electronics

MDPI

Article

A Zero-Watermarking Algorithm Based on Vortex-like Texture Feature Descriptors

Fan Li [1,2] and Zhongxun Wang [1,2,*]

[1] School of Physics and Electronic Information, Yantai University, Yantai 264005, China; lifantasyer@163.com
[2] Shandong Data Open Innovation Application Laboratory of Smart Grid Advanced Technology, Yantai University, Yantai 264005, China
* Correspondence: ytdxwzx@163.com

Abstract: For effective copyright protection of digital images, this paper proposes a zero-watermarking algorithm based on local image feature information. The feature matrix of the algorithm is derived from the keypoint set determined by the Speeded-Up Robust Features (SURF) algorithm, and it calculates both the gradient feature descriptors and the vortex-like texture feature (VTF) descriptors of the keypoint set. Unlike traditional texture feature descriptors, the vortex-like texture feature descriptors proposed in this paper contain richer information and exhibit better stability. The advantage of this algorithm lies in its ability to calculate the keypoints of the digital image and provide a stable vector description of the local features of these keypoints, thereby reducing the amount of erroneous information introduced during attacks. Analysis of experimental data shows that the algorithm has good effectiveness, distinguishability, security, and robustness.

Keywords: zero-watermarking; texture features; image encryption

check for updates

Citation: Li, F.; Wang, Z. A Zero-Watermarking Algorithm Based on Vortex-like Texture Feature Descriptors. *Electronics* **2024**, *13*, 3906. https://doi.org/10.3390/electronics13193906

Academic Editor: Subir Halder

Received: 7 September 2024
Revised: 24 September 2024
Accepted: 1 October 2024
Published: 2 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In everyday life, digital images are ubiquitous and play crucial roles in information dissemination and visual art expression. With the rapid development of image processing tools and AI technologies, the copying, modification, and sharing of digital images have become remarkably easy [1]. These processes involve low operational costs, high dissemination speed, and wide application areas. However, the lack of legal constraints on copyright often puts digital image copyrights at unprecedented risk.

To aid creators in protecting their copyright information, digital watermarking technology has emerged, particularly for web images. Digital watermarking can be classified into embedding watermarks and zero-watermarking based on whether the carrier information is modified. The core steps of the zero-watermarking algorithm involve extracting and constructing stable features from the carrier image to generate a unique feature matrix, which is then computationally bound with the copyright data. Zero-watermarking not only effectively protects the copyright information of digital images but also preserves the original state of the image intact. This technology is widely applied in the fields of medical imaging [2], content authentication [3], and 3D modeling [4].

Currently, research by experts and scholars both domestically and internationally on zero-watermarking is generally divided into two main directions. One direction involves generating features that exhibit both robustness and distinguishability through geometric moments and algebraic operations. For instance, C.P. Wang et al. [5] combined Polar Complex Exponential Transform (PCET) coefficients with Logistic mapping, generating binary feature images based on the amplitude of PCET selected by chaotic mapping. Although this method shows good robustness and security, its stability is relatively poor when resisting large-scale cropping attacks. Yang H.Y. et al. [6] proposed a zero-watermarking algorithm based on Fast Quaternion Generic Polar Complex Exponential Transform (FQGPCET), which improves the issue of high false positive rates in zero-watermarking algorithms

by blending low-order moment coefficients. Hosny, K.M. et al. [7] used high-precision Gaussian integration to compute Multi-Channel Fractional-Order Legendre-Fourier Moments (MFrLFMs) for constructing zero-watermarks. This algorithm demonstrates good stability in resisting geometric attacks. Another research direction involves applying matrix transformations to the spatial or frequency domain features of images. For example, Yang K. et al. [8] mapped cover images to a geometrically invariant space, extracted the normalized effective part using the square of the unit circle, and applied Non-Sampling Contourlet Transform (NSCT) to generate zero-watermark images resistant to noise, filtering, image compression, and scale transformations. Anand A. et al. [9] combined Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) technology with Hamming codes, applying it to the encryption and compression of medical images. This approach shows high robustness against Gaussian noise, speckle noise, and image compression attacks. Huang T. et al. [10] performed a Non-Sampled Contourlet Transform (NSCT) on the original image to obtain low-frequency information, which was then processed in blocks. They used Multi-Level Discrete Cosine Transform (MDCT) to obtain subband coefficient matrices in low-frequency directions, and constructed feature vectors using Double Singular Value Decomposition (DSVD), resulting in a zero-watermarking algorithm with fast computation and high accuracy.

2. Basic Theory

2.1. Structure of Feature Matrix

The SURF algorithm is a local feature descriptor method in the field of image processing. This algorithm employs box filters and the Hessian matrix, simplifying and improving upon the traditional Scale-Invariant Feature Transform (SIFT) algorithm. The expression for the Hessian matrix at each pixel is given by Formula (1). When the determinant of the Hessian matrix reaches a local maximum, it indicates that the current point is either the brightest or darkest in the surrounding neighborhood, thereby allowing for the localization of keypoints. The expression for the determinant of the Hessian matrix is provided in Formula (2).

$$H(f(x,y)) = \begin{bmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial x^2} \end{bmatrix} \tag{1}$$

$$\det(H) = \frac{\partial^2}{\partial x^2}\frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y}\right) \tag{2}$$

The box filter is used to approximate the Gaussian filter. The box filter transforms the image filtering calculations into simple addition and subtraction operations on the sums of pixel values within different regions of the image, which can be efficiently performed using an integral image. To determine the dominant orientation, the algorithm designs a sector sliding window with a central feature point and an opening angle of 60°. The total sum of Haar wavelet features within this sector is computed. The sector window is selected with a step size of 0.2 radians, and the sum of wavelet features is continuously calculated. The direction corresponding to the maximum sum of these features is considered the dominant orientation. The calculation of the feature sum involves accumulating the Haar wavelet response values dx and dy from the image to obtain a vector (m_w,θ_w), as shown in Formulas (3) and (4). The dominant orientation is the direction θ corresponding to the maximum Haar response accumulation value, as given in Formula (5).

