A Robust Color Image Zero-Watermarking Based on SURF and DCT Features

Saqib Ali Nawaz[1,2], Jingbing Li[1,2(✉)], Uzair Aslam Bhatti[3], Hui Li[1,2], Baoru Han[6], Anum Mehmood[1,4], Raza M. Ahmed[1,2], Muhammad Usman Shoukat[1,5], and Jingjun Zhou[1,2]

[1] College of Information and Communication Engineering, Hainan University, Haikou 570228, China
saqibsial20@gmail.com, jingbingli2008@hotmail.com, {lihui,juingzhou}@hainanu.edu.cn, gooddranam@yahoo.com, wenbo1147@yahoo.com, usmanryk12@gmail.com

[2] State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou 570228, Hainan, China

[3] Key Laboratory of Virtual Geographic Environment, MOE, Nanjing Normal University, Nanjing 210023, China
uzairaslambhatti@hotmail.com

[4] Department of Biochemistry and Molecular Biology, Hainan University, Haikou 570228, China

[5] School of Automation and Information, Sichuan University of Science and Engineering, Yibin 644000, China

[6] College of Medical Informatics, Chongqing Medical University, Chongqing 400016, China
baoruhan@cqmu.edu.cn

Abstract. For most of the current watermarking algorithms, a multi-function color image that can simultaneously perform copyright protection and content authentication is proposed as Dual watermarking algorithm. First, the original image is converted from RGB space to YUV space, and the SURF (speeded up robust feature) of the luminance component is extracted. The marker points, constructs a description vector according to the main direction of the feature point and splits it into two sub-vectors, respectively calculating the cosine clip between them and a reference vector Angle, construct a robust zero watermark sequence by comparing the size relationship of the angles; then 2×2 the original image, and the singular value norm of the sub-image block. The XOR operation is performed to generate fragile watermark information and embed it into the least significant bit of the image space. By calculating the original robust zero water at the time of copyright attribution. The correlation coefficient between the printed sequence and the watermark sequence extracted from the image to be detected is used as the basis for identification, and the content authentication is passed. Experimental results show that the proposed algorithm has good performance.

Keywords: SURF features · Watermarking · DCT · Secure image processing

X. Sun et al. (Eds.): ICAIS 2020, CCIS 1253, pp. 650–660, 2020.
https://doi.org/10.1007/978-981-15-8086-4_61

1 Introduction

With the increasing popularity of high-speed broadband networks and the rapid development of digital information technology, various forms of digital multimedia resources are stored, copied and disseminated through the network, and the problems of copyright protection and content authentication become an urgent need to be solved. problem. Copyright protection requires that the watermarking algorithm has strong robustness and can resist certain signal processing operations [1]. Content authentication requires the watermarking algorithm to be sensitive to tampering operations, and it is easy to implement tampering and content authentication. However, most current watermarking algorithms often Only a single copyright protection or content authentication function can not meet the actual needs. The performance of a semi-fragile watermark is between a robust watermark and a fragile watermark, but it is difficult to have two good performances at the same time.

Therefore, the researcher has carried out related research on the simultaneous embedding of robust and fragile dual watermarks in a vector image. [2] proposed a multi-function watermarking algorithm based on vector quantization, embedding robust watermark and fragile watermark respectively. To the quantized average coefficient and the residual coefficient, the purpose of copyright protection and content authentication is achieved, but the watermarking algorithm has high computational complexity and low transparency (Fig. 1).

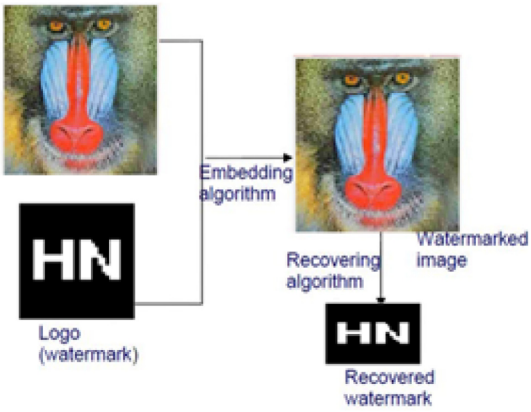

Fig. 1. Watermarking embedding and extraction step by step

The above multi-function image watermarking algorithm embeds both the robust watermark and the fragile watermark into the image carrier, which inevitably leads to a decrease in image quality, and the performance between the two watermarks also affects each other. In order to maintain image quality, the literature [3–6] proposed a zero watermarking technique. In view of this, a dual-function color image zero-watermarking algorithm is proposed. The stable feature of the image is extracted as a robust zero-watermark information by introducing a superior speed (SURF) (speeded up robust

feature) operator, and the least significant bit is changed in the airspace. The method embeds fragile watermark information to detect and locate malicious tampering. The advantages of the algorithm are as follows:

