development of computer-based communication in health services applications, the need for medical image security is urgent to protect the patients' sensitive data. Medical image analysis aims to solve medical problems using different imaging modalities and digital image analysis techniques. Images are easily manipulated using image processing tools, which have serious consequence [1]. Hence, protecting the credibility and respectability of medical images is of a significant importance [2], [3]. There are two main types of image verification strategies: cryptography based techniques [4], [5] and fragile watermarking based techniques [6]–[8]. A message authentication code (MAC) is computed in the cryptography based techniques, which utilizes a hash function to calculate the same code. Such MAC codes can decide whether an image tampering occurred without the ability to determine its region [9]–[11]. Fragile watermark is inserted in the image, which needs to be protected from the unauthorized access. To ensure the validity of a watermarked image, the fragile watermark needs to be produced using features of the host image or using pseudo deterministic random information of the host. Some fragile watermarking based schemes can only sense the tampered host images and are not able to self-recover the original host image [12]. The first known fragile watermarking scheme was proposed by Walton [14], which calculates the check sum of the first seven most significant bits (MSB) and provides limited alter recognition [16]. Yeung and Mintzer [8] implemented a watermarking method centered on pseudo-random sequence generation. In this method, a fragile watermark is implanted into the original host image using modified error diffusion. It suffers from fake image generation using a look up table [15].

TABLE 1. Summary of popular and recent image analysis watermarking works.

Paper	Block Size	Methodology	Tamper Detection Accuracy (%)	Recovered PSNR (dB)	Main Limitation
Walton [13]	N/A	LSB insertion	Very limited (10%)	N/A	One single LSB change can be detected
Yeung and Mintzer [8]	4×4	Chaotic pattern	70%	N/A	Not able to sustain VQ attack
Shao-Hui Liu *et al*. [14]	4×4	Chaotic pattern	85%	N/A	No self-recovery
Sanjay Rawat *et al*.[17]	4×4	Advance level of chaotic pattern	98%	N/A	No self-recovery
Patra *et al*. [20]	8×8	Chinese remainder theorem	93%	36dB	Low tamper localization
Dhole *et al*. [19]	4×4	Mean value of block	98%	34dB	Low self-recovery

This problem occurs because of the block independent nature of image watermarking. The watermarking that does not involve any blocks dependency can simply be damaged with specialized attacks such as Vector Quantization (VQ) attack [16]. The invader deduces the forged image with the aid of quantization code-book in VQ attack. This code book is created from a set of watermarked images. As each block validates itself only, the forged image seems to be true. To overcome VQ attack, [14], [16] suggested the inclusion of chaotic pattern in the watermarking design, which later helps to trace the tampered region in the watermarked host image. A difference image is mapped to binary watermark image and is inserted into the host image using its LSB. Interfered pixels can still be recognized because they do not convey the watermark information. However, some information generated from the new pixel values may coincide with the watermark change which makes it hard to notice these pixels. In such case, the localization and finding of tampered pixels cannot be done precisely [18]. Dhole *et al.* [19] proposed a self-embedding watermark scheme from tamper recovery, which provides a good tamper localization but it was unable to deal with the VQ attack. Patra *et al.* [20] proposed a fragile watermarking method based on the Chinese remainder theorem (CRT). The main advantage of these methods was improved computational complexity. A block size of 8×8 is usually used to provide the tamper localization. It provides a poor accuracy for tamper localization because of the large block size. The recovered image shows a decent image quality (36.77 dB) after a minor tampering rate. SVD demonstrates the basic building of matrix along with its algebraic essence, which makes it useful in many of applications such as image watermarking, image compression, voice recognition, etc. There are many watermarking methods developed, which employ SVD [21]–[23]. For instance, Sun *et al.* [24] proposed a SVD based approach in the class of semi fragile watermarking. In this scheme, the watermark is implanted in the host image by calculating SVD and then quantizing the singular value of each image block. It provides no self-recovery feature. Table 1 gives a summary of recent works.

This paper proposes a SVD-based fragile watermarking scheme for tamper localization and self-recovery to protect the sensitive images in medical applications. Two codes are used: one code contains the average value of the block information itself whereas the second contains block authentication information. To find out the embedding position, Arnold transform has been utilized. This helps to hide the neighboring pixel information at a distant location and provides better self-recovery. The proposed scheme aims to localize the attacked pixels/region. The main contribution of this work is the usage of Arnold transform which provides a more reliable and secure way for hiding image information. Moreover, PSNR ratio could be improved through the neighborhood block based recovery which relies on the fact that neighborhood blocks of a pixel contain mostly similar information. Hence, randomized insertion of neighborhood block enhances the recovery chance of approximate value for the pixels that are lost or changed by the attacker.

The rest of paper is organized as follow: Section 2 gives a detailed description of our proposed watermarking scheme.

Section 3 discusses the results. Section 4 presents the conclusion of our work.

II. THE PROPOSED SCHEME

SVD can be directly applied on digital images as they are nothing but a representation (matrix form) of the non-negative scalars numbers. SVD [23] is a method of Linear Algebra that is used to diagonalize any given symmetric image to obtain three new matrices U, S and V, which are known by the name of singular matrix (left), singular matrix (right) and singular matrix, respectively. The same can be expressed in mathematical form as follows:

$$\mathrm{A} = \mathrm{USV}^{\mathrm{T}} \tag{1}$$

SVD decomposes the original matrix A to three matrices: U, S and V.

