SURF based security of remote sensing images by encrypted watermark

Uzair Aslam Bhatti[1,2], **Zhaoyuan Yu**[1,2] , **Linwang Yuan**[1,2], **Saqib Ali Nawaz**[3], **Ahmad Hasnain**[1]

[1]School of Geography, Nanjing Normal University,Nanjing, 210023, China

[2]Key Laboratory of Virtual Geographic Environment, Ministry of Education, Nanjing Normal University, No. 1 Wenyuan Road, Nanjing, China

[3]College of Information and Communication Engineering, Hainan University, Haikou, China 570228

Corresponding Author : Linwang Yuan

Abstract: Aiming at the security protection of remote sensing images, a robust watermarking algorithm based on SURF (Speeded Up Robust Features) feature on selective regions is proposed. The algorithm first extracts the SURF feature points of the carrier, and then performs a 5/3 integer wavelet transform on the carrier image to filter out the low-frequency coefficients of the ROI and the intermediate frequency coefficients of the non-interest area (ROB); With sampling pyramid decomposition, the near subband after watermark decomposition is embedded in the low-frequency subband of the region of interest, and the residual subband is embedded in the intermediate frequency coefficient of the non-interesting region. Experimental data show that the algorithm can resist conventional geometric attacks. The similarity of the watermark is high, and the NC value is kept above 0.89, which has good reversibility and robustness.

Keywords: SURF feature detection; reversible watermark, remote sensing image

1. Introduction

Remote sensing imagery is an important carrier of geospatial information, and its military and economic value is increasingly prominent, and it plays an important role in many fields such as surveying and mapping, navigation, reconnaissance, and monitoring[1]. However, the digital storage method and open network environment not only realize the rapid transmission and efficient sharing of remote sensing images, but also bring new challenges to the security protection of image data. In recent years, data leakage, illegal tampering, and ownership violations against remote sensing images have been repeatedly prohibited. Digital watermarking technology is a cutting-edge technology developed in the field of information security and an important means of remote sensing image security protection.

Although the research of remote sensing image digital watermarking technology started relatively late, it has also achieved vigorous development due to its great practical significance. Bhatti et al. [2] studied the evaluation criteria of digital watermarking for high resolution color images, and pointed out that watermarking technology for ordinary images is not completely suitable for medical images images and can be used by separating the color images in RGB color space. Delaigle et al. [3] uses human visual characteristics and visual models to select important wavelet coefficients to embed the watermark, but the original image is required to participate in the detection, which is a non-blind algorithm and is not practical.

Saqib et al. [4] embeds the encrypted binary image watermark into the block-scrambling remote sensing image, which has good robustness to conventional attacks, but cannot resist geometric attacks. Pereira et al. [5] uses the template matching method to resist geometric attacks, but the key matrix is required to participate in the detection, which is a semi-blind algorithm. The literature [6] embeds the watermark into the normalized remote sensing image in the Controllet domain, but because it is embedded as a whole, the algorithm is not robust to the cutting of the image size. In general, the current research on remote sensing image watermarking algorithms mostly uses the first-generation watermarking method [2-7], and rarely involves the second-generation watermarking technology, that is, algorithms based on image features. However, in specific applications, remote sensing images embedded with watermarks inevitably need to be rotated, zoomed, cropped to change the original size, and tile stitching, etc., and the angle of rotation, zoom multiples, etc. during watermark detection The position relative to the original image after cutting and splicing is unknown. These geometric attacks destroy the synchronization of the watermark, resulting in detection failure. Algorithms based on image features provide a brand-new idea for solving this problem, and the research on algorithms for ordinary images has been relatively in-depth [8-13], which can provide methodological references for the research of remote sensing image watermarking.

Based on the existing algorithms, this paper designs a robust blind watermarking algorithm for remote sensing images based on SURF feature points and the excellent characteristics of region based feature selection using region of interest (ROI), which is strong against conventional attacks and geometric attacks. The main contributions of this study are:

1) Secure watermarking algorithm for security of remote sensing images.
2) Implementation of SURF using feature based region selection for watermarking.

