Hindawi
Security and Communication Networks
Volume 2021, Article ID 6675354, 16 pages
https://doi.org/10.1155/2021/6675354

Research Article

Visual Security Assessment via Saliency-Weighted Structure and Orientation Similarity for Selective Encrypted Images

Zhengguo Wu,[1] Kai Zhang,[1] Yannan Ren,[2] Jing Li,[3] Jiande Sun,[1] and Wenbo Wan[1]

[1]*School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China*
[2]*School of Information Science and Electrical Engineering, Shandong Jiaotong University, Jinan 250357, China*
[3]*College of Intelligent Engineering, Shandong Management University, Jinan 250357, China*

Correspondence should be addressed to Wenbo Wan; wanwenbo@sdnu.edu.cn

Received 17 November 2020; Revised 25 December 2020; Accepted 7 January 2021; Published 23 January 2021

Academic Editor: Jinwei Wang

Selective encryption has been widely used in image privacy protection. Visual security assessment is necessary for the effectiveness and practicability of image encryption methods, and there have been a series of research studies on this aspect. However, these methods do not take into account perceptual factors. In this paper, we propose a new visual security assessment (VSA) by saliency-weighted structure and orientation similarity. Considering that the human visual perception is sensitive to the characteristics of selective encrypted images, we extract the structure and orientation feature maps, and then similarity measurements are conducted on these feature maps to generate the structure and orientation similarity maps. Next, we compute the saliency map of the original image. Then, a simple saliency-based pooling strategy is subsequently used to combine these measurements and generate the final visual security score. Extensive experiments are conducted on two public encryption databases, and the results demonstrate the superiority and robustness of our proposed VSA compared with the existing most advanced work.

1. Introduction

Nowadays, with the widely pervasive usage of interaction devices, such as cameras, cloud storage devices, and the explosive growth of digital images, privacy protection has attracted a lot of attention from researchers [1–5]. Various security schemes, such as digital watermarking [6–8], steganography [9], and encryption [10], have been developed to protect copyright, and encryption is the mostly accepted approach which can ensure the security and integrity of data all the time. Roughly, the existing image encryption methods can be divided into two categories: full encryption and selective encryption. Full encryption refers to encrypting the entire image; therefore, we cannot get any information about the original image from the encrypted image. However, the content information of the image cannot be revealed if several kinds of redundant information are unencrypted. For this reason, traditional full encryption methods such as AES are not suitable for image data, because these methods always encrypt all the information of the image which cost a lot of time. Therefore, researchers proposed the selective encryption algorithm that has been widely used to protect the visual content of multimedia by only encrypting the specified parts of the multimedia data. A great variety of selective encryption algorithms [10–16] have been proposed in recent decades. Compared with full encryption algorithms, selective encryption has two main advantages as follows. First, it can be extremely fast on encryption and decryption because only a portion of the data needs to be encrypted. Second, the selective encrypted multimedia data can prevent the abuse of the essential visual property of the original data. These advantages make selective encryption highly desirable for protecting more and more image and video data which hide a large amount of personal privacy on the network.

The purpose of security analysis for selective image encryption is to measure the degree of visual security of selective encrypted images. Visual security analysis can measure the performance of the selective encryption methods and then help us to optimize the encryption methods. Since humans are the ultimate receivers of images, subjective tests conducted by human viewers are the most

suitable and accurate way to evaluate the visual security of selective encrypted images. However, such tests are too time-consuming and laborious to accomplish real-time applications. For this reason, visual security assessment [17] (VSA) is proposed to evaluate the visual security of selective encrypted images by measuring the unintelligibility or unrecognizability of the image automatically, which indicates the amount of useful information about the original image that an attacker can obtain from its selective encrypted image via visual perception. The higher the unrecognizability degree of the selective encrypted image is, the less visual information the attacker can obtain. In such a situation, it becomes more difficult for an attacker to obtain information about the original image and the selective encryption method is more secure.

In the past decades, many efforts have been conducted to design VSAs. At the beginning, researchers believe that visual security of images has a strong relationship with image quality. Therefore, they directly used the well-known image quality assessment [18] (IQA) methods to evaluate the visual security degree of selective encrypted images, such as peak signal-to-noise ratio (PSNR), structural similarity (SSIM) [19] and visual information fidelity (VIF) [20], and the images with lower quality tend to have higher security. However, these metrics may be inconsistent with the concept of security strength. For example, an image with a lower PSNR value may be even more recognizable than one with a higher PSNR value. These IQA methods do not take full account of the characteristics of the selective encrypted images. For selective encrypted images, an important feature is that the skeleton of the image is still intelligible but the details are almost unintelligible [21]. On the other hand, the structure information can express the skeleton of an image which plays a more important role in selective encrypted images. Subsequently, several VSAs have been developed based on some visual features of selective encrypted images, e.g., edge similarity score (ESS) [22] based on the edge, luminance similarity score (LSS) [22] utilizing luminance feature, local feature-based visual security (LFBVS) [23] using luminance and localized gradient, and the visual security index-based Canny (VSI-Canny) [21] which extracted edge and texture features. However, these VSAs do not fully consider the role of visual perception [24–26] factor in VSAs, because the visual perception of each region differs from another according to the principle of the human visual system (HVS), which also have different impacts on visual security evaluation. Additionally, HVS presents an obvious visual saliency mechanism. HVS focuses only on these important regions for detailed perception and withdraws the other regions. The regions have high saliency values play more important roles than the other regions for visual perception, and the information leakage on the high saliency regions has a larger influence on the visual security assessment.