1) The image features extracted by the SURF operator are robust to noise, filtering, rotation, and luminance transformation;
2) Relative to the currently used SIFT (scale invariant feature transform) operator, SURF operator has greatly improved the efficiency of the algorithm;
3) Fragile watermark information replaces the least significant bit of the original image in the spatial domain, which can guarantee the visual quality of the image and is very sensitive to malicious tampering and can be accurately positioned, with good real-time.

2 Background

2.1 SURF Feature Information Extraction

As an image local feature description operator based on scale space, SURF is an improvement of SIFT operator. The SURF algorithm uses the Hessian matrix for extreme point detection, and its Hessian matrix on the scale can be expressed as:

$$H = \begin{bmatrix} L_{XX}(X,\sigma)\ L_{XY}(X,\sigma) \\ L_{YX}(X,\sigma)\ L_{YY}(X,\sigma) \end{bmatrix} \tag{1}$$

Where $L_{xx}(X,\sigma)$ is the result of Gaussian second-order differential and image, $I(\mathrm{x}, y)$ convolution at point x, £., $L_{xy}(X,\sigma)$ and $L_{YX}(X,\sigma)$ have similar meanings. The SURF algorithm uses box filtering instead of Gauss filtering in feature extraction. The filtering operation of the image can be completed by simple addition and subtraction. Compared with the sI algorithm, the operation speed is greatly improved and the algorithm is improved. The efficiency of the algorithm is [7, 8].

Compared with the SIFT marking algorithm, the biggest advantage of the SURF algorithm is the improvement of the operation speed. The comparison results of the SURF algorithm, the SIFT algorithm, and the SIFT improved algorithm proposed in [9] in the feature matching time. The experimental results show that the SURF algorithm extracts a relatively small number of feature points, but still can clearly obtain the image transformation relationship. At the same time, the SURF algorithm runs only about l/3 of the SIFT algorithm, which has better real-time performance.

2.2 Robust Zero Watermarking Algorithm Based on SURF Feature

Image SURF feature information for rotation, scale scaling, mapping Operations such as transformation and grayscale change have strong robustness. Therefore, robust zero-watermark information is constructed by extracting the important feature information of SURF of color images [10]. The basic design idea of the algorithm is to spatially transform the original color carrier image, extract the SURF feature information of the luminance component, and select the feature points and feature vectors that satisfy the

scale condition. A reference vector is constructed by using a key, and the cosine angle between the reference vector and the eigenvector is calculated, and the relationship between the cosine angles is compared and a watermark sequence is generated according to a certain rule. Finally, the Amold scrambles the watermark sequence to generate the final copyright identification information [11]. When the watermark is detected, the SURF feature information of the image to be detected and the corresponding copyright identification information are extracted, and the bit correctness rate is detected with the original copyright information [12–15]. If the bit correctness is greater than a given threshold, then the watermark information is present, and vice versa. Figure 2 shows the proposed strategy of implementation of SURF features for watermarking.

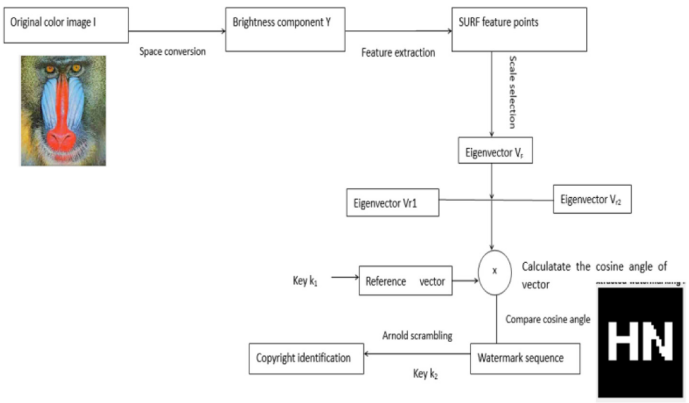

Fig. 2. The flowchart of robust zero-watermark

2.3 Construction of Robust Zero Watermark Information

The robust zero watermark information construction process based on the image SURF feature is shown in Fig. 2, and the flow is described as follows:

1) Convert the original color image from RGB space to YUV space, and convert the formula to:

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B \\ U &= -0.147R - 0.289G + 0.436B \\ V &= 0.615R - 0.515G - 0.100B \end{aligned} \tag{2}$$

Where 1 represents a luminance component, U, V and y represent chrominance components. According to the masking property of the human visual model, the feature value of the luminance component is extracted as the robust zero watermark information [16].