Matrix S follows few properties. For instance, it remains a rectangular diagonal matrix and the diagonal elements of singular matrix are kept on descending order. These diagonal elements of singular matrix are known as singular values. If the host image matrix 'A' has a size of $n \times n$, then the decomposed singular matrix S contains maximum ''n'' elements diagonally. These singular values contain the information about the participation of each layer in the final host image formation. The values of the singular elements show quite a robust nature towards intentional/unintentional attacks on host image. Thus, this property can be used to check the originality of the host image. If we use lesser elements of matrix S in the regeneration process of matrix A, then the image quality of regenerated image will get affected.

The left and right singular matrices follow the property $UU^T = I_n$ and $VV^T = I_n$. The singular values of diagonal matrix S follows the property.

$$\mathrm{s}_1 \geq \mathrm{s}_2 \ldots \mathrm{cs}_\mathrm{r} > \mathrm{s}_{\mathrm{r}+1} > \mathrm{s}_{\mathrm{r}+2} \ldots c > \mathrm{s}_\mathrm{n} = 0 \tag{2}$$

Here, ($\mathrm{r} \leq \mathrm{n}$) is showing the rank of the singular matrix S and $s_1, s_2 \ldots cs_n$ are singular values of matrix S.

To ensure the security of the host image blocks as well as provide self-recovery ability to the proposed scheme, the blocks need to be randomized in such fashion that it can only be reversed back by the unique key/code. Arnold transform is computed as follows:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_{i-1} \\ y_{i-1} \end{bmatrix} \bmod (\mathrm{h}) \tag{3}$$

where a and b are positive constant, which is used to determine the period of a given matrix. h is the size of the host image (Here we are considering a square image). $\boldsymbol{x_i}$ and $\boldsymbol{y_i}$ denotes the transformed value of $\boldsymbol{x}$ and $\boldsymbol{y}$ pixels after $\boldsymbol{i^{th}}$ number of iterations. The mathematical expression shown in Eqs (3) is periodic in nature (i.e. if we keep on transforming $\boldsymbol{x}$ and $\boldsymbol{y}$ elements then after a fixed numbers of repetitions '$\boldsymbol{T}$' the $\boldsymbol{x}$ and $\boldsymbol{y}$ elements repeat itself/ original values). $\boldsymbol{T}$ is known as time period of iteration and this time period $\boldsymbol{T}$ remain dependent on a, b and i. so these variables used to determine the key of the randomization process.

Let's suppose that 'i' transforms are followed during the element randomization stage. Then, to retrieve back the original host image, again (T-i) transforms needs to be applied on this pre-randomized image. As mentioned earlier, if we scramble the information throughout the image with the help of Arnold transformation and then perform a tampering of any type, the chances are quite high that some information will still remain undamaged.

To provide tamper localization in a host image and to recover the tampered region, the inserted watermark bits are made up of two different types:

1. Block authentication bits: The main idea behind the block authentication bits calculation is to authenticate each block separately. To achieve that purpose, host image is divided into 4×4 blocks and SVD is computed for each block. Then, traces of singular matrices are used as block authentication bit for each block.
2. Self-Recovery bits: The average values of the first 5 MSB are used as the self-recovery information for each 2×2.

This average helps us to recover the approximation of the original image in case it gets tampered. Another important aspect of proposed work is the use of randomized insertion of watermark information to improve the performance of the scheme. In order to provide a better self-recovery, Arnold transformation is used in present study so that neighborhood recovery information can be saved at distant locations. For each image block, these two types of bits (authentication and self-recovery) are hidden in the LSB of the block pixels. The positions used for insertion, are determined by the help of Arnold Transform, which is generated using a secret key and that key is only known to the owner of the image. If that key is changed, all the watermark bits can't be correctly extracted from the image block. Arnold transform provides an alternative way to recover the image data from the neighboring blocks when main information gets lost. So the use of Arnold Transform not only improves the security but also improves the performance of the proposed scheme. After that, the watermarked medical images are tested against various types of attacks to figure out its usefulness and efficiency.

A. WATERMARK EMBEDDING PROCESS

The diagram of our proposed method is shown in Figure 1. The host image is divided into small blocks of size 4×4 and the LSB of all these blocks are set as zero. This division guides us to calculate the tamper localization information for each block separately by the help of SVD operation on each 4×4 blocks. After SVD is computed for each block, the corresponding traces are also calculated. These calculated traces work as the Block Authentication Number (BAN) and used to authenticate each block. The traces are mapped to the range of [0, 4095] in order to restrict the number of bits as 12, used for the traces representation of each block. Further, block wise Arnold scrambling is performed and 4×4 blocks are again decomposed into 2×2 blocks as shown in figure 2 (a) so that neighborhood block is recovered. The