2.Related theories

2.1 SURF feature detection

SURF (speeded up robust features) is a fast-robust local feature detection algorithm proposed Based on SIFT operator. In general, the standard SURF operator is several times faster than the SIFT operator and has better robustness under multiple images [14]. This paper uses ROI selection based on SURF features. The basic idea is as follows: first, calculate the integral image and traverse the image once to get the sum of all pixels. Then construct the Hessian matrix [15] and perform Gaussian filtering on the image. After filtering, the Hessian matrix expression is**:**

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

If the Hessian matrix discriminator has an extreme value, the current point will be brighter or darker than the surrounding points, and the candidate object may be divided by the extreme value. To increase the speed, SURF uses a box filter to approximate a Gaussian filter. If the endpoint is a physical endpoint, it is very important to calculate the Hessian discriminant for each pixel. If it is a positive number, the pixel is a local extreme point, otherwise, it is not. The extreme point is obtained is used as a candidate feature point. Then, the non-maximum suppression of the 3 * 3 * 3 cube neighborhood adjacent to this point [16], that is, the candidate extremum point is related to 8 extremum points of the same scale neighborhood and 18 extremum points of the adjacent scale. In comparison, the higher the significance of the pixel and the greater the contribution to the ROI selection. The feature point contribution is defined as

$$w_p = \left|\frac{v_p - \mu_{N(P)}}{\mu_{N(P)}}\right| \tag{2}$$

Where v_p represents the d (H) value of the feature point p, and $\mu_{N(P)}$ is the average of the d (H) values of 26 points around the point p. The matrix composed of the contribution of feature points is the contribution matrix. Using the idea of dynamic programming to determine the largest sub-matrix, the matrix is the part with the largest contribution of feature points, that is, ROI.

SURF feature point correction: let $(\mathrm{X_i}, \mathrm{Y_i})$ and $(\mathrm{X_j}, \mathrm{Y_j})$ be any two feature points in the original image feature points, $(\mathrm{X'_i}, \mathrm{Y'_i})$ and $(\mathrm{X'_j}, \mathrm{Y'_j})$ are Feature points of image matching after suffering a geometric attack.

Rotation correction: If the number of matching feature points is N, then the angle between the vectors of the matching feature points of the two images is the angle of rotation. From the vector angle formula (3), the maximum rotation angle is removed. The obtained angle is averaged to obtain the rotation angle β.

$$\beta_i = \frac{(x_i - x_j)(x'_i - x'_j) + (y_i - y_j)(y'_i - y'_j)}{\sqrt{(x_i - x_j)^2 + (x'_i - x'_j)^2}\sqrt{(y_i - y_j)^2 + (y'_i - y'_j)^2}} \tag{3}$$

$$\beta = \frac{1}{n}\sum_{i=1}^{n} \beta_i \qquad i \le N - 1, n \le N - 1 \tag{4}$$

Scaling correction: According to the matching feature points of the two images, the scaling ratio of the image length and width can be estimated, and the points with larger errors can be removed, and the scaling ratio of length and width can be obtained by averaging.

$$\alpha_x = \frac{|x_i - x_j|}{|x'_i - x'_j|}\ , \quad \alpha_y = \frac{|y_i - y_j|}{|y'_i - y'_j|} \tag{5}$$

Translation correction: Calculate the difference between the abscissa and ordinate of each pair of matching feature points of the two images, remove the larger error value, and calculate the average value to get the translation distance.

$$\begin{cases} \Delta x = |x_i - x'_i| \\ \Delta y = |y_i - y'_i| \end{cases} \tag{6}$$

2.2 Sampling pyramid decomposition

The digital watermark is sampled, and the residual sub-band is calculated to generate a sampling golden tower composed of a series of residual sub-bands and an approximate sub-band. The image of this golden tower structure has scalable characteristics. Set the original image G_0 as the bottom layer of the sampling pyramid (layer 0), down-sampling G_0 to obtain the first layer G_1 of the sampling golden tower, and then fill the G_1 with the interpolation method to form the same as the original image The size of the image G_0^*. Then the difference between G_0 and G_0^* is used to construct the residual image L_0. After decomposing the sampled golden tower in one layer, an approximate image G_1 and a residual image L_0 are generated. If the sampling gold tower decomposition needs to be continued, a similar operation is performed on the approximate sub-band image G_1 to generate an approximate image G_2 and a residual image L_1.

$$G_0^*(i,j) = 4\sum_{m=-2}^{2}\sum_{n=-2}^{2} w(m,n)G_0\left(\frac{i+m}{2},\frac{j+n}{2}\right) \tag{7}$$

Among them:

The image is composed of 5/3 3-level IWT to decompose the extract of wavelet coefficients of ROI and ROB.