$$m_w = \sum_w dx + \sum_w dy \tag{3}$$

$$\theta_w = \arctan\left(\sum_w dx / \sum_w dy\right) \tag{4}$$

$$\theta = \theta_w | \max\{m_w\} \tag{5}$$

The SURF descriptors not only possess scale and rotation invariance [11] but also have illumination invariance, which is inherent to the wavelet responses themselves. Contrast invariance is achieved through the normalization of the feature vectors. Generally, higher-dimensional feature vectors contain more information, which enhances the distinguishability of the feature descriptors but also increases the time required for target matching. However, in zero-watermarking algorithms, the construction and extraction of watermark feature matrices do not involve target-matching issues, thus overcoming the limitations related to the dimensionality of feature descriptors in the SURF algorithm. Therefore, this paper proposes a novel zero-watermarking algorithm that combines the vortex-like texture feature descriptors with pre-processed SURF descriptors and introduces a constraint of approximately equal 0–1 element quantities. The overall process of this new algorithm is illustrated in Figure 1.

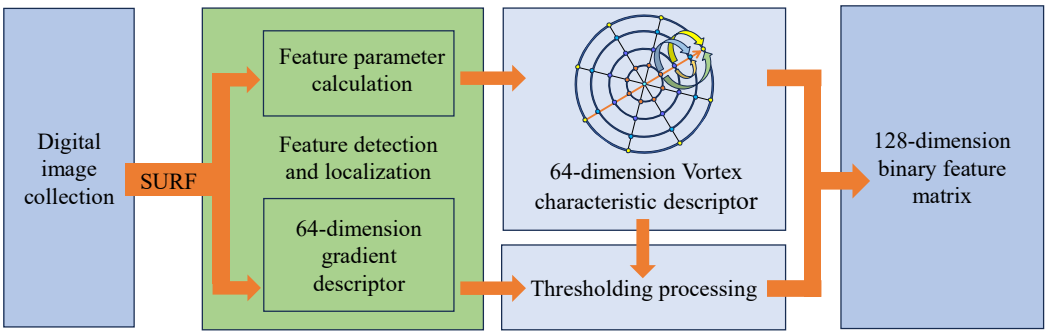


Figure 1. Construction process of vortex-like texture feature matrix.

2.2. Vortex-like Texture Feature Descriptors

Distinguishability is one of the criteria for evaluating the performance of zero-waterma rking algorithms. To further enhance the distinguishability of the feature matrix, this paper introduces a novel texture feature descriptor into the feature matrix construction process. With the image keypoint as the center and the principal orientation as the initial angle, the neighborhood radius is divided into four equal parts to form four concentric annular texture layers. The size of the sector angle is determined based on the dimensions of the copyright image being processed. In this paper, the annular neighborhood is divided into eight equal parts, with the coordinates of the intersection points of the angle segmentation lines and the four concentric rings defined as (x_{npi},y_{npi}), calculated using Formulas (6) and (7).

$$x_{npi} = x_n + \frac{i}{4} Rn \cos\left(\frac{2\pi p}{P} + \theta n\right) \tag{6}$$

$$y_{npi} = y_n - \frac{i}{4} Rn \sin\left(\frac{2\pi p}{P} + \theta n\right) \tag{7}$$

Here, n represents the n-th keypoint, R_n denotes the radius size of the neighborhood around the n-th keypoint, and θ_n indicates the principal orientation of the n-th keypoint. $i \in \{1,2,3,4\}$, and P is the total number of sampling points for a single radius neighborhood, thus P = 8. This value can be flexibly adjusted based on the specific needs of the copyright information. p represents the (p + 1)-th sampling point in the single radius neighborhood, where p is an integer within the range [0, 7]. Since pixel points in digital images are discrete, the computed coordinate values are likely not integers, meaning that the computed points cannot be directly mapped onto the digital image and hence do not correspond to actual pixel values. To address this issue, this paper introduces bilinear interpolation, which can estimate the corresponding pixel values at any position within the image [12]. This method reduces the distortion of feature information during the numerical–to–symbolic conversion process, preserves the continuity of the image, and better matches the gradual changes in real-world analog quantities, thereby facilitating the generation of more accurate

feature descriptors. This texture feature belongs to the geometric texture features category. Because the shape of its computational model approximates a vortex, it is named the vortex-like feature descriptor. The calculation of this feature descriptor is always based on the principal orientation and feature strength of the keypoint, and it constructs the subsequent feature vectors, providing good rotation and scale invariance. The dimensionality of the single-point feature vector is set to 64 dimensions, where 32 dimensions are derived from comparing the angular points in the neighborhood with the feature keypoint, and the remaining 32 dimensions are derived from comparing pixel points at the same angle within the four concentric rings. This geometric structure ensures that the vector not only fully represents the texture information within the feature point's domain but also possesses enhanced distinguishability and robustness, as shown in Figure 2.

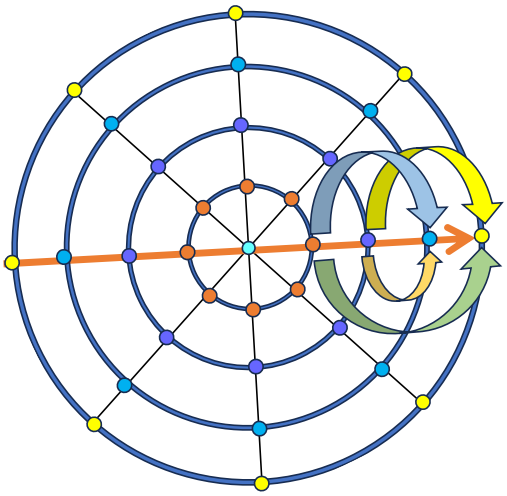


Figure 2. Geometric structure diagram of vortex-like texture feature descriptors.

In Figure 2, the orange arrow that coincides with the diameter represents the main direction of the keypoint of this feature. The neighborhood is determined as four concentric rings with different radii. The purpose is to ensure the rotational invariance of the texture feature. The sampling points on different rings are distinguished by different colors for easy observation by the human eye. The four curved arrows represent four calculations in a single radius direction and are used to generate four feature elements. This step needs to be repeated for each radius direction. The overall direction of the arrows can be defined as from inside to outside, and the comparison calculation is carried out layer by layer. This vortex-type texture feature descriptor uses rings and straight lines in different directions as shape constraints, enhancing the stability and distinguishability of the subsequent feature matrix.