2) Extract the SURF feature points of the luminance component, and set the feature point set to S, i.e.

$$S = \{S_P | S_P = (\mathrm{x}_i, y_j), l_p, \theta_p, p \in (0, m)\} \tag{3}$$

Where, (x_i, y_j) is the position of the feature point in the image, l_p For the scale of the feature point, θ_p For the main direction of the feature point, m is the number of original image feature points.

The literature [13] shows that the larger the scale space of the feature points, the higher the matching probability. Assume $\mathrm{l}_{\max}$ Is the maximum value of the feature point scale in the feature point set, i.e.

$$\mathrm{l}_{\max} = \max(l_p, p \in (0, m)) \tag{4}$$

Let the scale selection factor be a($0 < \mathrm{a} < 1$), then the set of feature points that satisfy the condition can be expressed as

$$\mathrm{s}' = \{s_p | s_p = (x_i, y_j), l_p', \theta_p, p \in (0, m')\} \tag{5}$$

Where m' is the number of feature points that satisfy the scale condition,

$$\mathrm{l}_\mathrm{p}' \in \{l_p | \partial l_{\max} \leq l_p \leq l_{\max}, p \in (0, m)$$

3) Selecting a set of feature points that satisfy the scale condition, and constructing a 64-dimensional description vector V_r according to the main direction of each feature point, which can be expressed as

$$V_\mathrm{r} = \{V_p | V_p = (\xi_{p0}, \xi_{p1}, \ldots.., \xi_{p63}), P \in (0, m')\} \tag{6}$$

4) Use the private key K_1 Create a 32-dimensional reference vector V_D, calculate V_D and V_{r1}, V_{r2} respectively, % vector cosine angle φ_{r1}, φ_{r2} the calculation formula is

$$\cos\varphi = \frac{a.b}{|a||b|} \tag{7}$$

5) Generate a binary watermark sequence according to the vector cosine angle relationship, and the generation rule is

$$w_i = \begin{cases} 1 \ \varphi_{r1} \geq \varphi_{r2} \\ 0 \ \varphi_{r1} < \varphi_{r2} \end{cases} \tag{8}$$

Where, $\mathrm{i} = 1, 2, \ldots., m'$.

2.4 Robust Zero Watermark Information Extraction and Detection

As with the watermark information construction process, the image to be detected is spatially transformed, the SURF feature points of the luminance component are extracted,

and the corresponding feature vectors are constructed. Use the key K_1 And K_2 get the extracted copyright identification information $\widehat{U}$.

The performance of the robust zero-watermarking algorithm is evaluated by the bit correctness rate (BCR). The BCR value is,

$$R_{BC}(U, \hat{U}) = 1 - (\sum_{i=1}^{m'} U \oplus \hat{U}_i)/m' \tag{9}$$

Where, $\oplus$ represents an exclusive OR operation, and if the sequences U and $\hat{U}$ are the same, then BCR value is equal to 1, otherwise it tends to 0. In the process of detecting the watermark information, the setting of the T detection threshold r may cause a false alarm, that is, the image that is not embedded in the watermark is judged to have a watermark. The random binary sequence and the constructed zero watermark sequence have a probability of matching each bit of 0.5, so the false alarm probability can be expressed as [15].

$$P = \sum_{z=T}^{\text{m'}} (0.5^2 \times C_{m'}^2) \tag{10}$$

In the formula, T is the detection threshold, z is the number of matched bits, $C_{\text{m}'}^2$ is the combination of m' and z.

2.5 Security Analysis of Robust Zero Watermarking Algorithm

A 32-dimensional reference vector V_D is created using the key K_2. If the attacker cannot obtain the correct key K_2, the targeted watermark attack cannot be performed. The number of times that Amold scrambles. If you can't get fear, the attacker can't generate the correct copyright logo. Therefore, the robust zero watermark algorithm is fully public, and its security depends on the key K_2 And ink.