Motivated by the problems mentioned above, in this paper, we propose a visual security assessment via saliency-weighted structure and orientation similarity. Structure is the basic element that conveys important visual information, and selective encryption can cause obvious structure changes of an image [21]. Therefore, we can measure the visual security of selective encrypted images by the change of structure. The gradient magnitude (GM) and the phase congruence [27] (PC) are widely used to extract the image structure information. However, GM and PC cannot effectively reflect the structure degradation in the selective encryption images. GM is sensitive to luminance and it can well reflect the changes of image luminance [28]. However, this characteristic of GM also makes it is not effective to extract the structure information of the areas with similar grayscale values. Compared with GM, PC is not affected by luminance [27]. However, PC cannot extract the clear structure information of the areas with similar frequencies as it is calculated based on frequency [27]. Therefore, we integrated PC with GM to obtain the structure features of the selective encrypted images. Studies show that HVS is highly adapted to extract orientation information [29] and selective encryption can cause obvious orientation changes of an image. Therefore, we can extract the orientation information of a selective encrypted image to measure its security. The structure and the orientation feature maps are extracted from both original and selective encrypted images. Finally, an image saliency-based pooling strategy is introduced to combine these measurements and generate a visual security score. Our main contributions can be summarized as follows:

(1) We propose to extract the structure and orientation features for the visual security evaluation of the selective encrypted images, because selective encryption can cause obvious changes in structure and orientation of an image and the HVS is highly sensitive to the change of structure and orientation. We combine GM and PC to extract the structure information to measure the structure similarity of original images and selective encrypted images and utilize the change of image orientation to measure the orientation similarity.

(2) Considering that different regions of an image have different effects on visual security assessment of selective encrypted images, we combine the saliency map with the structure and orientation similarity maps to generate the final VSA.

(3) We conduct comparative experiments on two common encryption image databases to evaluate the performance of our proposed VSA. The experimental results show that the proposed method achieves superior and robust performance compared with other state-of-the-art VSAs, especially on the images in low- and moderate-quality ranges.

The structure of the rest of the paper is as follows. Section 2 reviews the related work. The details of our proposed VSA method are in Section 3. Then, we describe the experimental evaluation of our proposed VSA and existing VSAs in Section 4. Finally, Section 5 concludes this paper.

2. Related Work

A variety of methods have been proposed to estimate the visual security of selective encrypted images. The initial solutions usually employ well-known IQAs to evaluate the

visual security. Subsequently, several VSAs have been proposed to evaluate the visual security.

2.1. Image Quality Assessment. Many researchers believe that the images with higher visual security tend to have lower visual quality, so many IQA methods designed for the assessment of image visual quality have been employed to measure the visual security of selective encrypted images. For instance, PSNR is the simplest and the most widely used method [30, 31]. PSNR, which evaluates visual security by calculating the Euclidean distance between the original image and distorted image, is the simplest and most popular visual quality assessment metric. SSIM [19] is also adopted for visual security evaluation [30, 31] by measuring the similarities of luminance, contrast, and structure between two images in consideration of the HVS. VIF [20] is another IQA method used to estimate the visual security of selective encrypted images. It measures the amount of information contained in original and selective encrypted images, respectively, and then measures the relationship between image information and visual quality. However, these IQA metrics often exhibit unsatisfactory performance when they are used to estimate the visual security of selective encrypted images of low quality. Since the task of IQA is inconsistent with that of VSA, an image with poor visual quality may not indicate its visual security [21].

For example, an image with a higher VIF, PSNR, or SSIM may even be more visually secure than one with a lower value of one of these indices. Figures 1(a)–1(c) show the performance of the PSNR, VIF, and SSIM indices on several images from the PEID database [33]. Figure 1(a) shows an original image, and Figures 1(b) and 1(c) show two encrypted images. It is clear that Figure 1(c) has a higher visual security, but this image is found to have better visual quality as assessed using the PSNR, VIF, and SSIM.

We can find that many IQAs cannot achieve excellent performance on visual security assessment because the targets of image quality assessment and visual security assessment are different: image quality assessment focuses on the fidelity of an image, but visual security assessment is concerned with the leakage degree of an image's content.

2.2. Visual Security Assessment. Several VSAs have been proposed to evaluate the visual security of selective encrypted images. They are usually more accurate and effective than IQA methods because they are specifically designed for the visual security evaluation of selective encrypted images. Mao and Wu [22] proposed the ESS and LSS to compute the edge similarity and the luminance similarity between original and selective encrypted images. However, the ESS and LSS focus only on local information of the images, which may not cover the various types of distortions that appear in selective encrypted images. Tong et al. [23] presented the LFBVS by considering various types of distortions present in selective encrypted images and measured the similarities of luminance and the localized gradient between original and selective encrypted images. Although the LFBVS utilizes more visual information compared with the ESS and LSS, its performance is still unsatisfactory when tested on various encrypted image databases. Xiang et al. [21] proposed the VSI-Canny by calculating the edge and texture similarities between original and selective encrypted images. VSI-Canny considers more visual features of selective encrypted images and has relatively good performance, but it does not consider the image's visual saliency, which is a critical property of the HVS.

For example, Figures 1(d)–1(f) illustrate the performance of different VSA indices on an image from the IVC-SelectEncrypt database. Figure 1(d) shows the original image, and two encrypted versions of which are shown in Figures 1(e) and 1(f). It is clear that Figure 1(f) is more visually secure than Figure 1(e). However, Figure 1(f) has higher LSS and VSI-Canny values than Figure 1(e).

As mentioned above, the problems of the existing visual security metrics exhibit many aspects. These questions will lead to the inaccurate evaluation of image security by visual security indicators. We consider and address these issues in our proposed scheme, as described in the following section.

3. Proposed Visual Security Assessment

In this work, we describe our proposed VSA and the flowchart of the proposed VSA is shown in Figure 2. First, we combine GM and PC to extract the structure information and we can compute the structure similarity map of the original and selective encrypted image. Secondly, based on the fact that the HVS is sensitive to the change of orientation, we extract the orientation information by the GM and we can compute the orientation similarity map. Next, considering that the security of a selective encrypted image depends on the degree of disclosure of its visual content, which is obtained by comparing it with the original image, we only compute the saliency map of the original image. At last, the generated structure and orientation similarity maps are further fused by saliency-based polling method to obtain the final score.