The vortex-like texture feature descriptors and the SURF descriptors share similar feature properties. Both are centered around keypoints and are computed within the same neighborhood range, representing different feature information within the same area. Therefore, this paper combines the two feature descriptors based on their similarities, using the vortex-like feature matrix as the baseline. For each vector in the SURF matrix, different thresholds are determined to achieve binarization of the matrix while maintaining the balance of 0–1 elements across the entire matrix. This algorithm does not compute the overall feature information of the image but focuses on stable keypoints and representative points within their neighborhood. By introducing more distinguishable vectors and maintaining the matrix's robustness through vortex-like geometric constraints, the algorithm mitigates the distortion effects of strong single-point attacks and buffers the impact of global attacks on the feature matrix.

2.3. Henon Encryption Model

Compared to embedded digital watermarking algorithms, zero-watermarking offers the advantage of perfect invisibility. However, this technology typically requires a rigorous encryption model to enhance security. The construction process of zero-watermarking necessitates the introduction of various encryption techniques to ensure that, even if the feature matrix construction process is exposed, malicious actors cannot perform secondary operations or alter copyright ownership. In this paper's algorithm, the watermark image is first subjected to Arnold mapping for positional scrambling, which disrupts the image's visual information. Then, using keys generated by the Henon map, logical operations are performed to encrypt the binary feature image and the scrambled watermark image, thereby ensuring the security of the zero-watermarking algorithm. The Henon map is a two-dimensional chaotic mapping model characterized by nonlinearity, randomness, sensitivity to initial conditions, and convenience [13]. Its basic mapping formula is given in Formula (8).

$$\begin{aligned} x_{n+1} &= 1 + y_n - ax_n^2 \\ y_{n+1} &= bx_n \end{aligned} \tag{8}$$

Among them, a and b are parameters of the chaotic system. As parameter a increases, the Henon system enters a chaotic state through period-doubling bifurcation. A common parameter combination is a = 1.4 and b = 0.3. Under this parameter combination, the maximum Lyapunov exponent of the Henon system is positive. The Lyapunov exponent is an important indicator for measuring the degree of chaos of a system. When the maximum Lyapunov exponent of the system is greater than 0, it proves that the system is in a chaotic state. In addition, when the value range of a is within (1.03, 1.4), the system will also exhibit chaotic characteristics. As the two parameters a and b change, the system may change from a chaotic state to a periodic state or a stable state. Therefore, this parameter combination will not change frequently. We can have an intuitive understanding of the chaotic system with the help of the following chaotic model, as shown in Figure 3.

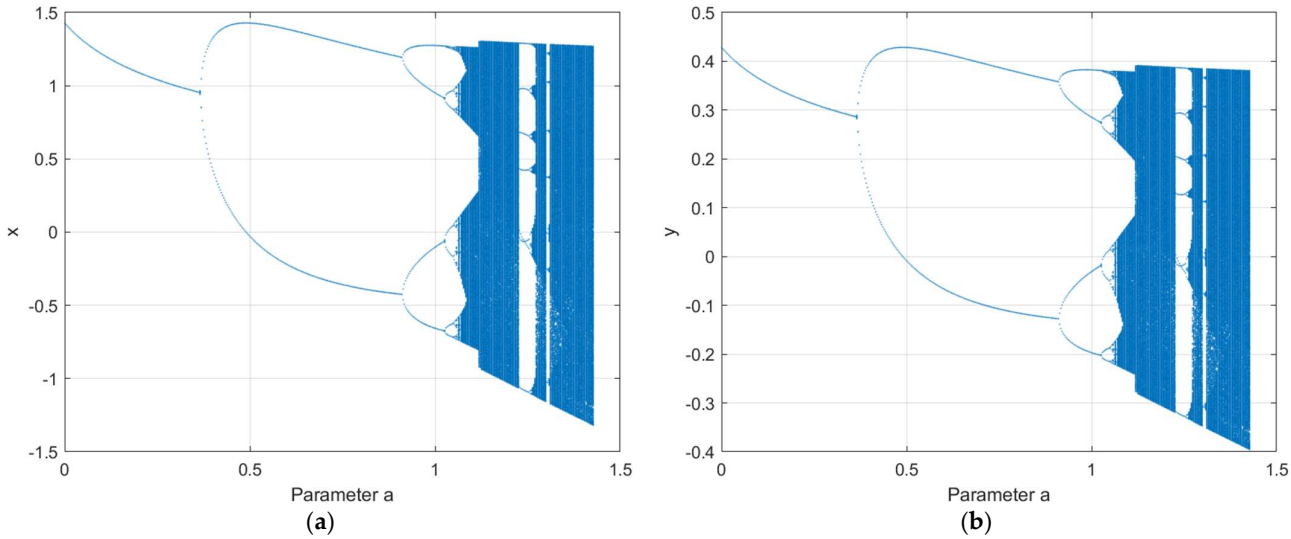


Figure 3. Chaos model of x and y components in Henon mapping. (**a**) The bifurcation diagram formed by the variation of the x-component with the system parameter a; (**b**) The bifurcation diagram formed by the variation of the y-component with the system parameter a.

As can be seen from Figure 3, when parameter a is within the range of (1.03, 1.4), the system state suddenly bifurcates, resulting in the simultaneous existence of multiple stable states and periodic states in the system. These branches extend in a bifurcated manner, forming the characteristic structure on the bifurcation diagram. The bifurcation diagram

can provide an intuitive understanding of the chaotic system. It shows the phase transition phenomenon of the system state as the parameters change.