(3) Arnold scrambling of watermark and three-level sampling pyramid decomposition to obtain 4 subband data: G_3, L_2, L_1 and L_0, where G_3 is approximate subband, L_2, L_1 and L_0 are the third level, second Level, and the first level residual subband.

(4) The approximate G_3 sub-band watermark is decomposed into a sampling pyramid, and then ROI is embedded in the LL_3 sub-band using the reversible watermark histogram algorithm.

(5) The residual subbands L_2, L_1 and L_0 of the watermark are embedded into LH_3, LH_2 and LH_1 of ROB through singular value decomposition. Embedding method: After each h-h block is divided into h × h blocks, SVD decomposition is performed, $\mathrm{A} = \mathrm{USV}^{\mathrm{T}}$, and Q = round (S (1,1) / Q) is calculated. S (1,1) represents the first singular value after singular value decomposition of each block, q is the embedding strength, and round is rounding.

Embed the watermark according to equation (10).

$$G_0^*\left(\frac{i+m}{2},\frac{j+n}{2}\right) = \begin{cases} G_0\left(\frac{i+m}{2},\frac{j+n}{2}\right) & \frac{i+m}{2},\frac{j+n}{2} \text{ is an integer} \\ 0 & else \end{cases} \tag{8}$$

When reconstructing the image sampling pyramid, from the top to the bottom of the sampling golden tower, the following formula is used to restore layer by layer, and then the original image is obtained.

When reconstructing the image sampling pyramid from the top to the bottom of the tower, use the following formula to copy the sampled gold layer by layer, and then save the original image.

$$\begin{cases} G_1 = L_1 + G_{l+1}^* & 0 \le l \le N \\ G_N = L_N & l = N \end{cases} \tag{9}$$

3. Watermark embedding and extraction

3.1 Watermark embedding

The specific steps of watermark embedding are shown in Figure 1. Extract the SURF feature points of the carrier image, as described in Section 1.1, select the image ROI according to the part with a large contribution of feature points;

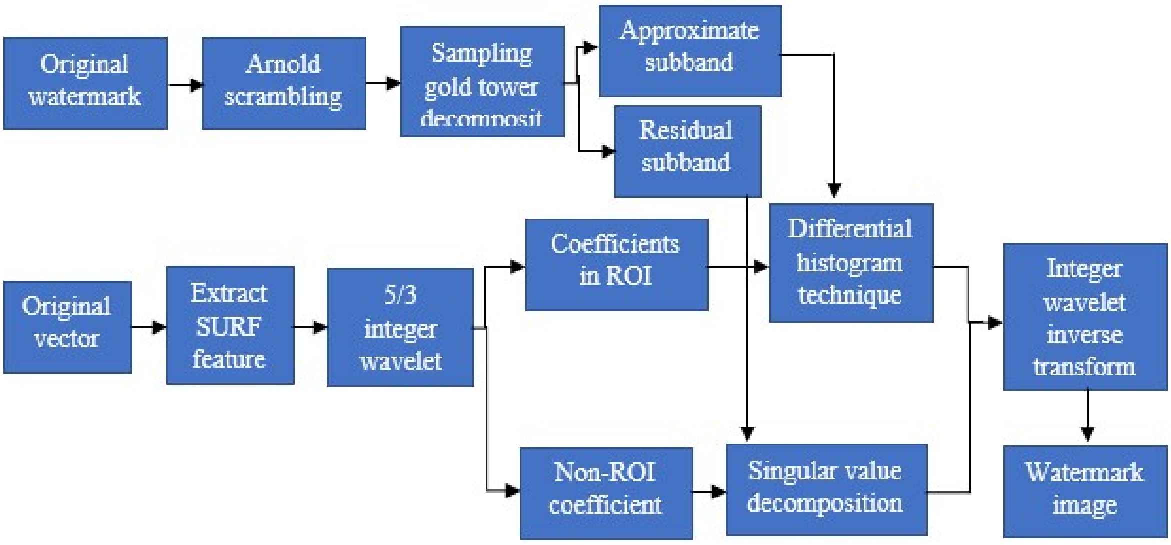


Fig.1 Watermark embedding algorithm block diagram

$$S'(1.1) = \begin{cases} (Q - 0.5) \times q & if \;\; T_i = 1 \\ (Q + 0.5) \times q & if \;\; T_i = 0 \end{cases} \tag{10}$$

After the singular value is modified, an inverse SVD transformation is performed.