3.1. Structure Similarity. The structure of an image has important information which is highly sensitive to the visual perception. Both GM and PC can extract structural information of images and we found that they can complement each other. Therefore, we integrated the GM map with the PC map to generate the structure features of selective encrypted images.

3.1.1. Gradient Magnitude. Image gradient magnitude can be defined as a transition in intensity. The GM of an image is represented by a vector which consists of gradient in the horizontal and vertical directions at each pixel, and it reflects the maximum strength of structure variation. The gradient magnitude of an image is defined as

$$\mathrm{GM}(i, j) = \sqrt{G_h^2(i, j) + G_v^2(i, j)}, \tag{1}$$

where (i, j) is the index of an image I. In this work, for image I, G_h and G_v are calculated as

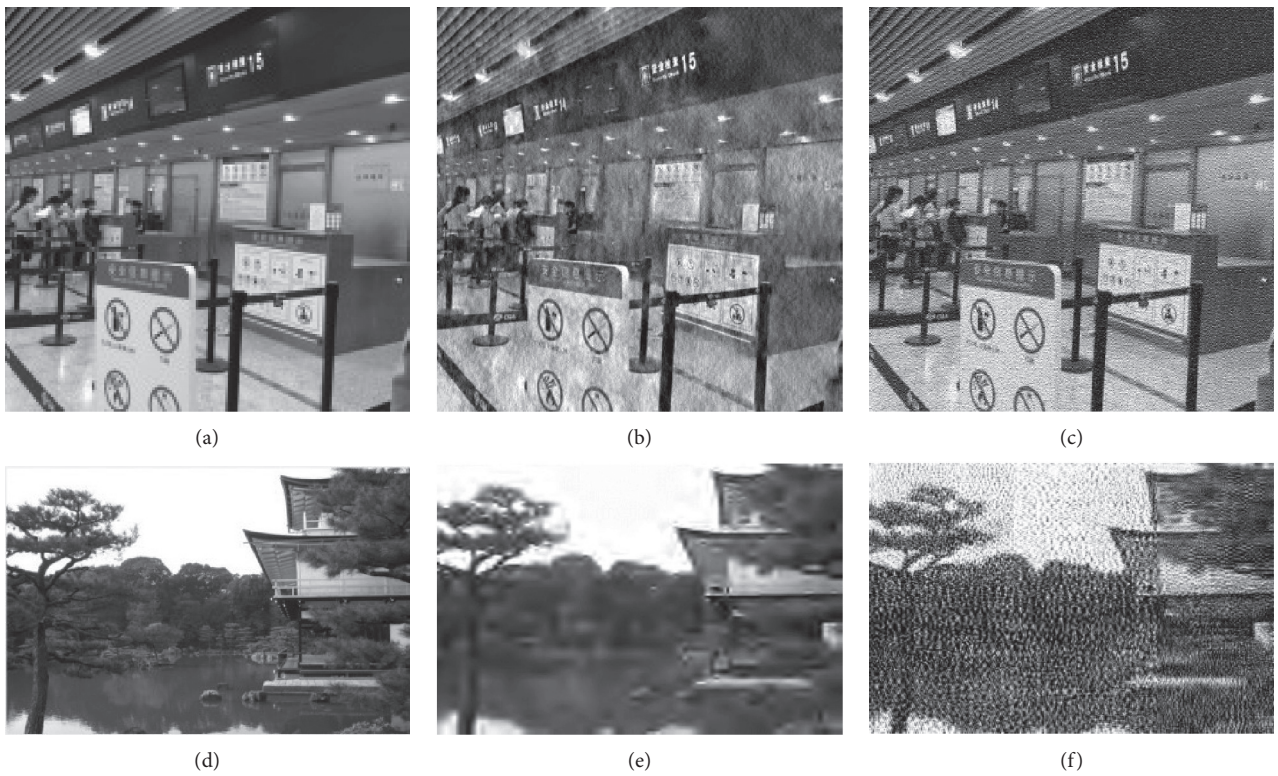


Figure 1: The performances of IQAs on images from the IVC-SelectEncrypt database [32] and PEID [33] database. (a) Original image from the PEID database. (b) Encrypted image with PSNR = 14.5 and SSIM = 0.19. (c) Encrypted image with PSNR = 20.3 and SSIM = 0.51. (d) Original image from the IVC-SelectEncrypt database. (e) Encrypted image with LSS = −0.007 and VSI-Canny = 0.0752. (f) Encrypted image with LSS = −0.02 and VSI-Canny = 0.1893.

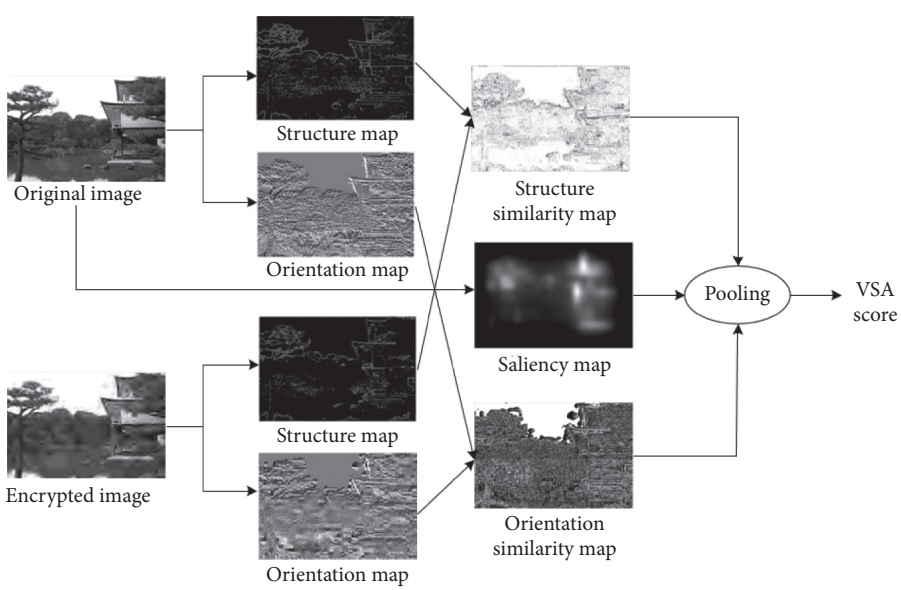


Figure 2: Flowchart illustration of the proposed security model for selective encrypted images.