3. Algorithm Process

3.1. Zero-Watermarking Generation Algorithm

Whether in the generation process of zero-watermark images or the subsequent extraction of copyright information, a crucial step is the creation of the binary feature matrix for the carrier image. The calculation process for the vortex-like feature matrix can be referenced in Algorithm 1. In this context: let C represent the carrier image, with the experimental material size set at 2000 × 2000 pixels. The dimensions of the carrier image must exceed those of the copyright information image. Let T denote the computed matrix, with its dimensions equal to N, which is typically determined by the size of the copyright pixel image. N is the number of keypoints, R is the sequence matrix used to store the preprocessed SURF vector group, S is the SURF descriptors matrix, V is the Vortex-like Feature Descriptors (VFT) matrix,Vi represents the difference in the number of 0–1 elements in V(:,i), and Di indicates the threshold for binarization in S(:,i).

The value of N must be maintained within an appropriate range; an excessively large N will lead to a linear increase in computational complexity and extended processing time, while a small N may reduce the information capacity of the zero-watermark image, rendering it incapable of storing effective information and diminishing the distinguishability of the zero watermark. To ensure consistency of the N keypoints in the images before and after attacks, this paper improves upon the traditional SURF algorithm by introducing a threshold determination system. A keypoint is identified as a stable feature only when multiple parameters meet the criteria. The weighted results of the maximum and second maximum values in the feature vector are then used as the basis for ranking the subsequent N keypoints, thereby enhancing the stability of the feature keypoints.

1. Read the carrier image that requires copyright protection and the copyright information to be embedded. Initially determine the dimensional parameters of the feature matrix. Use the SURF algorithm to identify N keypoints in the image with suitable and stable intensity values, and store the corresponding descriptors arrays.
2. Apply the VTF (Vortex-like Texture Feature) generation algorithm. For each keypoint, use the neighborhood radius as a parameter to generate 64-dimensional local texture feature descriptor vectors and count the number of 0–1 elements in these vectors. Based on the number of 0–1 elements in the 64-dimensional VTF generation descriptor vector, determine the threshold size for the corresponding SURF descriptor vector and binarize it, ensuring that the number of 0–1 elements in the concatenated 128-dimensional vector is similar. Combine and arrange the binarized feature vector matrix with the vortex-like texture feature matrix to generate a binary feature matrix based on VTF generation descriptors.
3. Perform Arnold positional scrambling and Henon mapping chaotic encryption on the watermark information to be embedded. XOR the encrypted image with the final encrypted VFT matrix to obtain the zero-watermarking image. Apply for a timestamp from an authoritative timestamp authority and bind the final zero-watermarking signal with it. Subsequently, register the bound signal in the Intellectual Property Rights Database (IPRD). The process of constructing and registering the zero-watermarking signal is thus completed.

The above algorithm steps illustrate the process of feature extraction for digital copyright images and the generation of zero-watermark images, as shown in Figure 4.

Algorithm 1: Vortex-like texture feature generation algorithm

Input: C; %Carrier iamge
Output: T; %Binary feature image
Initialization: L←zero(64*N);%Sequence matrix
Invoke the SURF algorithm to determine N keypoints.
for (k = 1 to N) **do**
  Compute the SURF descriptors matrix: S_{64*N}
  Compute the VFT descriptors matrix: V_{64*N},
  for (i = 1 to N) **do**
    Ai0← sum(V(:, i) == 0) ;Ai1←sum(V(:, i) == 1) ;
    V_i = abs(Ai0-Ai1);
    R(:,i)←Sort S(:,i);
    r←R(:,i); %vector
    while (Ai0 > Ai1) **do**
    D_i = r((64-V_i)/2); %threshold value
    for (j = 1 to 64) **do**
      if (S(j,i) > Di) **then**
        S(j,i) = 0
      else S(j,i) = 1
    end
    while(Ai0 ≤ Ai1) **do**
    D_i = r((64 + V_i)/2);
    for (j = 1 to 64) **do**
      if (S(j,i) > D_i) **then**
        S(j,i) = 0
      else S(j,i) = 1
    end
  end
end
T←vertcat(V,S);
return T;

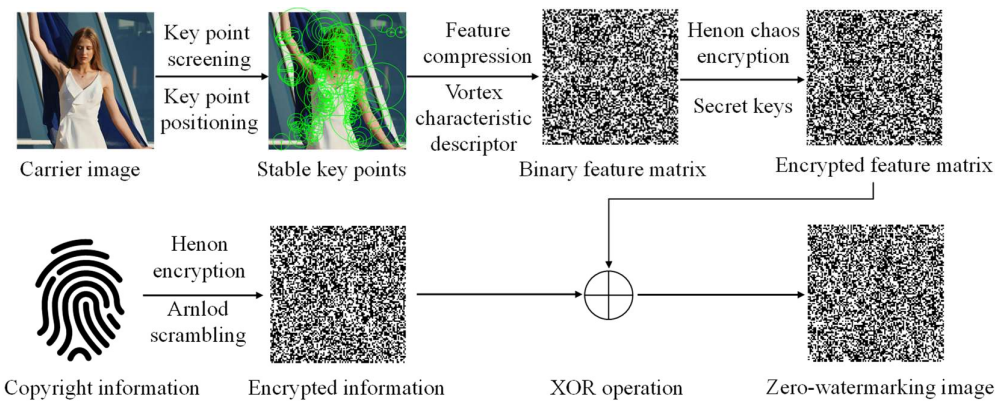


Figure 4. Zero-watermarking generation algorithm process.

3.2. Copyright Information Extraction Algorithm

The copyright information extraction algorithm is largely similar to the zero-watermark generation algorithm, with the main difference being that the zero-watermark generation algorithm operates on the feature matrix and the encrypted watermark image, whereas the copyright information extraction algorithm works with the damaged feature matrix and the zero-watermark image. Therefore, this section will only describe the algorithmic steps involved in copyright extraction.

1. Preprocess the attacked copyright image and use the first two steps from Section 3.1 to obtain the binary feature matrix based on the VFT generation algorithm. Encrypt this matrix using a private key. Retrieve the zero-watermarking image bound to it from a third-party intellectual property rights database, and perform an XOR operation with the encrypted VFT binary image to generate the watermark information image that needs to be decrypted and have its scrambling order restored.
2. Decrypt the above ciphertext watermark information image to obtain an image containing symbolic copyright information, ensuring that the copyright information can be recognized and distinguished both subjectively and objectively. If multiple copyright disputes are involved, a timestamp authority can be requested to issue a timestamp with the binding date for legal copyright tier protection. Since zero-watermarking does not involve embedding capacity issues, a single image can have multiple public keys added based on the private key.