3.2 Watermark extraction

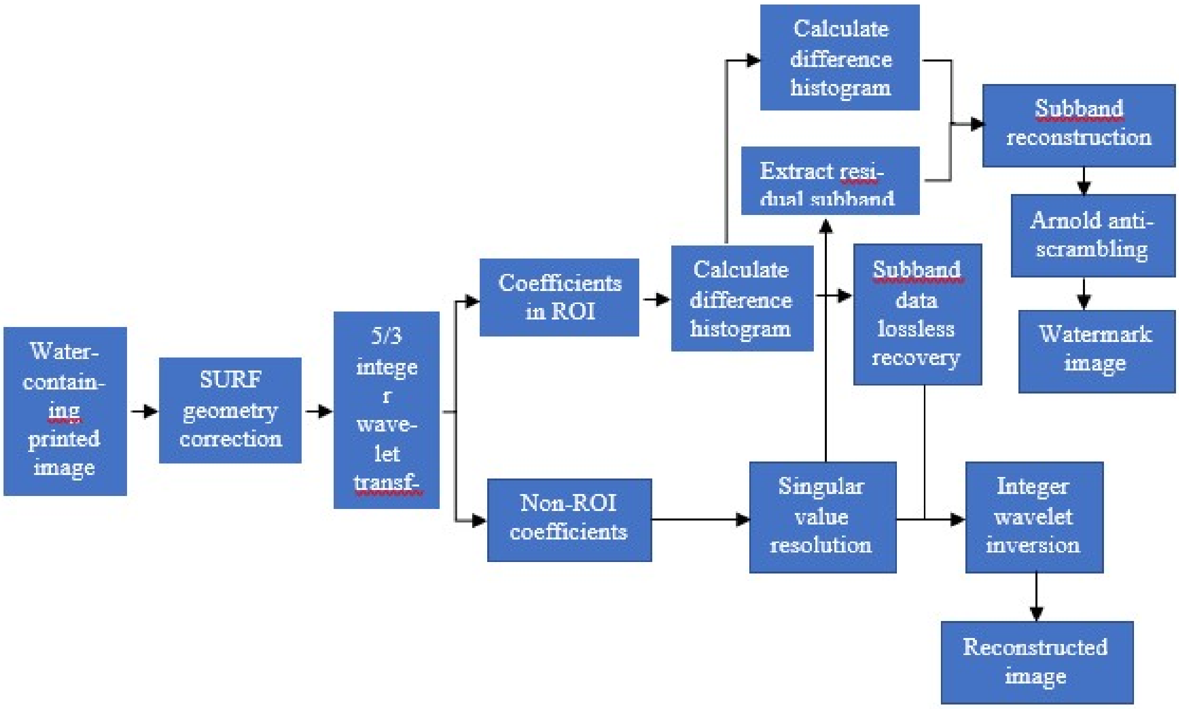
The specific steps of watermark extraction are shown in Figure 2.

(1) Use the SURF feature point S' and the original carrier SURF feature point S after the geometric attack on the watermark carrier to correct the geometric attack on the watermark carrier.

(2) The corrected image undergoes a three-level integer wavelet transform to extract the coefficients in ROI and ROB respectively.

(3) Extract the approximate subband information of the watermark in the LL_3 subband of the region of interest using the differential histogram reversible watermarking algorithm and restore the wavelet subband data of the ROI.

(4) Using the singular value decomposition algorithm to extract the watermark residual subband information L_2, L_1, L_0 of LH_3, LH_2, LH_1 in ROB. The extraction method is similar to the embedding method, and SVD.