$$G_h = F * I,$$
$$G_v = F^T * I, \tag{2}$$

where $*$ and T denote the convolution and transpose, respectively, and F is the gradient operator:

$$F = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix}. \tag{3}$$

As shown in Figure 3(b), it can be seen that the GM maps of the encrypted images have obvious changes. However, there are no obvious changes in the GM values in some areas with similar grayscale values. GM is sensitive to luminance; therefore, it can well reflect the changes of image luminance [28]. However, this characteristic of GM also makes it is not effective to extract the structure information of the areas with similar grayscale values.

3.1.2. Phase Congruency. The phase congruency model [27], which is based on frequency domain processing of an image, means that features with similar edges appear more frequently at the same stage. It assumes that the visual system is more competent in performing operations using the phase and amplitude of the individual frequency components in an image than handing of image information spatially. Compared with GM, PC is invariant to local smooth luminance changes. Given an image I, its PC is computed as

$$PC(i,j) = \frac{\sum_s \sum_\theta W(i,j) \lfloor A_{s\theta}(i,j) \cdot \Delta\varphi_{s\theta}(i,j) - T \rfloor}{\sum_s \sum_\theta A_{s\theta}(i,j) + \varepsilon}, \tag{4}$$

with

$$\begin{aligned} \Delta\varphi_{s\theta}(i,j) &= \cos\left(\varphi_{s\theta}(i,j) - \bar{\varphi}_{s\theta}(i,j)\right) - \left|\sin\left(\varphi_{s\theta}(i,j) - \bar{\varphi}_{s\theta}(i,j)\right)\right|, \\ W(i,j) &= \frac{1}{1 + e^{\gamma(c - v(i,j))}}, \\ A_{s\theta} &= \sqrt{E_{s\theta}^2(i,j) + O_{s\theta}^2(i,j)}, \\ \varphi_{s\theta}(i,j) &= a\tan\left(E_{s\theta}(i,j), O_{s\theta}(i,j)\right), \\ \left[E_{s\theta}(i,j), O_{s\theta}(i,j)\right] &= \left[I(i,j) * M_{s\theta}^E, I(i,j) * M_{s\theta}^O\right], \end{aligned} \tag{5}$$

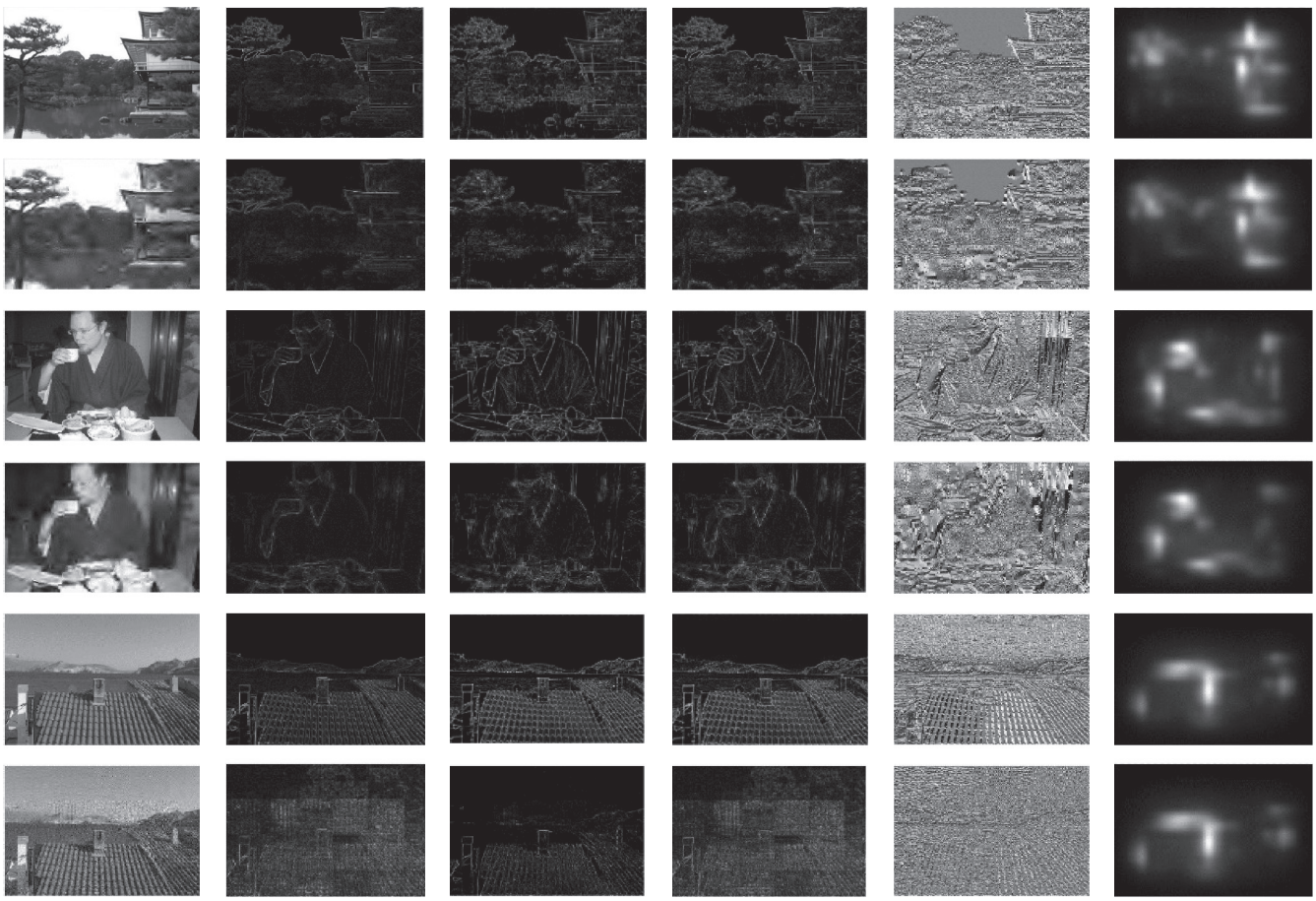
where $W(i,j)$ denotes the weighting parameter to reduce the effect of frequency spread at position (i, j); $v(i,j) = (1/N)\sum_s \sum_\theta A_{s\theta}(i,j)(A_{\max}(i,j) + l_{\text{norm}}(i,j))^{-1}$ denotes the manipulating function by weighting; N is the scale number; c offers a cutoff value for penalizing low PC values under it; $l_{\text{norm}}(i,j)$is the normalized luminance at (i, j) to avoid the effect of luminance. γ, as the gain variable, controls the cutoff sharpness; and symbol $\lfloor \cdot \rfloor$ aims to set negative value to zero. To determine two-dimensional phase congruency of a given image, the image is first convoluted with a Log-Gabor filters bank s and θ are the scale and orientation of the Log-Gabor filter. And the even symmetric filter and odd-symmetric filter at scale s and orientation θ are $M_{s\theta}^E$ and $M_{s\theta}^O$, respectively. $A_{s\theta}(i,j)$ and $\varphi_{s\theta}(i,j)$ represent the amplitude and phase at position (i, j), respectively; T is a quantity introduced to compensate image noise; ε is a small positive constant to preserve stability; $\overline{\varphi_{s\theta}}(i,j)$represents the mean value of phase. Since it is out of scope to investigate these parameters' influence on the PC map, in this study, we directly set them according to [27].