The original author and various levels of copyright holders can use their respective keys to generate corresponding chaotic watermarks to confirm tiered copyrights. The above algorithm steps illustrate the process of feature extraction from damaged digital copyright images and the extraction of watermark images containing copyright information, as shown in Figure 5.

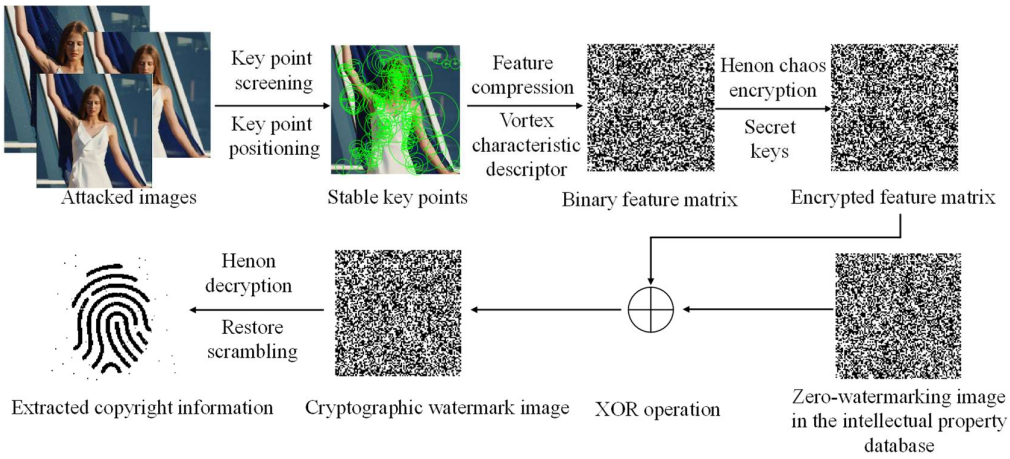


Figure 5. Copyright information extraction algorithm process.

4. Experimental Results and Analysis

4.1. Experimental Materials

This paper selects the following non-copyrighted images as experimental materials and labels them with alphabetical characters for subsequent streamlined processing. This approach aims to demonstrate the effectiveness, security, distinguishability, and robustness of the zero-watermarking algorithm. The carrier image is chosen to be 2000 × 2000 pixels in size, while the copyright watermark information image is 128 × 128 pixels, as shown in Figure 6.

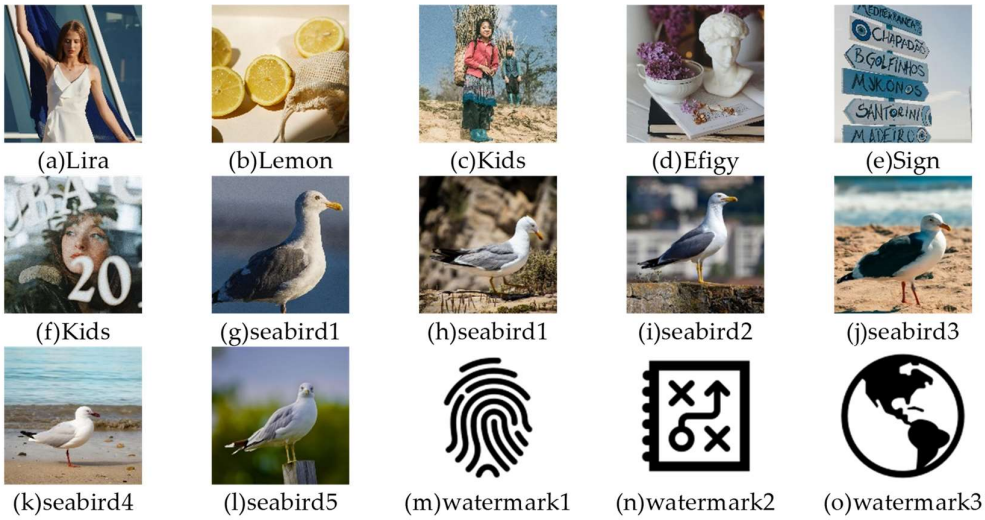


Figure 6. Experimental material images and their labels.

4.2. Effectiveness and Distinguishability Experiments

The performance of a zero-watermarking algorithm largely depends on its effectiveness and distinguishability. Effectiveness and distinguishability refer to the degree of correlation between feature matrices of different images and similar images after applying the same zero-watermarking algorithm. This paper uses the Normalized Correlation (NC) value to measure the similarity between feature matrices. The NC value ranges from 0 to 1, with a smaller value indicating lower similarity between feature matrices and better performance of the zero-watermarking algorithm. The specific calculation method is given in Formula 9.

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i,j)^2}} \tag{9}$$

A high-performance zero-watermarking algorithm can keep the NC values of different images and even similar images within a lower range, thereby enhancing the technical credibility of the copyright holder. To verify the effectiveness and distinguishability of the zero-watermarking algorithm, NC values of the binary feature matrices of the aforementioned sample images are compared. The specific values are shown in Figure 7.