3 Watermarking Implementation

3.1 Vulnerable Watermark Embedding

1) 2×2 partitioning of the original carrier image, defined as

$$B_{\text{q}} = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, x_i$$

where is the pixel value. The most pixel value for each block low significant bit (LSB) is set to zero to get

$$B_q^{'} = \begin{bmatrix} x_1^{'} & x_2^{'} \\ x_3^{'} & x_4^{'} \end{bmatrix}$$

2) According to the singular value perturbation theorem, the sub-image block singular value norm is XORed to generate fragile watermark information [16]. First, the norm of the two singular values of the sub-image block is calculated and rounded.

$$N_{\mathrm{m}} = f\left(\sqrt{\sum_{i=1}^{2}\sigma_i^2}\right) \tag{11}$$

In the formula f is a rounding function.

2) For N_{m} the 8-bit plane is XOR to generate fragile watermark information, and the fragile watermark information is closely related to each block pixel, which is beneficial to enhance the sensitivity of the fragile watermark to malicious tampering. The rule is [16]:

$$w_f = \begin{bmatrix} w_{f_1} & w_{f_2} \\ w_{f_3} & w_{f_4} \end{bmatrix} \tag{12}$$

Where b_i is N_{m} the i bit, w_f is the resulting fragile watermark information, training Is the w_{f_i} pixel value of the fragile watermark.

3) Embedding the fragile watermark information into the least significant bits of the corresponding block pixel, and reconstructing each sub-image block to obtain an image embedded in the fragile watermark.

3.2 Fragile Watermark Extraction

First, the water-printed image is 2 × 2 divided, and then the least significant digit value of each pixel value in the sub-image block is extracted, and the definition is defined, $l = \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix}$. l_i The lowest value of each pixel in the 2 × 2 sub-image block effectiveness. Similar to the fragile watermark embedding step, the sub-image block is subjected to SVD (singular values decomposition) transformation, norm rounding, pixel value exclusive OR, etc. to extract the fragile watermark w_f. w_f will l compared with z, if the images are completely identical, the image has not been tampered with; if there are inconsistent values, the image is tampered with and the location of the tampering is marked [16].

4 Experimental Results

4.1 Experiment Setup and Validation

In this paper, the NC (normalized correlation coefficient) value is used to compare the similitude between the original watermark image and the extracted watermark image to evaluate the strength of the algorithm. The NC value is calculated as shown in Eq. (14).

The higher the NC value, the better the watermark similarity and the stronger the strength of the algorithm. The second part of the experiment verifies the effect of the algorithm tampering by adding different tampering attacks to different vector images. Two different images were used for the validation of our proposed algorithm as shown in Fig. 3 respectively:

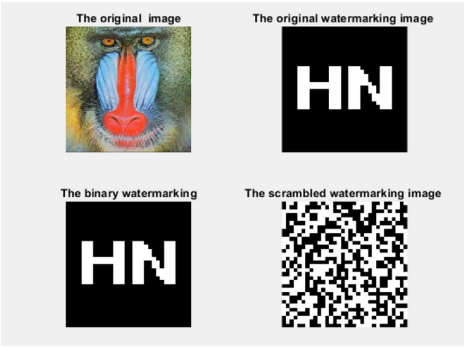

Fig. 3. Baboon Colored image

Compared with other multi-function watermarking algorithms, this paper extracts the SURF feature of the image to construct robust zero-watermark information, instead of embedding the watermark into the carrier image, thus "embedding" the robust watermark information. At the same time, the fragile watermark information is embedded in the least significant bit of the image space, which has a slight impact on the human visual effect. Therefore, the watermarking algorithm has good transparency. The objective evaluation index of transparency uses a peak signal-to-noise ratio (PSNR) value, and the higher the value, the better the transparency. If $I(i,j)$ represents the original image, and $I'(i,j)$ represents an image embedded in the watermark, the PSNR is:

$$PSNR = 10lg\frac{MN\max I^2(x,y)}{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-I'(i,j)]^2} \tag{13}$$

The normalized correlation coefficient NC [17, 18] is:

$$NC = \frac{\sum_i \sum_j W_{(i,j)} W'_{(i,j)}}{\sum_i \sum_j W^2_{(i,j)}} \tag{14}$$

4.2 Robustness Analysis of Watermarking Algorithm

In order to verify the robustness of the algorithm, the conventional and geometric attack tests are performed on the image after embedding the watermark, and the watermark information is extracted from the image after the attack (Table 1). Detection rate the

robustness is measured by the ratio of the number of feature regions in which the watermark is successfully detected to the number of feature regions in the original image and the maximum NC value of the watermark.