The effectiveness of PC can be demonstrated in Figure 3(c), and the PC maps of the encrypted images have obvious changes. However, there are no obvious changes in the PC values in some areas with similar frequencies. Compared with GM, PC is not affected by luminance [27]. However, PC cannot extract the clear structure information of the areas with similar frequencies as it is calculated based on frequency [28].

3.1.3. Structure Map Integrating GM with PC. As mentioned above, GM and PC cannot effectively reflect the structure degradation in the selective encryption images. Therefore, after extracting the GM and PC of the image, we proposed to reflect the structure map of the image by integrating GM with PC, and the structure information ST of the image can be obtained as

$$\text{ST}(i,j) = \max\left\{\frac{\text{GM}(i,j)}{\text{GM}_{\max}}, \text{PC}(i,j)\right\}, \tag{6}$$

where (i, j) is the index of the pixel, $\text{GM}_{\max}$ represents the maximum value of GM, the maximum value of the corresponding positions of GM and PC is used to form ST, and GM uses the maximum value for normalization. If one of the two values has a larger value, the pixel is considered to be a structural feature point, and the maximum fusion strategy



(a) (b) (c) (d) (e) (f)

Figure 3: Illustrations of different feature maps. (a) First column is the input images. (b) Second column is the GM maps of the images in (a). (c) Third column is the PC maps of the images in (a). (d) Fourth column is the ST maps of the images in (a). (e) Fifth column is the orientation maps of the images in (a). (f) Sixth column is the saliency maps of the images in (a). And the images in second, fourth, and sixth rows in (a) are the encrypted images of first, third, and fifth rows in (a), respectively.

can comprehensively extract the structural features of the image. GM and PC can play complementary roles in extracting structural information. Here, we give an example in Figure 3 to demonstrate the effectiveness of our structure extraction method. Figure 3 shows different feature maps from the reference images and their selective encrypted images. Apparently, as compared with the other feature map, the proposed structure map has a remarkable effect on structure degradation of a selective encrypted image. From Figure 3(d), we can observe the more accurate and clearer structure information in the selective encrypted image.

Analogous to the practice exercised in [19, 34], the structure similarity map S_{ST} of the original and the encrypted images can be measured as

$$S_{ST}(i, j) = \frac{2 \cdot ST_O(i, j) \cdot ST_E(i, j) + R}{ST_O(i, j)^2 \cdot ST_E(i, j)^2 + R}, \tag{7}$$

where $S_{ST}(i, j) \varepsilon (0, 1]$, $S_O(i, j)$ and $S_E(i, j)$ are the structure maps of the original image O and the encrypted image E, respectively, and R is a positive constant used to avoid instability when the denominator converges to zero.

3.2. Orientation Similarity. In addition to the structure similarity, we also consider the orientation similarity between the original and encrypted images because the orientation information is an indispensable element for human visual perception. The orientation of an image, which has been widely used to the image quality assessment [35], conveys important information [29], which has an important effect on the visual security evaluation of selective encrypted images. The orientation change of each pixel can reflect the degradation of the selective encrypted image details.

A visual pattern was built by orientation information in [35], which can be used for IQA. However, this pattern ignores some intuitive visual information; therefore, this pattern does not fully apply to VSA.

Considering the above question, we design a new algorithm to compute the orientation similarity. In this work, for an image I, the preferred orientation of each pixel is calculated as its gradient direction θ_I:

$$\theta_I(i, j) = \arctan\left(\frac{G_v(i, j)}{G_h(i, j)}\right) \cdot \frac{180}{\pi}, \tag{8}$$

where $G_h(i, j)$ and $G_v(i, j)$ are the gradient magnitudes along the horizontal and vertical directions, respectively, which can be obtained from equation (2). And (i, j) is the index of the pixel in I. So, we can obtain the quantitative orientation information. We give an example in Figure 3, and we can find that the orientation information of the image has obvious changes.