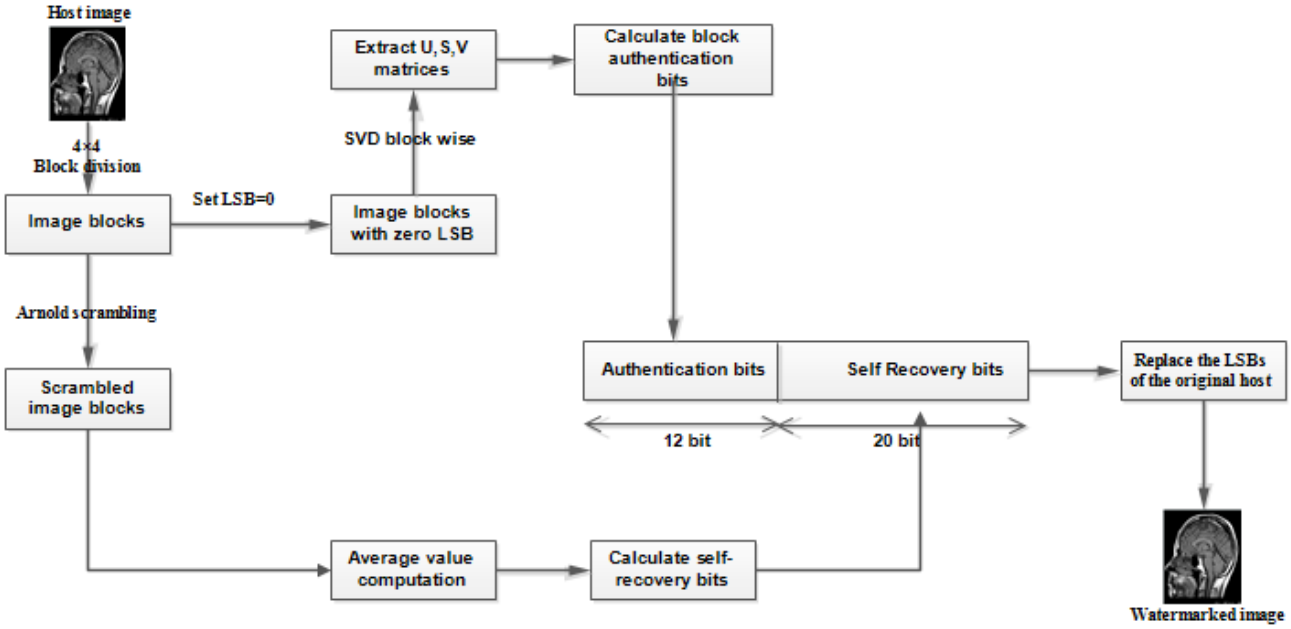


FIGURE 1. Block representation of watermark embedding method.

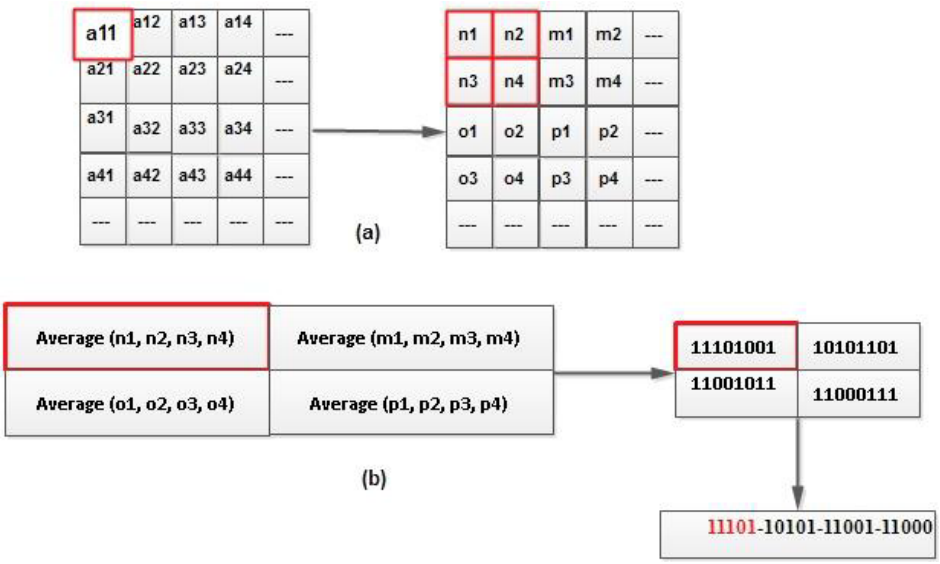


FIGURE 2. (a) Block division of 4 × 4 block (a11-a44) into 2 × 2 blocks (n1-n4, m1-m4, o1-o4, p1-p4) and (b) Average value computation from 5 MSB.

self-recovery information is calculated with the help of the average value of these 2 × 2 blocks as shown in figure 2 (b). The obtained BAN and average value of Arnold scrambled 4 × 4 blocks are combined with each other with the help of a secret key in order to generate the complete watermark information. This complete watermark is inserted into the host image by replacing the last two LSBs of each 4 × 4 block (32 bits) with the generated watermark information of each 4 × 4 block.

The last 2 LSB of each pixel i.e. 16 × 2 = 32 are replaced by the watermark.

B. WATERMARK EXTRACTION PROCESS

The extraction process is quite similar to that of embedding process. The block diagram of complete extraction process is shown in figure 3. Here are the details of step involved:

Firstly, the watermarked image is divided into small blocks of size 4 × 4. As the LSB contained the watermarked infor-