Water-containing printed image
SURF geometry correction
5/3 integer wave-let transf-
Coefficients in ROI
Non-ROI coefficients
Calculate difference histogram
Calculate difference histogram
Extract resi-dual subband
Subband data lossless recovery
Singular value resolution
Integer wavelet inversion
Reconstructed image
Subband reconstruction
Arnold anti-scrambling
Watermark image

Fig.2 Watermark extraction algorithm block diagram

decomposition is performed on each h × h block, $A' = US'V^T$ and calculate $d = \text{floor}\ (S'(1,1)/q)$, where floor is rounded down and $S'(1,1)$ is the first singular value of each sub-block. Calculate the value of mod(d,2), and use parity discriminant (11), to extract the subband information of each resolution watermark.

$$W = \begin{cases} 1 & if\ \mathrm{mod}(d,2) = 1 \\ 0 & if\ \mathrm{mod}(d,2) = 0 \end{cases} \tag{11}$$

(5) Perform sampling pyramid reconstruction on the watermark subband information extracted in step (3) and step (4). Then, the inverse Arnold transformation is performed on the reconstructed image to obtain the extracted watermark.

4. Results analysis and discussion

The experimental environment is MATLAB2018, which performs invisibility test, multi-resolution extraction test and robustness test respectively. The experimental carrier is 512 × 512 remote sensing image, and the watermark is 32 × 32 binary image. Fig. 5 shows that remote sensing image and the method of watermark embedding.

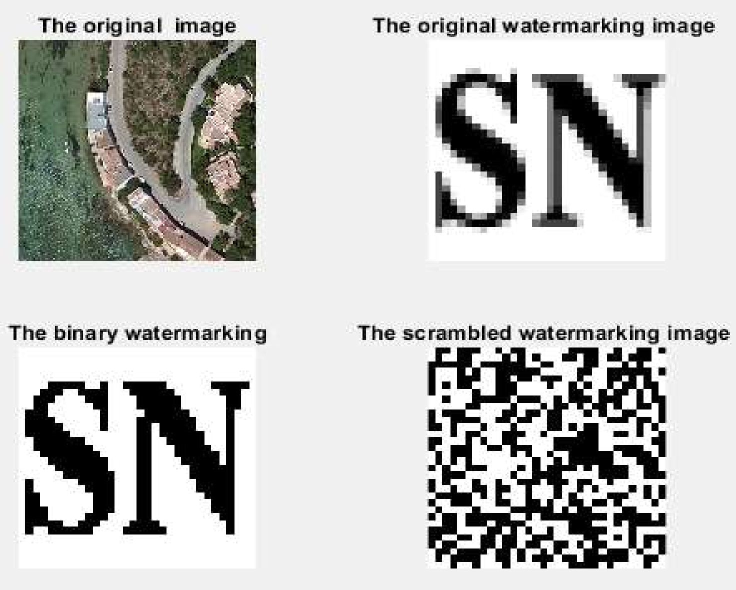

The original image
The original watermarking image
The binary watermarking
The scrambled watermarking image

Figure 3. Original remote sensing image and watermark

4.1 Conventional Attacks

The carrier images of the experiment are remote sensing image. The embedding intensity of the watermark in ROB and remote sensing image is obtained after embedding the watermark, as shown in Figure 3, and the peak signal-to-noise ratio (PSNR) is shown in Table 1. The Gaussian noise 4% and JPEG 20% shows that NC is 0.93 and 1 after extraction, and the robustness is very good.

Table 1. The NC PSNR under Conventional Attacks .

	Gaussian noise			JPEG Compression		
Conventional attack	2%	4%	6%	10%	20%	50%
PSNR (db)	17.32	14.65	13.18	25.57	28.66	32.54
NC	0.92	0.93	0.93	0.91	1	1

4.2 Geometric attack

According to the algorithm proposed in this paper, the image under attack is corrected and then the watermark is extracted, and the image is only rotated, respectively. The rotation angle of the test is set to $10^{\circ}.-50^{\circ}$. The algorithm first calculates the difference of the original image, calculates the difference histogram of the image and finds the peak value, and embeds the watermark through the peak value.

. Table 2 and Figure 6 shows that the results against different attacks: For geometric attacks such as translation, rotation, and scaling, the NC values extracted by the algorithm in this paper are all above 0.81, and the NC value can be 1 when the rotation angle anticlockwise is 10° and translation down 10%. It can be seen that all attack results of NC value are good.