Then, we compute the orientation change D_O of the original image O and its encrypted image E by calculating their distance:

$$D_O(i, j) = \left|\theta_O(i, j) - \theta_E(i, j)\right|, \tag{9}$$

where $|.|$ denotes the absolute operation, (i, j) is the index of the pixel, and θ_O and θ_E are the orientation maps of the original image O and its encrypted image E, respectively.

Because the range of θ_O and θ_E is $[-180, 180]$, the range of D_O is $[0, 360]$. Considering that HVS has a similar perception of relative orientation (such as 90° and 270°), we set the range of D_O to $[0, 180]$ by setting $D_O\ (D_O > 180) = 360 - D_O\ (D_O > 180)$.

Then, the orientation similarity map S_O of the original and the encrypted images can be measured as

$$S_O(i, j) = 1 + \frac{\log_2 D_O(i, j)}{\log_2(1/180)}. \tag{10}$$

3.3. Saliency-Weighted Pooling. It is observed that different regions have drastically different effects on the visual understanding of an image. Most of the contribution to visual perception is provided by the information loss and distortion in important regions. An image importance map refers to the important regions that provide a greater contribution to the visual perception, and such maps have been studied extensively in recent years. So, we highlight these important regions and suppress the other regions with a salient map for visual content extraction. To this end, the salient value of each pixel is required. As illustrated in Figure 3(f), visual saliency map highlights the important regions in an image, and the visual saliency map can extract the important areas of an image and then get a better VSA. In the past decades, a large number of saliency models [36–40] have been proposed and these models can help us complete a better VSA.

$S_{ST}(i, j)$ and $S_O(i, j)$, obtained by equations (7) and (10), respectively, are two feature similarity maps with the same size as the image. However, we need a VSA score to represent the visual security. Therefore, we need a pooling method to compress the two feature maps into two scores to represent the feature similarities. In our work, we take the simple and classic saliency-weighted pooling method. Considering that the security of a selective encrypted image depends on the degree of disclosure of its visual content, which is obtained by comparing it with the original image. So, we select the original image's saliency map $SM_O(i, j)$ to combine with the structure similarity map $S_{ST}(i, j)$ and orientation similarity map $S_O(i, j)$, respectively:

$$\begin{aligned} \mathrm{VS}_{ST} &= \frac{\sum_{(i,j)} S_{ST}(i, j) \cdot \mathrm{SM}_O(i, j)}{\sum_{(i,j)} \mathrm{SM}_O(i, j)}, \\ \mathrm{VS}_O &= \frac{\sum_{(i,j)} S_O(i, j) \cdot \mathrm{SM}_O(i, j)}{\sum_{(i,j)} \mathrm{SM}_O(i, j)}. \end{aligned} \tag{11}$$

Considering that different saliency models affect the performance and communicational cost of our proposed VSA, we calculate the performance and running time of different saliency models. To eliminate the possible bias due to specific image selection, we randomly choose 100 images from the IVC-SelectEncrypt database and then calculate the average running time as the computation cost of each saliency model. Table 1 shows the results. From Table 1, we can find that the more appropriate saliency model is GBVS. Therefore, as a simple but powerful saliency model, graph-based visual saliency [36] (GBVS) is employed. A saliency map of an original image generated by GBVS can be seen in Figure 3(f).

After performing the similarity measurements on the structure and the orientation features between the original and encrypted images, respectively, the generated structure similarity VS_{ST} and orientation similarity VS_O are combined together to calculate the visual security:

$$\mathrm{VSA} = \alpha \cdot \mathrm{VS}_{ST} + \beta \cdot \mathrm{VS}_O, \tag{12}$$

where α and β are two parameters used to adjust the relative importance of VS_{ST} and VS_O. The structure and orientation features of an image are important which are highly sensitive to the visual perception. For selective encrypted images, an important feature is that the skeleton of the image is still intelligible but the details are almost unintelligible. Therefore, structure obviously plays a more important role than orientation, and we explore the effect of the structure information and orientation information, respectively, in Table 2. So that the value of α should be greater than β. In our experiments, α and β are set to 0.8 and 0.2, respectively, because this setting was found to be optimal.

4. Experiments

In this section, the performance of our proposed VSA is analyzed by comparing with other IQAs and VSAs. We evaluate the performance from confidence, monotonicity, linearity, and accuracy and provide comparisons with other IQAs and VSAs.

4.1. Experimental Protocol

4.1.1. Test Database. To verify the performance of our proposed method, experiments are conducted on two common encrypted databases: IVC-SelectEncrypt [32] and PEID [33].

The IVC-SelectEncrypt can be downloaded from http://www.polytech.univ-nantes.fr/autrusseau-f/Databases/SelectiveEncryption/. The PEID is from https://sites.google.com/site/xiangtaooo/. Their detailed statistical information is summarized in Table 3.

Table 1: Performance comparison employing different saliency models: graph-based visual saliency (GBVS), context-aware visual saliency (CAVS), saliency estimation using region covariance (CovSal), saliency through adaptive whitening of color and scale features (AWS), and Boolean map saliency (BMS).

Metric	PLCC	SRCC	KRCC	RMSE	Time(s)
Without saliency	0.943	0.935	0.769	0.435	**0.356**
GBVS [36]	**0.956**	**0.954**	**0.815**	**0.388**	**0.476**
CAVS [37]	**0.958**	**0.956**	**0.815**	**0.386**	21.43
CovSal [38]	0.949	0.943	0.809	0.395	1.256
AWS [39]	0.953	0.947	0.817	0.396	0.789
BMS [40]	0.951	0.948	0.813	0.401	6.579

Table 2: Performance of structure similarity VS_{ST}, orientation similarity VS_O, and final VSA.

Metric	PLCC	SRCC	KRCC	RMSE
VS_{ST}	0.951	0.947	0.833	0.398
VS_O	0.943	0.939	0.802	0.418
VSA	**0.958**	**0.956**	**0.815**	**0.386**

Table 3: Statistical information of the test databases.