Table 1. PSNR and NC value of different types of Geometric Attack on Colored Image (Baboon)

Geometric attacks	Attack strength	PSNR(dB)	NC
Rotation (clockwise)	5° 10° 30°	15.70 13.67 10.58	0.95 0.91 0.91
Rotation (Anticlockwise)	5° 10° 20°	15.60 13.54 11.41	1 1 0.91
Scaling	x 0.6 x 0.8	- -	0.72 0.73
Translation (Left)	10% 15% 25%	11.00 9.70 9.12	0.92 0.86 0.88
Translation (down)	8% 15% 25%	13.30 11.45 9.78	1 1 1
Clipping (Y direction)	10% 30%	– –	1 1
Clipping (X direction)	10% 30%	– -	1 1

From Table 1, it is clear that proposed algorithm is more robust against geometric attacks. In coloured image of Bamboo Clipping X and Y direction, Translation attack and Rotation attack have the NC value more than 90% and nearly 100%, thus results of our proposed DCT and SURF are satisfactory and robust in watermarking an image. Figure 4 shows the implementation results of our proposed algorithm on different attacks and recovering of the watermark algorithm after extraction process.

Therefore, the algorithm presented in this paper is outstanding in all kinds of attack situations, especially so in solving the problem that existing algorithms cannot balance resistance to geometric attacks and robustness. It has strong resistance to geometric attacks and shows a good level of robustness.

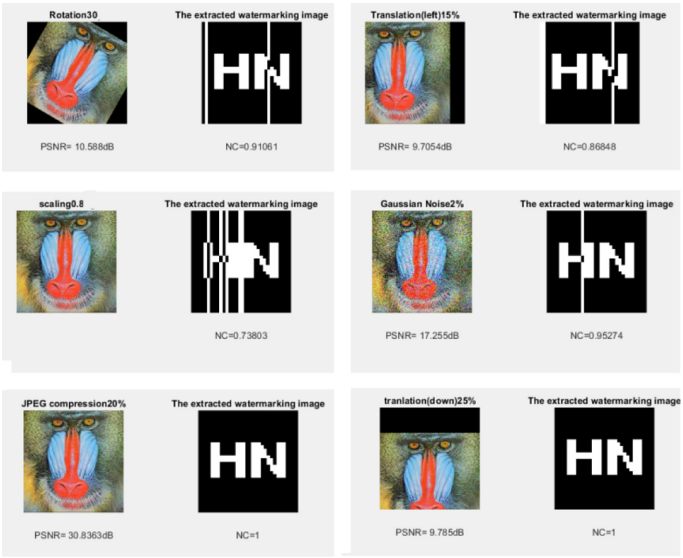

Fig. 4. Different attacks on Baboon Coloured scale image

5 Conclusion

Aiming at the limitations of most image watermarking algorithms at present, a multi-function colour image watermarking algorithm which can realize copyright protection and content authentication is proposed. Utilize image SURF features for common signal operation remains stable. The robust zero watermark sequence is constructed to implement the copyright protection function, and the mutual interference between the watermarks is avoided. The content authentication is realized by embedding the fragile watermark on the least significant bit of the image space. The experimental results show that the watermarking algorithm has better transparency, improved computational efficiency and robustness to common image operations. At the same time, the area where the image can be maliciously tampered with domain is accurately detected and located.

Acknowledgements. This work is supported by Hainan Provincial Natural Science Foundation of China [No. 2019RC018], and by the Natural Science Foundation of Hainan[617048, 2018CXTD333], and by the Science and Technology Research Project of Chongqing Education Commission [KJQN201800442] and by the Special Scientific Research Project of Philosophy and Social Sciences of Chongqing Medical University [201703].