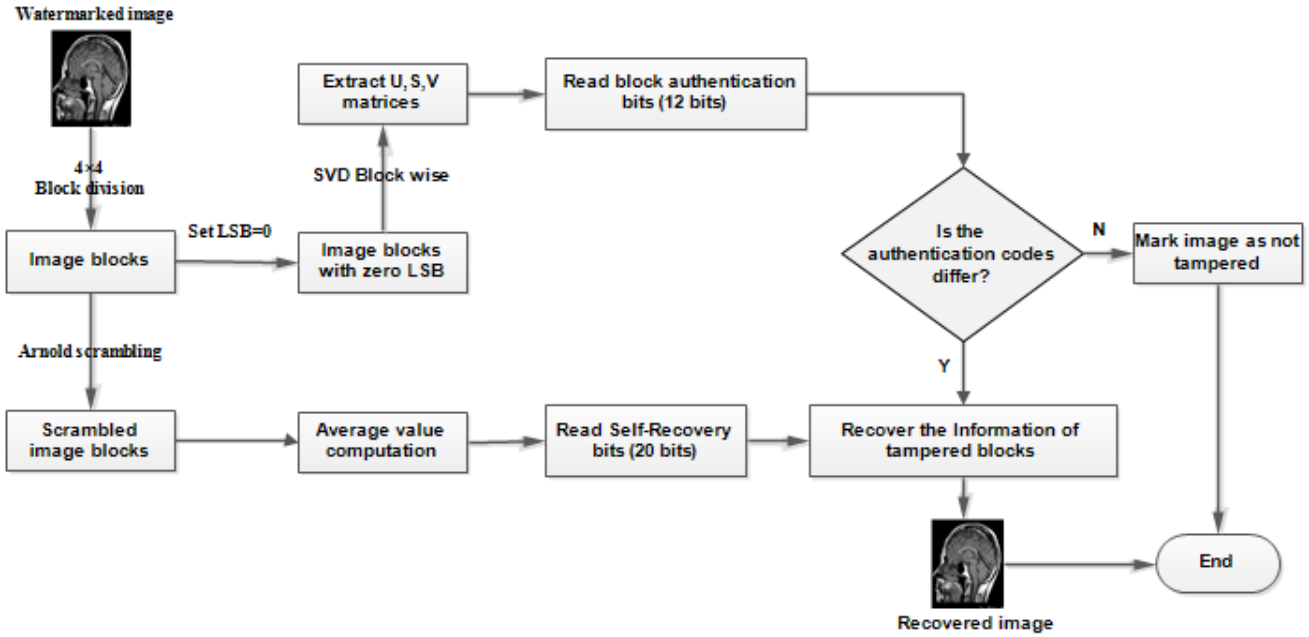


FIGURE 3. Block representation of tamper localization along with self-recovery using the extracted watermark.

mation so it is separated out from the watermarked image and then LSB is set as zero in order to re-calculate the Block Authentication Bits (12 bits). Then, BAN is calculated in the same way as calculated in embedding process. After that block based scrambling is performed on this watermarked image with the same key as used during embedding process. The average value and self-recovery information is calculated in the same way as it is done in embedding.

The calculated BAN and LSB extracted BAN are compared with other for each block along with the average information too. The blocks having same authentication bits are marked as not-tampered and rest are marked as tampered. Then, the tampered blocks information is recovered with the help of extracted self-recovery information from the extracted LSB data from watermarked image and finally the neighborhood block based recovery is performed in order to improve the self-recovery even further. This helps us to achieve the improved self-recovery because of the fact that neighborhood blocks of any image's pixels contain almost similar information.

III. RESULTS AND DISCUSSIONS

A. EXPERIMENTAL METRICS

In order to figure out the effectiveness of the proposed scheme, five different factors are calculated, which are defined as follows:

1) False positive rate (FPR) [28]: error in classifying non-tampered pixels as tampered ones. Mathematically defined as:

$$FPR = \frac{False\ classified\ pixels}{Total\ tampered\ pixels} \times 100 \tag{4}$$

2) False negative rate (FNR) [14]: error in classifying tampered pixels as non-tampered ones. Mathematically defined as:

$$\mathrm{FNR} = \frac{\text{False classified pixels}}{\text{Total non-tampered pixels}} \times 100 \tag{5}$$

3) Tamper detection rate (TDR) [18]: The detection rate of tampered pixels in the overall tampered area. Mathematically defined as:

$$\mathrm{TDR} = \frac{\text{Detected tampered pixels}}{\text{Total no. of tampered pixels}} \times 100 \tag{6}$$

It also called tamper localization accuracy.

4) Peak signal to noise ratio (PSNR) [29], [30]: is used to measure the accuracy of recovered image compared with the original image. it is used to describe the image quality. Mathematically defined as:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{n}\times\mathrm{n}\times(\mathrm{X}_{\max})^2}{\sum_{i=1}^{\mathrm{n}}\sum_{i=1}^{\mathrm{n}}(\mathrm{X}(\mathrm{i},\mathrm{j})-\mathrm{X}^*(\mathrm{i},\mathrm{j}))^2}\right) \tag{7}$$

Where $n \times n$ represent the size of host image, $X\ (i, j)$ is pixel of first image, $X^*\ (i, j)$ is pixel of second image and X_{max} is maximum allowed pixel intensity.

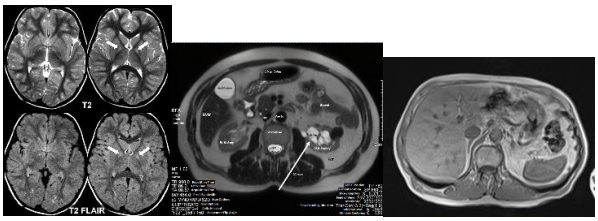
5) The normalized cross-correlation (NCC) [7]: check the similarity between two images. Mathematically defined as:

$$\mathrm{NCC}\left(\mathrm{X},\mathrm{Y}^*\right) = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}}\sum_{\mathrm{j}=1}^{\mathrm{n}}\overline{X_{(\mathrm{i},\mathrm{j})}\oplus Y^*_{(\mathrm{i},\mathrm{j})}}}{\mathrm{n}\times\mathrm{n}} \tag{8}$$

Here X and Y represent two matrices, whose similarity need to be checked and $\oplus$ represents the XOR operation. $n \times n$ is the block size.

TABLE 2. Comparison of accuracy and PSNR values with other techniques.