Database	IVC-SelectEncrypt	PEID
Reference image	8	20
Encrypted image	200	1080
Encryption type	5	10
Subjective score	MOS	MOS
Score range	[1, 5]	[0, 6]
Low quality	[1, 2.5]	[0, 2]
Moderate quality	(2.5, 3.5]	(2, 4]
High quality	(3.5, 5]	(4, 6]

The IVC-SelectEncrypt database consists of 8 original images, 200 encrypted images are generated from them using 5 different encrypted algorithms with 5 different encryption degrees. The range of its mean opinion scores (MOS) is [1, 5].

The PEID database has 1080 encrypted images obtained from 20 original images by using 10 encryption schemes. It has two subjective scores: the visual quality score and visual security score. We use only the visual security score here because our task is visual security assessment, and the range of its mean opinion scores (MOS) is [0, 6].

4.1.2. Evaluation Methodology. We evaluate the performance from confidence, monotonicity, linearity, and accuracy.

Confidence is utilized to establish how well a VSA actually reflects the human judgment [17]. Given a subjective score $x(x \varepsilon \text{MOS})$ on a database D, and for this score x, each image I has a subjective score V_I. We define $V_{\max}(x)$ as the maximum of the objective scores of those images on D and define $V_{\min}(x)$ as the minimum of the objective scores. Confidence $C_x = |V_{\max}(x) - V_{\min}(x)|$ measures the difference between these two extrema. The normalized mean confidence μ_D, the normalized standard deviation σ_D, and the normalized maximum confidence $\max_D$ are the evaluation criteria which are generated based on C_x.

To ascertain the correlation between the subject VSA scores and object scores MOS, we compute the Spearman rank correlation coefficient (SRCC), the Kendall rank correlation coefficient (KRCC), the Person linear correlation coefficient (PLCC), and the root mean-squared error (RMSE). SRCC and KRCC can evaluate performance monotonicity, PLCC can evaluate linearity, and RMSE can evaluate accuracy. Before the calculation of the correlation between the subject VSA scores and object scores MOS, a five-parameter logistic regression function is applied to reduce the nonlinearity of the subject VSA scores [33], which is defined as

$$S' = \beta_1\left(\frac{1}{2} - \frac{1}{e^{\beta_2(S-\beta_3)}}\right) + \beta_4 S + \beta_5, \tag{13}$$

where S' is the fitted VSA score, S is the objective VSA score, and β_i $(i = 1, 2, 3, 4, 5)$ denotes the parameters determined via curve fitting.

A better VSA should have lower μ_D, σ_D, $\max_D$, and RMSE values but have higher SRCC, KRCC, and PLCC values.

4.2. Comparative Analysis. We compare our proposed VSA with other IQAs and VSAs by the evaluation criterions mentioned above from the following three aspects. And these IQAs and VSAs include the PSNR, SSIM [19], VIF [20], ESS [22], LSS [22], LFBVS [23], and VSI-Canny [21].

4.2.1. Overall Evaluation. The results of the confidence evaluation of all IQAs and VSAs on the IVC-SelectEncrypt database are shown in Figure 4. A better VSA should have lower and more stable C_x values. From Figure 4, we can find that the C_x values of VIF, VSI-Canny, and our VSA are more stable.

Table 4 lists the overall performance of all IQAs and VSAs on the IVC-SelectEncrypt and PEID databases, and the best is marked in bold. Obviously, our proposed VSA performs best on IVC-SelectEncrypt. On the PEID database, VIF achieves the best monotonicity (the highest SRCC and KRCC) and the lowest RMSE, LSS has the lowest σ_D, ESS achieves the lowest $\max_D$, and our proposed VSA achieves the best μ_D and PLCC. Although our proposed VSA is not the best in some values, it is very close to the best one. Compared with other methods, the extracted structure and orientation features of our proposed VSA are more consistent with HVS because HVS is very sensitive to structure and orientation changes caused by selective encryption. In addition, we also considered the visual saliency that was not considered by other IQAs and VSAs. Therefore, it is clear and reasonable that our proposed VSA exhibits the better overall performance.

4.2.2. Evaluation on Different Quality Ranges. The selective encrypted images usually have low and moderate visual quality [21, 26]. Therefore, to evaluate the performance of these VSAs more comprehensively, we should evaluate the performance of these VSAs on different image quality ranges (i.e., low, moderate, and high). The detailed division information can be found in Table 2. Considering that the