Table2.PSNR and NC under Geometric Attacks.

Geometric Attacks	Attack strength	PSNR（dB）	NC
Rotation (clockwise)	10º	11.62	0.86
	30º	10.83	1
	50º	10.33	0.77
Rotation (Anticlockwise)	10º	11.51	1
	30º	10.69	0.81
	50º	10.41	0.88
Scaling	ˣ 0.6	-	0.75
	ˣ 0.8	-	0.81
Translation (Right)	10%	10.74	0.84
	20%	10.22	0.84
	30%	9.78	0.84
Translation (down)	10%	11.27	1
	30%	9.82	0.80
	50%	8.67	0.74
Clipping (Y direction)	10%	-	1
	30%	-	0.84
Clipping (X direction)	10%	-	0.93
	30%	-	0.93

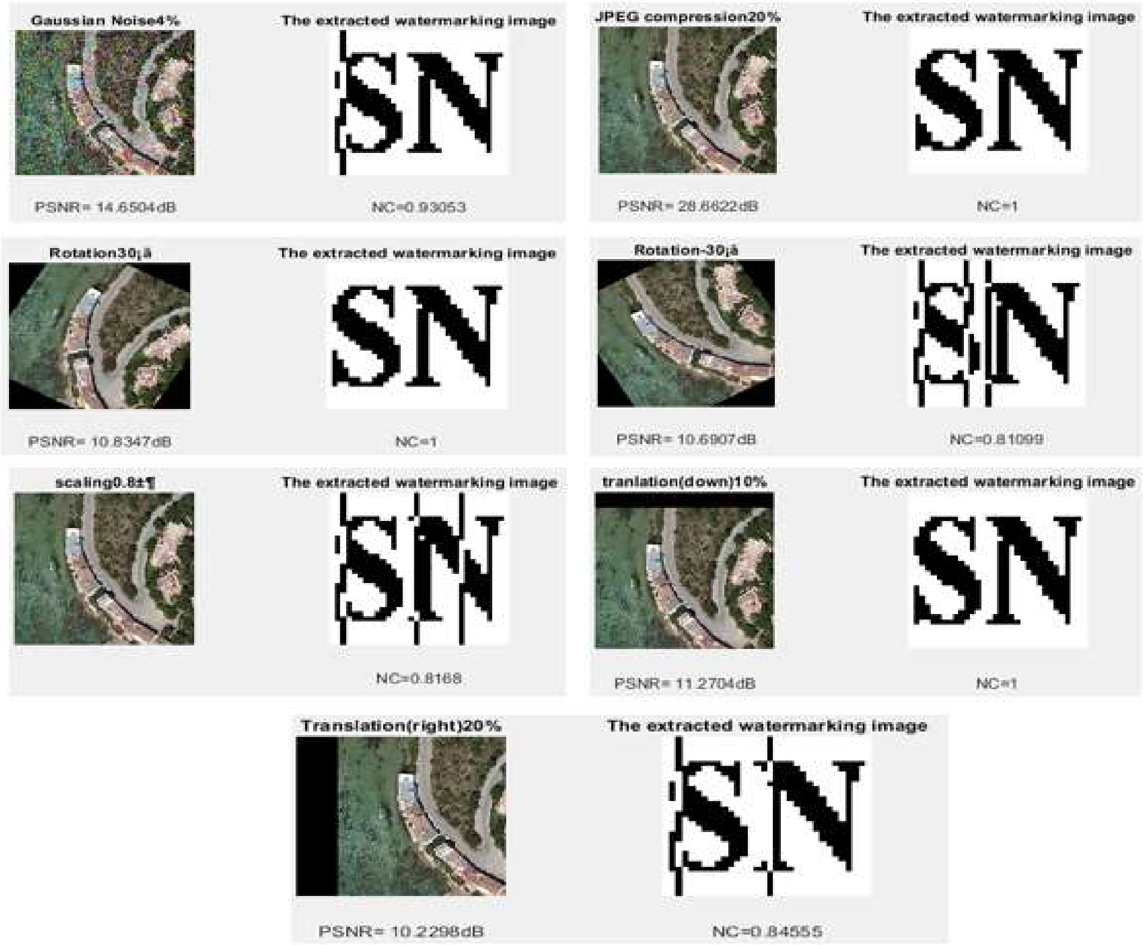


Fig 4: Different attacks on remote sensing image

5. Conclusion

This paper adopts the idea of the second generation of watermarking, combining the excellent characteristics of SURF operator and integer wavelet transform, taking into account the characteristics of remote sensing images, and proposes a robust blind watermarking algorithm for remote sensing images based on SURF feature regions. While maintaining the accuracy of remote sensing image data, the algorithm can effectively resist conventional attacks such as noise, filtering, JPEG compression, brightness adjustment, and geometric attacks such as rotation, scaling, cutting, and stitching, without the need to correct and restore the attacked image. Watermark can be extracted from it, which has strong practicability and efficiency, and can effectively protect the security of remote sensing images.

References

[1] Bhatti, U. A., Yu, Z., Yuan, L., Zeeshan, Z., Nawaz, S. A., Bhatti, M., ... & Wen, L. (2020). Geometric algebra applications in geospatial artificial intelligence and remote sensing image processing. IEEE Access, 8, 155783-155796.

[2] Bhatti, U. A., Yu, Z., Li, J., Nawaz, S. A., Mehmood, A., Zhang, K., & Yuan, L. (2020). Hybrid watermarking algorithm using clifford algebra with Arnold scrambling and chaotic encryption. *IEEE Access*, *8*, 76386-76398.

[3] Delaigle, J. F., Devleeschouwer, C., Macq, B., & Langendijk, L. (2002, August). Human visual system features enabling watermarking. In Proceedings. IEEE International Conference on Multimedia and Expo (Vol. 2, pp. 489-492). IEEE..

[4] Nawaz, S. A., Li, J., Bhatti, U. A., Mehmood, A., Shoukat, M. U., & Bhatti, M. A. (2020). Advance hybrid medical watermarking algorithm using speeded up robust features and discrete cosine transform. *Plos one*, *15*(6), e0232902