Type of Attack	Host images	Preda et al [27]		El'arbi et al [28]		Dhole et al [19]		Patra et al [20]		Proposed Scheme	
		Tamper Localization (%)	Recovered PSNR (dB)	Tamper Localization (%)	Recovered PSNR (dB)	Tamper Localization (%)	Recovered PSNR (dB)	Tamper Localization (%)	Recovered PSNR (dB)	Tamper Localization (%)	Recovered PSNR (dB)
Copy and paste Type 1	Plane	99.45	28.56	94.52	34.56	98.56	34.36	93.14	36.12	99.56	38.96
	Classic bicycle	99.65	27.54	94.24	36.69	97.34	34.55	93.56	35.98	99.34	37.95
Copy and paste Type 2	Barbara	98.65	28.69	94.36	35.41	96.26	34.65	93.27	36.02	99.26	38.54
	Classic bicycle	99.59	27.56	94.56	35.43	97.46	35.12	93.21	36.15	99.46	38.56
Text addition	Barbara	98.64	28.78	93.74	36.48	98.49	34.51	92.59	36.29	99.49	38.25
	Cameraman	99.56	25.56	92.69	35.56	98.17	34.25	92.04	36.54	99.17	38.15
Content removal	Lena	98.68	24.56	93.36	31.48	97.57	32.28	92.58	30.54	99.11	33.49
	Barbara	98.56	28.56	95.48	35.13	98.26	38.56	94.58	36.24	99.54	38.56
VQ	Lena+ Girl	99.56	28.54	91.25	29.16	0	12.56	0	12.56	99.02	30.25



(a) (b) (c)

FIGURE 4. Sample host images: (a) Brain (b) Kidney and (c) Liver.

B. EXPERIMENT ASSUMPTION

In our experiments, 12 grayscale medical images were used. The sizes of these images are 512×512 pixels. Figure 4 shows sample host images for brain, kidney, and liver used in this study. The watermark is generated from the host itself and inserted into the LSBs. The parameters for Arnold transform include $m = 1$, $n = 1$ and $i = 30$.

C. COPY AND PASTE ATTACK

Watermarked medical images are subject to different attacks. Two types of copy and paste attack have been performed over the watermarked medical images. The first type is applied to the same watermarked image. In 'brain' image, for example extra left ventricle in the brain has been copy and paste. In 'kidney' image, the outer tissue of left kidney has been copied from the left side to right side. In 'liver' image, cross-sectional area from the bottom has been copied to upper right corner. Figure 5 shows the visual results for copy and paste attack for a tampered host, a tamper localization and a self-recovered image. The results shows that the PSNR values of all watermarked images are in the range of 50.17dB and 51.25dB.

In the second attack, we copy some portion from liver to the brain watermarked image and vice versa. Figure 6 shows the results.

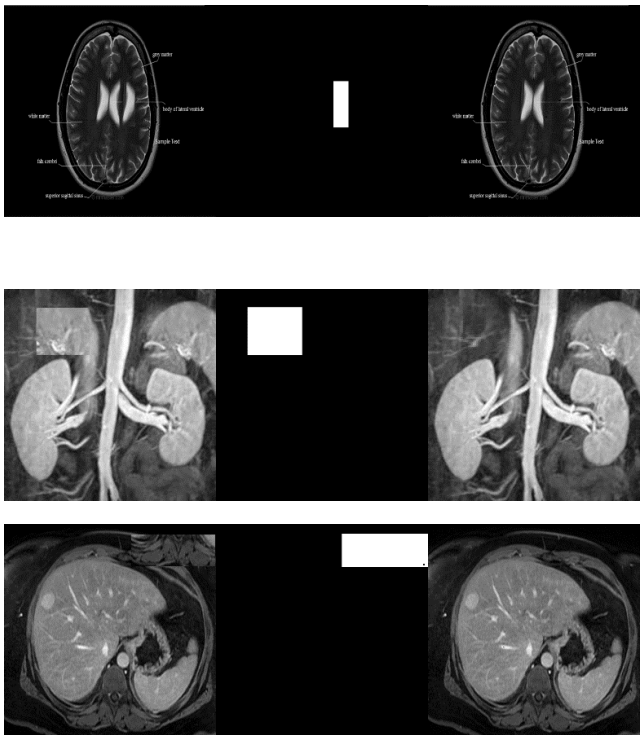


FIGURE 5. Result of copy and paste attack – Type 1: Attacked watermarked images (rightmost), localization of tamper (center), self-recovered host (leftmost).

D. TEXT ADDITION

In this attack, addition of text ''Sample Text'' has been done in different colors, location, and font sizes in brain, kidney, and liver host images. The result of text addition attack is shown figure 7.

E. CONTENT REMOVAL

In this type of attack, some content has been removed from watermarked medical images with no degradation of the image quality. The result of content removal attack is shown figure 8.

TABLE 3. The FPR, FNR, and NCC results using Copy and paste, Text addition, and Content removal attacks.

Type of Attacks	Host images	FPR	FNR	NCC_1	NCC_2
Copy and paste-Type1	Brain	0.41	0.008	0.9998	0.9982
	Kidney	0.35	0.007	0.9999	0.9980
	Liver	0.45	0.06	0.9998	0.9978
Copy and paste-Type2	Brain	0.39	0.008	0.9997	0.9982
	Kidney	0.36	0.008	0.9998	0.9984
	Liver	0.38	0.006	0.9996	0.9985
Text addition	Brain	0.31	0.007	0.9997	0.9983
	Kidney	0.42	0.008	0.9998	0.9982
	Liver	0.42	0.008	0.9998	0.9982
Content removal	Brain	0.51	0.01	0.9998	0.9978
	Kidney	0.38	0.008	0.9999	0.9982
	Liver	0.48	0.009	0.9996	0.9978
VQ	Brain+ Kidney	0.89	0.03	0.9997	0.9961

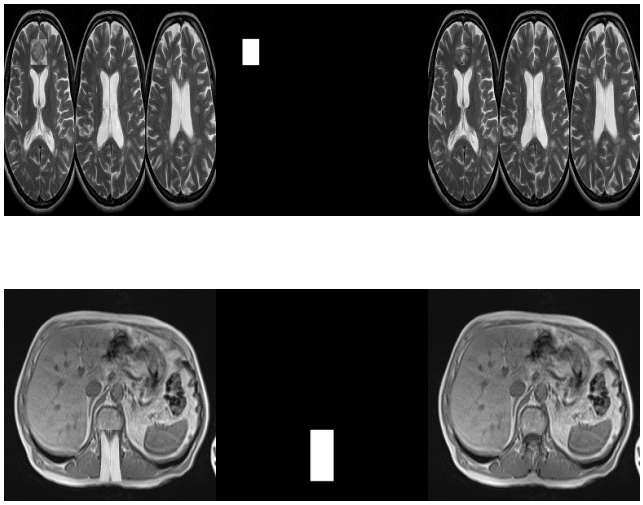


FIGURE 6. Result of copy paste attack – Type 2: Attacked watermarked Images (rightmost), localization of attack (center), self-recovered host (leftmost).