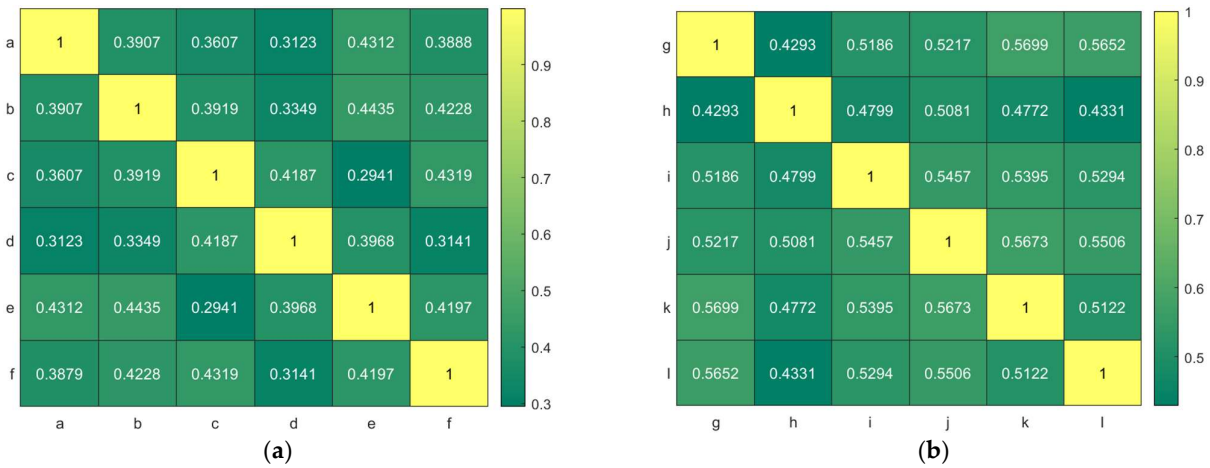


Figure 7. Comparison of NC values in the feature matrix of carrier images. (**a**) Analysis of feature matrix correlation for different images; (**b**) Similarity analysis of feature matrices for similar images.

From the analysis of the data in Figure 7, it can be seen that the zero-watermarking algorithm proposed in this paper controls the feature similarity between different images at around 0.4 and the feature similarity between similar images at around 0.5. The similar images refer to six seagull images in the experimental material with similar feature themes. Even though images g-h may appear highly similar to the human eye, the feature matrix construction algorithm can still accurately distinguish their differences. This demonstrates the effectiveness and distinguishability of the proposed algorithm.

4.3. Security Experiments

From the perspectives of the commercial and copyright protection sectors, the procedural steps and encryption steps of a zero-watermarking algorithm must be publicly transparent to provide strong credibility. Most details of the zero-watermarking algorithm need to be openly demonstrated, which presents a significant challenge to the algorithm's security. To validate the security of the proposed algorithm, we conduct experiments from two aspects: the security of the feature matrix and the security of the watermark information.

Assuming that all information except the private key is publicly available, an attacker would only need to crack one key sequence. We assume the correct key is K1 = 0.17124650 and test 100 key sequences in the neighborhood of the correct sequence. The feature matrices generated with these keys are compared with those generated using the correct key. The encryption model based on Henon mapping shows a stable sensitivity to incorrect keys, with correlations remaining stable between [0.4842, 0.5147], consistently fluctuating around 0.5. According to this experimental analysis, the feature matrix encryption model of the algorithm responds very consistently to incorrect keys. The probability of brute-forcing the feature matrix without knowing the key length and specific range is extremely low. The experimental results are shown in Figure 8.

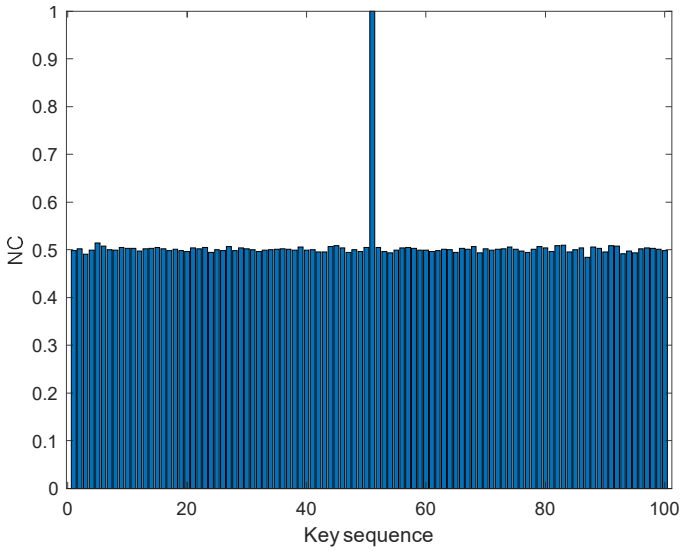


Figure 8. Comparison of feature similarity under approximate key conditions.

In Figure 8, the vertical axis represents the similarity between the feature matrix generated by different key sequences and the correct feature matrix, while the horizontal axis indicates the indices of 100 similar keys within the neighborhood of the correct key. It is evident that the computed matrix aligns with the feature matrix only when the key corresponds to the correct key itself, while the similarities for other incorrect keys remain stable, further ensuring the security of the algorithm.

Since zero-watermarking algorithms do not modify the carrier image and the image containing watermark information has relatively few pixels, attackers may focus on differential attacks targeting the watermark information to analyze the image and attempt

to decipher the original information. To address this, the encryption model in this paper incorporates anti-differential attack mechanisms. By using Henon mapping as the encryption model and integrating the coordinate information of the binary watermark into the initial value calculations of the key, the model can effectively counter differential attacks.

In this paper, experiments on single-pixel tampering of images containing watermark information are conducted. The tampered image and the untampered image are both input into the Henon mapping encryption model to obtain a control group of encrypted watermark images. To present the differences between encrypted images more objectively, a performance metric is introduced: the Number of Pixels Change Rate (NPCR). The specific calculation method is given in Formula (10).

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{10}$$

where M and N represent the height and width of the image, and i and j represent the coordinates of the pixels. If the pixel values at the same coordinates in the two images are identical, D(i,j) = 0; otherwise, D(i,j) = 1. The experiment compares the NPCR values between the encrypted image with single-pixel tampering and the encrypted image of the original watermark. The results are shown in Figure 9.