References

1. Wu, X., Li, J., Tu, R., Cheng, J., Bhatti, U.A., Ma, J.: Contourlet-DCT based multiple robust watermarkings for medical images. Multimedia Tools Appl. **78**(7), 8463–8480 (2018). https://doi.org/10.1007/s11042-018-6877-5

2. Jayashree, N., Bhuvaneswaran, R.S.: A robust image watermarking scheme using Z-transform, discrete wavelet transform and bidiagonal singular value decomposition. Comput. Mater. Continua **58**(1), 263–285 (2019)
3. Jiansheng, M., Sukang, L., Xiaomei, T.: A digital watermarking algorithm based on DCT and DWT. In: Proceedings of The 2009 International Symposium on Web Information Systems and Applications (WISA 2009). Academy Publisher (2009)
4. Feng, J.-B., et al.: Reversible watermarking: current status and key issues. IJ Netw. Secur. **2**(3), 161–170 (2006)
5. Bianchi, T., Piva, A.: Secure watermarking for multimedia content protection: A review of its benefits and open issues. IEEE Signal Process. Mag. **30**(2), 87–96 (2013)
6. Xiang, L., Li, Y., Hao, W., Yang, P., Shen, X.: Reversible natural language watermarking using synonym substitution and arithmetic coding. Comput. Mater. Continua **55**(3), 541–559 (2018)
7. Bhatti, U.A., Huang, M., Di, W., Zhang, Y., Mehmood, A., Han, H.: Recommendation system using feature extraction and pattern recognition in clinical care systems. Enterp. Inf. Syst. **13**(3), 329–351 (2019)
8. Wang, Y., Ni, R., Zhao, Y., Xian, M.: Watermark embedding for direct binary searched halftone images by adopting visual cryptography. Comput. Mater. Continua **55**(2), 255–265 (2018)
9. Liu, Y., Li, J., Liu, J., Bhatti, U.A., Chen, Y., Hu, S.: Watermarking algorithm for encrypted medical image based on DCT-DFRFT. In: Chen, Y.-W., Zimmermann, A., Howlett, R.J., Jain, L.C. (eds.) Innovation in Medicine and Healthcare Systems, and Multimedia. SIST, vol. 145, pp. 105–114. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-8566-7_10
10. Luo, H., et al.: A robust image watermarking based on image restoration using SIFT. Radioengineering **20**(2), 525–532 (2011)
11. Liu, J., Li, J., Zhang, K., Bhatti, U.A., Ai, Y.: Zero-watermarking algorithm for medical images based on dual-tree complex wavelet transform and discrete cosine transform. J. Med. Imaging Health Inform. **9**(1), 188–194 (2019)
12. Dai, Q., Li, J., Bhatti, U.A., Chen, Y.-W., Liu, J.: SWT-DCT-based robust watermarking for medical image. In: Chen, Y.-W., Zimmermann, A., Howlett, R.J., Jain, L.C. (eds.) Innovation in Medicine and Healthcare Systems, and Multimedia. SIST, vol. 145, pp. 93–103. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-8566-7_9
13. Dai, Q., Li, J., Bhatti, U.A., Cheng, J., Bai, X.: An automatic identification algorithm for encrypted anti-counterfeiting tag based on DWT-DCT and Chen's chaos. In: Sun, X., Pan, Z., Bertino, E. (eds.) ICAIS 2019. LNCS, vol. 11634, pp. 596–608. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-24271-8_53
14. Wu, X., Li, J., Bhatti, U.A., Chen, Y.-W.: Logistic map and contourlet-based robust zero watermark for medical images. In: Chen, Y.-W., Zimmermann, A., Howlett, R.J., Jain, L.C. (eds.) Innovation in Medicine and Healthcare Systems, and Multimedia. SIST, vol. 145, pp. 115–123. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-8566-7_11
15. Liu, J., Li, J., Chen, Y., Zou, X., Cheng, J., Liu, Y., Bhatti, U.A.: A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain. CMC-Comput. Mater. Continua **61**(1), 363–378 (2019)
16. Nawaz, S.A., Li, J., Liu, J., Bhatti, U.A., Zhou, J., Ahmad, R.M.: A feature-based hybrid medical image watermarking algorithm based on SURF-DCT. In: Liu, Y., Wang, L., Zhao, L., Yu, Z. (eds.) ICNC-FSKD 2019. AISC, vol. 1075, pp. 1080–1090. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-32591-6_118
17. Nawaz, S.A., Li, J., Bhatti, U.A., Mehmood, A., Shoukat, M.U., Bhatti, M.A.: Advance hybrid medical watermarking algorithm using speeded up robust features and discrete cosine transform. Plos one **15**(6), e0232902 (2020)
18. Bhatti, U.A., Yu, Z., Li, J., Nawaz, S.A., Mehmood, A., Zhang, K., Yuan, L.: Hybrid watermarking algorithm using clifford algebra with arnold scrambling and chaotic encryption. IEEE Access **8**, 76386–76398 (2020)