F. VQ ATTACK

To verify the working of proposed scheme with VQ attack, a forged image is designed by adding different parts of several watermarked images (watermarked with same method). During this construction, the relative spatial position of watermarked images is not important because all the blocks will get authenticated individually. A new host image for the brain has been taken in this experiment as shown in figure 9. The sizes of host images are 512 × 512 and the watermarked images have a PSNR as 50.97 dB and 51.03 dB respectively for 'brain' and 'kidney. The result of VQ attack is shown figure 9.

G. A COMPARISON STUDY

A comparison with existing methods is presented in Table 2 in terms of both tamper localization accuracy and the PSNR of self-recovered image.

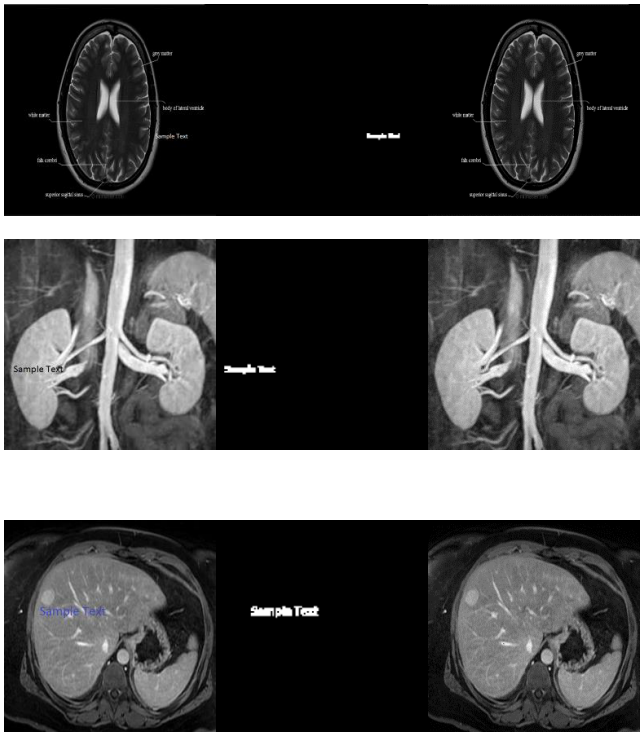


FIGURE 7. Result of text addition: Attacked watermarked Images (rightmost), localization of attack (center), self-recovered host (leftmost).

Table 3 summarizes the evaluation based on FPR, FNR and NCC (watermarked medical image) and NCC (recovered image) corresponding to different attacks. The FNR and FPR of the proposed scheme are quite low and pretty acceptable as we can see from Table 3. Even in case of vector quantization attack too, which indicates that our scheme is more efficient and accurate for practical usage. The NCC of the watermarked image (NCC_1) is very close to one, which indicates that the difference between watermarked image and original host image is quite small. Moreover, the NCC value of

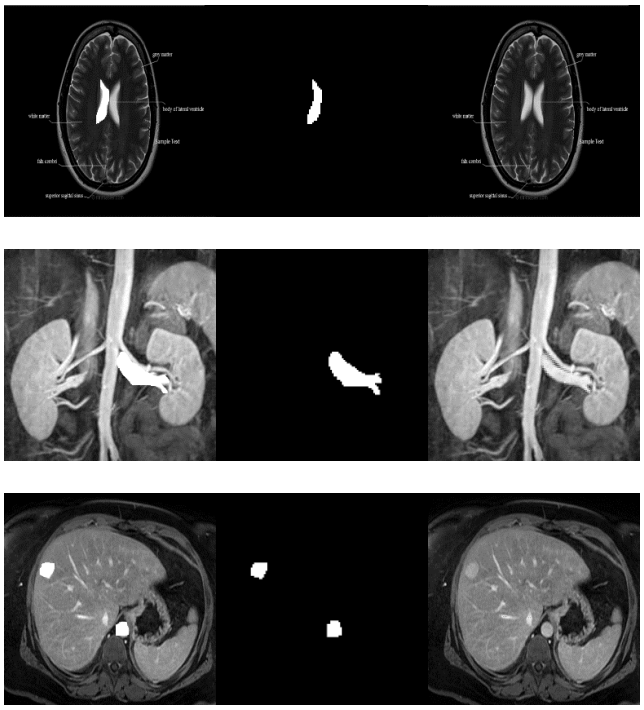


FIGURE 8. Result of content removal: Attacked Watermarked Images (rightmost), localization of attack (center), self-recovered host (leftmost).