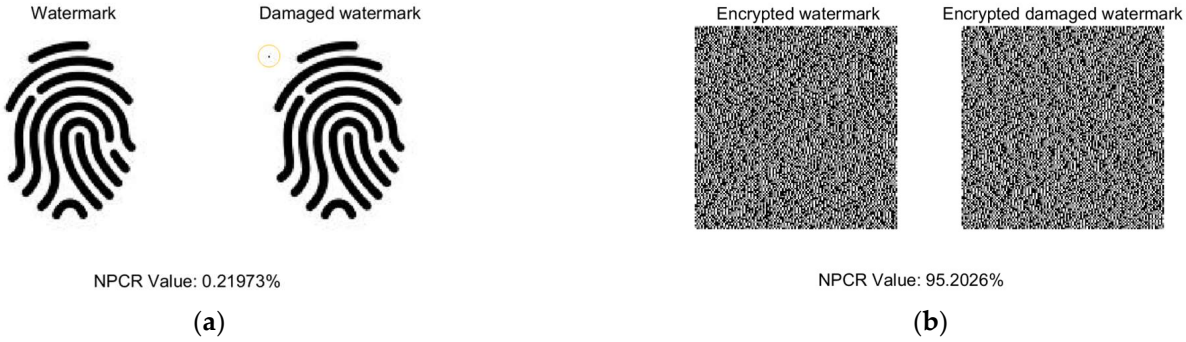


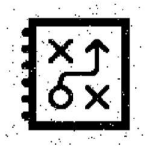
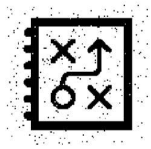
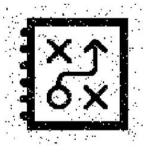
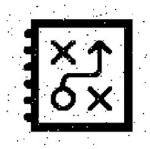
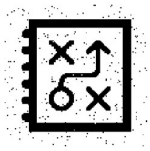
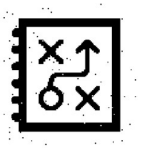
Figure 9. Comparison experiment on anti-differential attacks. (**a**) NPCR value of the original watermark image after single-pixel tampering; (**b**) NPCR value of the encrypted watermark image after single-pixel tampering.

It can be observed that while the impact of single-pixel tampering on the original watermark is minimal, the NPCR value of the tampered encrypted image reaches 95.2026%, which is very close to the ideal value. This demonstrates the security of the encryption algorithm.

4.4. Robustness Experiments

In addition to effectiveness, distinguishability, and security, a reliable zero-watermarking algorithm should also exhibit excellent robustness. Robustness ensures that the copyright information embedded in the watermark can be stably and clearly extracted from the carrier image even after various digital attacks. In this section, we simulate several common image attacks (such as noise addition, filtering, JPEG compression, rotation, and scaling) and compare the NC values between the damaged and original watermarked images. This comparison is conducted from both the subjective visual perception of the human eye and objective data parameters, in order to validate the information integrity of the three copyright watermark images. The results are presented in Table 1.

Table 1. The integrity of watermarking information under various attacks.

	Gaussian Noise	Salt and Pepper Noise	JPEG	Rotation	Gaussian Filtering	Median Filtering	Scaling
Lira	 0.9999	 0.9946	 1	 0.9911	 1	 0.9978	 1
Lemon	 0.9999	 0.9948	 1	 0.9907	 1	 0.9962	 1
Kids	 0.9999	 0.9953	 1	 0.9903	 1	 0.9876	 1
Efigy	 0.9999	 0.9950	 1	 0.9906	 1	 0.9973	 1
Sign	 1	 0.9940	 1	 0.9910	 1	 0.9949	 1
Tina	 0.9997	 0.9942	 0.9998	 0.9908	 0.9998	0.9982	0.9998

As shown in Table 1, the integrity of copyright information in the three watermarked images is largely preserved. The zero-watermarking algorithm proposed in this paper demonstrates remarkable robustness against various attacks. Specifically, the watermark information remains almost intact with near 100% integrity when subjected to Gaussian noise with a mean of 0 and a variance of 0.01, Gaussian filtering with a 3×3 convolution kernel, JPEG compression with a quality factor of 30, and scaling attacks with a size coefficient of 25%. Similarly, the integrity of the watermark information is maintained at over 99% when exposed to salt-and-pepper noise with a mean of 0 and a variance of 0.01, rotation attacks with a 5° rotation angle, and median filtering with a 3×3 convolution kernel. From a subjective evaluation perspective, it is observed that the edge information of the three watermarked images is well preserved. Most noise is scattered around the periphery of the

images, with only a small amount of noise affecting the central regions. This section of the experiments demonstrates that the proposed zero-watermarking algorithm can effectively withstand common image processing attacks, exhibiting exceptional robustness.

The performance of the proposed algorithm was compared with several recently published digital watermarking algorithms, and the results are presented in Table 2.

Table 2. Robustness comparison between the VFT algorithm and other algorithms.

Attack Mode	Attack Intensity	Normalized Correlation						
		VFT	[14]	[15]	[16]	[17]	[18]	[19]
Gaussian noise	0.01	0.9999	0.9861	0.9470	0.9946	0.9932	0.9974	0.9502
Salt and pepper noise	0.01	0.9947	0.9925	0.9544	1	0.9922	0.9994	0.9750
Scaling	25%	1	0.9985	0.9585	1	0.9932	0.9967	0.9960
Rotation	5°	0.9908	0.9672	0.9892	0.9946	0.9948	0.9993	0.9906
Gaussian filtering	3×3	1	NAN	0.9946	0.9964	1	0.9996	NAN
Median filtering	3×3	0.9953	0.9967	0.9818	0.9946	0.9951	0.9960	0.9897
JPEG	30	1	0.9955	0.9762	NAN	0.9939	0.9938	0.9794

Table 2 shows that the zero-watermarking algorithm based on VTF descriptors proposed in this paper has performance comparable to other algorithms. However, it provides more complete preservation of copyright information in watermarked images against attacks such as Gaussian noise, scaling, Gaussian filtering, and JPEG compression, with the highest average NC values in the group. This is due to the properties of the VTF matrix, which focuses on the features of stable keypoints and their local neighborhoods rather than global image characteristics. As a result, the algorithm's robustness is superior to that of other methods listed in Table 2, especially against attacks that do not significantly disrupt the image's texture.