[5] Pereira, S., & Pun, T. (2000). Robust template matching for affine resistant image watermarks. IEEE transactions on image Processing, 9(6), 1123-1129.

[6] Jing, L., Zhang, Y., & Chen, G. (2008, October). Zero-watermarking for copyright protection of remote sensing image. In *2008 9th International Conference on Signal Processing* (pp. 1083-1086). IEEE.

[7] Cayre, F., Fontaine, C., & Furon, T. (2005). Watermarking security: theory and practice. IEEE Transactions on signal processing, 53(10), 3976-3987.

[8] Jiansheng, M., Sukang, L., & Xiaomei, T. (2009). A digital watermarking algorithm based on DCT and DWT. In Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009) (p. 104). Academy publisher.

[9] Kang, X., Huang, J., Shi, Y. Q., & Lin, Y. (2003). A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE transactions on circuits and systems for video technology, 13(8), 776-786.

[10] Bhatnagar, G., & Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. Computer Standards & Interfaces, 31(5), 1002-1013.

[11] Al-Haj, A., Mohammad, A. A., & Bata, L. (2011). DWT-based audio watermarking. Int. Arab J. Inf. Technol., 8(3), 326-333.

[12] Thakkar, F. N., & Srivastava, V. K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools and Applications, 76(3), 3669-3697.

[13] Gupta, P., & Parmar, G. (2017, July). Image Watermarking using IWT-SVD and its Comparative Analysis with DWT-SVD. In 2017 International Conference on Computer, Communications and Electronics (Comptelix) (pp. 527-531). IEEE.

[14] Alotaibi, R. A., & Elrefaei, L. A. (2019). Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). Applied Computing and Informatics, 15(2), 191-202.

[15] Solanki, N., Malik, S. K., & Chhikara, S. (2014). Roni medical image watermarking using dwt and rsa. International Journal of Computer Applications, 96(9).

[16] Ayubi, P., Barani, M. J., Valandar, M. Y., Irani, B. Y., & Sadigh, R. S. M. (2021). A new chaotic complex map for robust video watermarking. Artificial Intelligence Review, 54(2), 1237-1280.

[17] Nazari, M., & Mehrabian, M. (2021). A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. Multimedia Tools and Applications, 80(7), 10615-10655.