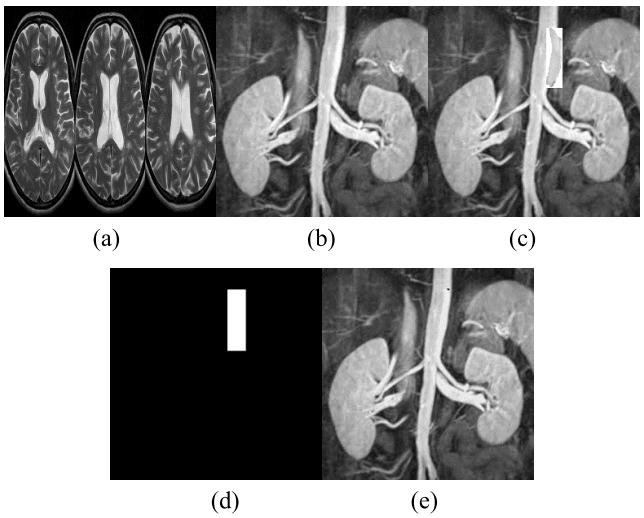


FIGURE 9. Result of VQ attack: (a) Lena (b) Girl (c) VQ attacked Image (d) localization of attack and (e) self-recovered host.

recovered host image (NCC_2) is also close to one, which indicates a reliable recovery of tampered host. Overall, the proposed scheme demonstrates a robust and satisfactory performance.

IV. CONCLUSION

This paper presents a SVD based fragile watermarking scheme using grouped block method to offer more security and provide a supplementary way to locate the attacked areas inside different medical images. Two authentication bits namely block authentication and self-recovery bits were used to survive the vector quantization attack. The usage of Arnold transform makes it possible to recover the tampered region from the neighboring blocks, which ultimately increases the NCC and PSNR of the recovered host. Our experimental results showed that the proposed scheme is highly reliable and is able to locate the attacked blocks efficiently. The proposed scheme effectively prevents copy and paste attack, content removal attack, text addition attack and VQ attack. Compared to the state-of-the art methods, the proposed scheme greatly improves both tamper localization accuracy and the PSNR of self-recovered image. Although our proposed method showed good performance in handling fragile tampered images, yet additional experiments are required to evaluate its efficiency with non-fragile tampered images. In our future work, we plan to resolve this issue. Furthermore, we will focus on detecting other tampering issues such as image resize, skew, and rotate operations.

REFERENCES

[1] M. Sajjad *et al.*, "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3519–3536, 2017.
[2] R. Hamza, K. Muhammad, Z. Lv, and F. Titouna, "Secure video summarization framework for personalized wireless capsule endoscopy," *Pervasive Mobile Comput.*, vol. 41, pp. 436–450, Oct. 2017. [Online]. Available: https://doi.org/10.1016/j.pmcj.2017.03.011
[3] R. Hamza, K. Muhammad, A. Nachiappan, and G. R. González, "Hash based encryption for keyframes of diagnostic hysteroscopy," *IEEE Access*, to be published. [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2762405
[4] Z. Jan *et al.*, "A review on automated diagnosis of malaria parasite in microscopic blood smears images," *Multimedia Tools Appl.*, pp. 1–26, 2017. [Online]. Available: https://doi.org/10.1007/s11042-017-4495-2
[5] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," *Future Generat. Comput. Syst.*, to be published. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.029
[6] T. Matsuo and K. Kurosawa, "On parallel hash functions based on block-ciphers," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E87-A, no. 1, pp. 67–74, 2004.
[7] N. Li, W. Du, and A. D. Boneh, "Oblivious signature-based envelope," *Distrib. Comput.*, vol. 17, no. 4, pp. 293–302, 2005.
[8] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. Int. Conf. Image Process.*, vol. 2. Oct. 1997, pp. 680–683.
[9] P. W. Wong and A. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1593–1601, Oct. 2001.
[10] S. Suthaharan, "Fragile image watermarking using a gradient image for improved localization and security," *Pattern Recognit. Lett.*, vol. 25, no. 16, pp. 1893–1903, 2004.
[11] C.-S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," *IEEE Trans. Multimedia*, vol. 5, no. 2, pp. 161–173, Jun. 2003.
[12] Y.-C. Hu, C.-C. Lo, C.-M. Wu, W.-L. Chen, and A. C.-H. Wen, "Probability-based tamper detection scheme for BTC-compressed images based on quantization levels modification," *Int. J. Secur. Appl.*, vol. 7, no. 3, pp. 11–32, 2013.
[13] S. Walton, "Information authentication for a slippery new age," *Dr. Dobb's J.*, vol. 20, no. 4, pp. 18–26, 1995.
[14] S.-H. Liu, H.-X. Yao, W. Gao, and A. Y.-L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel-pairs," *Appl. Math. Comput.*, vol. 185, no. 2, pp. 869–882, 2007.
[15] N. Memon, S. Shende, and A. P. W. Wong, "On the security of the Yeung-Mintzer authentication watermark," in *Proc. TS PICS Conf. Soc. Imag. Sci. Technol.*, 1999, pp. 301–306.