5. Conclusions

This paper proposes a zero-watermarking algorithm based on VTF descriptors, which integrates the stable feature matrix from the SURF algorithm with a novel VTF matrix, creating a multi-threshold feature matrix constrained by binary elements. The stability and distinguishability of this feature matrix are derived from the domain information of stable keypoints in the carrier image. The VTF descriptors in the neighborhood combine vortex plane geometric topology with gradient features, resulting in a robust structure resistant to rotation, scaling, and noise attacks. In terms of security, we incorporate the Henon map encryption model and a key sequence resistant to differential attacks, leveraging the chaotic model's sensitivity to initial values for private key encryption of critical information at each step of the algorithm. Consequently, the VTF-based zero-watermarking algorithm demonstrates excellent effectiveness, distinguishability, security, and robustness.

However, the algorithm has limitations in resisting large-scale cropping attacks, which indiscriminately remove keypoints and result in the loss of information in the constructed feature matrix, thus failing to protect copyright information. Future research will consider incorporating error-correcting codes among keypoints to restore removed information through encoding constraints and subsequent computations [20], ensuring the integrity of copyright information in watermarked images.

Author Contributions: Writing—original draft preparation, F.L.; supervision, Z.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by Yantai City 2021 School-Land Integration Development Project Fund under Grant 1521001-WL21JY01,the Science and Technology-Based Small and Medium-Sized Enterprise Innovation Capacity Enhancement Project of Shandong Province under Grant 2023TSGC0823. Science and Technology-Based Small and Medium-Sized Enterprise Innovation Capacity Enhancement Project of Shandong Province under Grant 2023TSGC0823.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kadian, P.; Arora, S.M.; Arora, N. Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. *Wirel. Pers. Commun.* **2021**, *118*, 3225–3249. [CrossRef]
2. Xia, Z.; Wang, X.; Zhou, W.; Li, R.; Wang, C.; Zhang, C. Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms. *Signal Process.* **2019**, *157*, 108–118. [CrossRef]
3. Zhao, C.; Liu, W. Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm. *Acta Autom. Sin.* **2012**, *38*, 609–617. [CrossRef]
4. Zhang, Z.; Zhang, L.; Wang, P.; Zhang, M.; Tan, T. Robust watermarking algorithm based on mahalanobis distance and ISS feature point for 3D point cloud data. *Earth Sci. Inform.* **2024**, *17*, 783–796. [CrossRef]
5. Wang, C.-P.; Wang, X.-Y.; Chen, X.-J.; Zhang, C. Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. *Multimed. Tools Appl.* **2016**, *76*, 26355–26376. [CrossRef]
6. Yang, H.-Y.; Qi, S.-R.; Niu, P.-P.; Wang, X.-Y. Color image zero-watermarking based on fast quaternion generic polar complex exponential transform. *Signal Process. Image Commun.* **2019**, *82*, 115747. [CrossRef]
7. Hosny, K.M.; Darwish, M.M.; Fouda, M.M. New Color Image Zero-Watermarking Using Orthogonal Multi-Channel Fractional-Order Legendre-Fourier Moments. *IEEE Access* **2021**, *9*, 91209–91219. [CrossRef]
8. Yang, K.; Wang, W.; Yuan, Z.; Zhao, W. Strong robust zero watermarking algorithm based on NSCT transform and image normalization. In Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 October 2018. [CrossRef]
9. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [CrossRef]
10. Huang, T.; Xu, J.; Yang, Y.; Tu, S.; Han, B. Zero-Watermarking Algorithm for Medical Images Based on Nonsubsampled Contourlet Transform and Double Singular Value Decomposition. In Proceedings of the 2021 5th Asian Conference on Artificial Intelligence Technology (ACAIT), Haikou, China, 29–31 October 2021; pp. 65–76. [CrossRef]
11. Kaur, P.; Kumar, N.; Singh, M. Surfbcs: Speeded up robust features based fuzzy vault scheme in biometric cryptosystem. *J. Supercomput.* **2023**, *79*, 12292–12316. [CrossRef]
12. Bilal, M.; Ullah, Z.; Mujahid, O.; Fouzder, T. Fast Linde–Buzo–Gray (FLBG) Algorithm for Image Compression through Rescaling Using Bilinear Interpolation. *J. Imaging* **2024**, *10*, 124. [CrossRef] [PubMed]
13. Wang, B.; Zhang, Z.; Siarry, P.; Liu, X.; Królczyk, G.; Hua, D.; Brumercik, F.; Li, Z. A nonlinear African vulture optimization algorithm combining Henon chaotic mapping theory and reverse learning competition strategy. *Expert Syst. Appl.* **2024**, *236*, 121413. [CrossRef]
14. Wang, R.; Han, S.; Zhang, P.; Yue, M.; Cheng, Z.; Zhang, Y. A Novel Zero-Watermarking Scheme Based on Variable Parameter Chaotic Mapping in NSPD-DCT Domain. *IEEE Access* **2020**, *8*, 182391–182411. [CrossRef]
15. Kang, X.; Zhao, F.; Chen, Y.; Lin, G.; Jing, C. Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm. *J. Vis. Commun. Image Represent.* **2020**, *70*, 102804. [CrossRef]
16. Wang, X.; Wen, M.; Tan, X.; Zhang, H.; Hu, J.; Qin, H. A novel zero-watermarking algorithm based on robust statistical features for natural images. *Vis. Comput.* **2022**, *38*, 3175–3188. [CrossRef]
17. Wang, H.; Chen, Y.; Zhao, T. Modified Zernike Moments and Its Application in Geometrically Resilient Image Zero-Watermarking. *Circuits Syst. Signal Process.* **2022**, *41*, 6844–6861. [CrossRef]
18. Yang, J.; Hu, K.; Wang, X.; Wang, H.; Liu, Q.; Mao, Y. An efficient and robust zero watermarking algorithm. *Multimed. Tools Appl.* **2022**, *81*, 20127–20145. [CrossRef]
19. Chu, R.; Zhang, S.; Mou, J.; Gao, X. A zero-watermarking for color image based on LWT-SVD and chaotic system. *Multimed. Tools Appl.* **2023**, *82*, 34565–34588. [CrossRef]
20. Ramos, A.M.; Artiles, J.A.P.; Chaves, D.P.B.; Pimentel, C. A Fragile Image Watermarking Scheme in DWT Domain Using Chaotic Sequences and Error-Correcting Codes. *Entropy* **2023**, *25*, 508. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.