[16] M. Holliman and A. N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. Image Process.*, vol. 9, no. 3, pp. 432–441, Mar. 2000.
[17] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *AEU-Int. J. Electron. Commun.*, vol. 65, no. 10, pp. 840–847, 2011.
[18] X. Zhang and S. Wang, "Statistical fragile watermarking capable of locating individual tampered pixels," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 727–730, Oct. 2007.
[19] V. S. Dhole and N. N. Patil, "Self embedding fragile watermarking for image tampering detection and image recovery using self recovery blocks," in *Proc. Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Feb. 2015, pp. 752–757.
[20] B. Patra and J. C. Patra, "Crt-based fragile self-recovery watermarking scheme for image authentication and recovery," in *Proc. IEEE Int. Symp. Intell. Signal Process. Commun. Syst. (ISPACS)*, Nov. 2012, pp. 430–435.
[21] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Digit. Signal Process.*, vol. 21, no. 4, pp. 522–527, 2011.
[22] I. A. Ansari, A. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Eng. Appl. Artif. Intell.*, vol. 49, pp. 114–125, Mar. 2016.
[23] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.
[24] R. Sun, H. Sun, and A. T. Yao, "A SVD- and quantization based semi-fragile watermarking technique for image authentication," in *Proc. 6th Int. Conf. Signal Process.*, vol. 2. Aug. 2002, pp. 1592–1595.
[25] C. F. Van Loan, "Generalizing the singular value decomposition," *SIAM J. Numer. Anal.*, vol. 13, no. 1, pp. 76–83, 1976.
[26] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold transformation algorithm and anti-Arnold transformation algorithm," in *Proc. 1st IEEE Int. Conf. Inf. Sci. Eng.*, Dec. 2009, pp. 1164–1167.
[27] R. O. Preda, "Self-recovery of unauthentic images using a new digital watermarking approach in the wavelet domain," in *Proc. 10th Int. Conf. IEEE Commun. (COMM)*, May 2014, pp. 1–4.
[28] M. El'Arbi and C. Ben Amar, "Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain," *IET Image Process.*, vol. 8, no. 11, pp. 619–626, 2014.
[29] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.
[30] K. Muhammad, M. Sajjad, and S. W. Baik, "Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy," *J. Med. Syst.*, vol. 40, no. 5, p. 114, 2016.

ABDULAZIZ SHEHAB received the Ph.D. degree in computer and information sciences from Mansoura University, Egypt, in 2015. He is currently an Associate Professor with the Faculty of Computers and Information, Mansoura University, where he is also the Chair of the E-Learning Center. His research interests include data mining, data security, image processing, and robotics.

MOHAMED ELHOSENY received the B.S. degree in computer and information sciences from the Faculty of Computers and Information, Mansoura University, Egypt, and the Ph.D. degree in computer and information sciences from Mansoura University (in a scientific research channel with the Department of Computer Science and Engineering, University of North Texas, USA). He is currently an Assistant Professor with the Faculty of Computers and Information, Mansoura University, Egypt. He has authored/co-authored over 50 international journal articles, conference proceedings, book chapters, and one Springer brief book. His research interests include network security, cryptography, machine learning techniques, Internet of Things, and quantum computing. He has several publications in reputed and high impact journals published by the IEEE, Elsevier, Springer, and others. His Ph.D. thesis received the Best Ph.D. Thesis Prize (2016) at Mansoura University. He is a TPC Member or Reviewer for over 30 international conferences and workshops. He has been reviewing papers for over 20 international journals.

KHAN MUHAMMAD (S'16) received the bachelor's degree in computer science with research in information security from the Islamia College, Peshawar, Pakistan. He is currently pursuing M.S. degree leading to the Ph.D. degree in digitals contents from Sejong University, Seoul, South Korea. He has been a Research Associate with the Intelligent Media Laboratory, since 2015. His research interests include image and video processing, wireless networks, information security, image and video steganography, video summarization, diagnostic hysteroscopy, wireless capsule endoscopy, deep learning, computer vision, and CCTV video analysis. He has authored over 45 papers in peer-reviewed international journals and conferences, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Future Generation Computer Systems*, *Neurocomputing*, the IEEE ACCESS, the *Plos ONE*, the *Journal of Medical Systems*, *Biomedical Signal Processing and Control*, *Multimedia Tools and Applications*, *Pervasive and Mobile Computing*, *SpringerPlus*, the *KSII Transactions on Internet and Information Systems*, the *Journal of Korean Institute of Next Generation Computing*, MITA 2015, PlatCon 2016, FIT 2016, and ICNGC 2017.

ARUN KUMAR SANGAIAH received the Ph.D. degree in computer science and engineering from the Vellore Institute of Technology, Vellore, India. He is currently an Associate Professor with the School of Computer Science and Engineering, Vellore Institute of Technology. His area of interest includes software engineering, computational intelligence, wireless networks, bio-informatics, and embedded systems. He has authored over 100 publications in different journals and conference of national and international repute. His current research work includes global software development, wireless ad hoc and sensor networks, machine learning, cognitive networks and advances in mobile computing and communications. Also, he was registered a one Indian patent in the area of computational intelligence. He is responsible for the Editorial Board Member/Associate Editor of various international journals.

PO YANG (M'13) received the B.Sc. degree in computer science from Wuhan University, Wuhan, China, in 2004, the M.Sc. degree in computer science from the University of Bristol, Bristol, U.K., in 2006, and the Ph.D. degree in electronic engineering from the University of Staffordshire, Stoke-on-Trent, U.K., in 2010. He is currently a Senior Lecturer with the Department of Computing Science, Liverpool John Moores University, Liverpool, U.K. He holds a strong tracking of high-quality publications and research experiences. He has published over 40 papers. His current research interests include Internet of Things, RFID and indoor localization, pervasive health, image processing, GPU, and parallel computing.

HAOJUN HUANG received the B.S. degree from the School of Computer Science and Technology, Wuhan University of Technology, in 2005, and the Ph.D. degree from the School of Communication and Information Engineering, University of Electronic Science and Technology of China, in 2012. He held a post-doctoral position at the research institute of information technology, Tsinghua University from 2012 to 2015. He is currently a Professor of computing with the Department of Computer Science, College of Computer, China University of Geosciences, China. His current research interests include wireless communication, ad hoc networks, big data, and software-defined networking.

GUOLIN HOU received the B.S. degree from the School of Optical and Electronic Engineering, Ordnance Engineering College, in 2003, and the M.A. degree from the School of software engineering, PLA University of Science and Technology, in 2015. She is currently an Engineer with the Key Laboratory of Near-Surface Detection Technology. Her current research interests include wireless communication and software-defined networking.