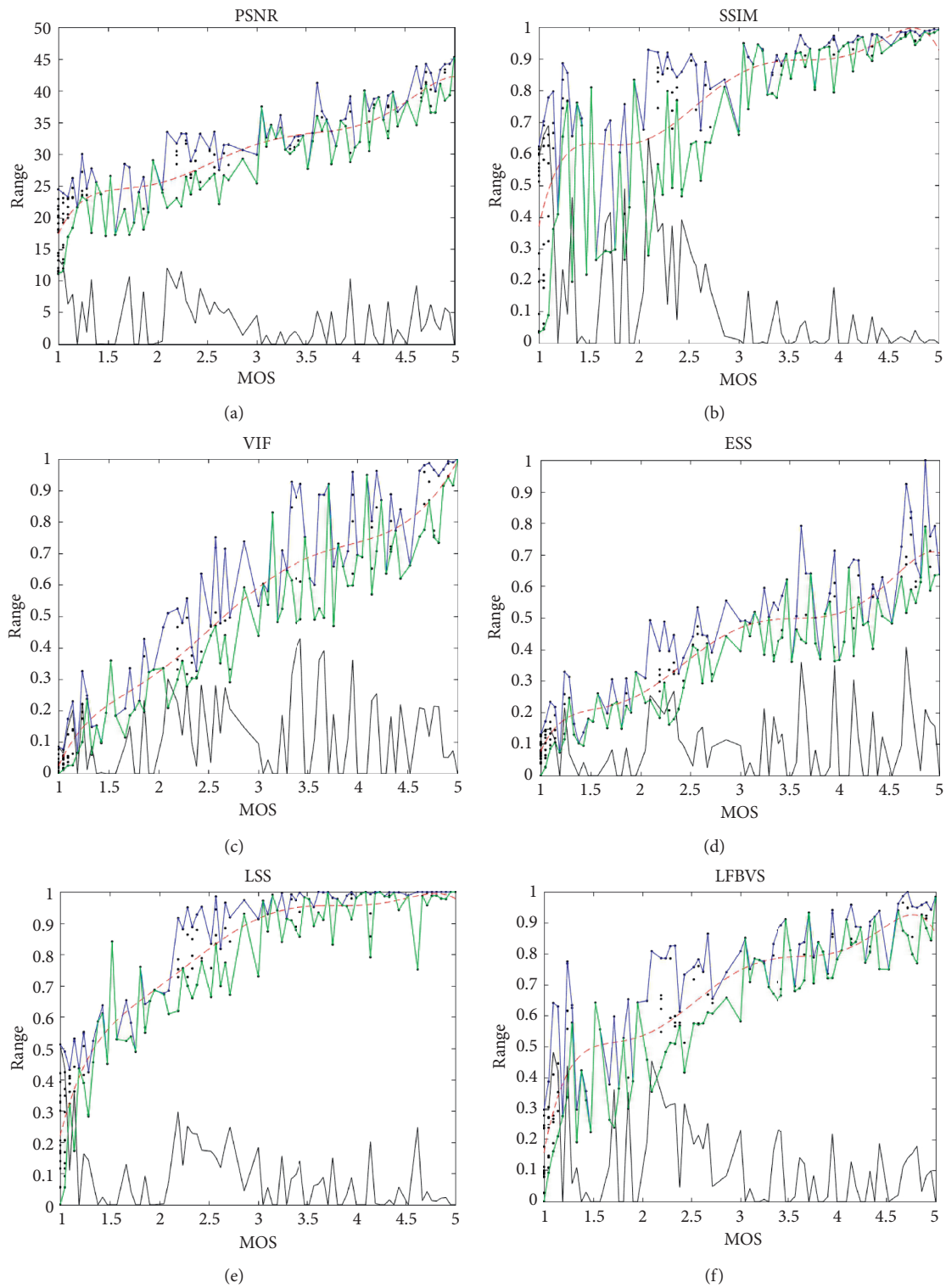
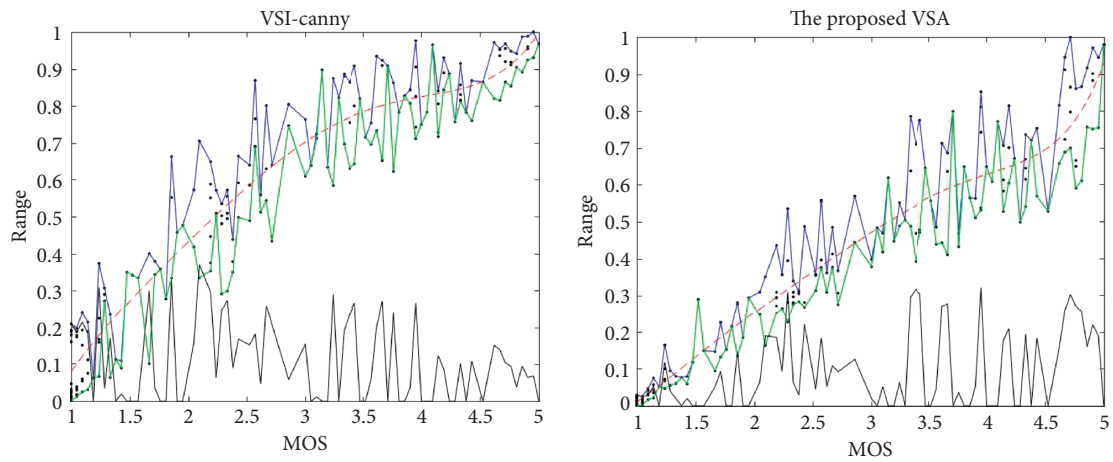


Figure 4: Continued.



(g) (h)

Figure 4: Confidence evaluation of all the VSAs on the IVC-SelectEncrypt database, where the pairs of the MOS values and the objective scores are plotted as black dots. The nonlinear fitting results are plotted as red dashed lines, and $V_{\max}(x)$, $V_{\min}(x)$, and C_x are plotted as blue, green, and black solid lines, respectively. (a) PSNR. (b) SSIM. (c) VIF. (d) LSS. (e) ESS. (f) LFBVS. (g) VSI-Canny. (h) The proposed VSA.

Table 4: Overall performance comparison on different databases.

Database	Evaluation	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-Canny	Proposed
IVC-SelectEncrypt	μ_D	0.156	0.122	0.170	0.222	0.343	0.254	0.154	**0.098**
	σ_D	0.101	0.184	0.101	0.188	0.188	0.174	**0.089**	0.099
	$\max_D$	0.394	0.689	0.404	0.520	0.399	0.479	0.353	**0.343**
	PLCC	0.915	0.891	0.939	0.919	0.901	0.891	0.942	**0.956**
	SRCC	0.911	0.869	0.939	0.932	0.909	0.891	0.935	**0.954**
	KRCC	0.743	0.702	0.791	0.786	0.747	0.712	0.776	**0.815**
	RMSE	0.543	0.645	0.455	0.658	0.506	0.601	0.446	**0.388**
PEID	μ_D	0.189	0.431	0.169	0.098	0.158	0.116	0.333	**0.096**
	σ_D	0.144	0.239	0.077	**0.044**	0.137	0.105	0.210	0.059
	$\max_D$	0.538	0.853	0.534	0.771	**0.479**	0.530	0.882	0.774
	PLCC	0.825	0.845	0.854	0823	0.808	0.724	0.850	**0.886**
	SRCC	0.796	0.831	**0.910**	0.796	0.772	0.618	0.726	0.870
	KRCC	0.616	0.657	**0.768**	0.616	0.592	0.458	0.557	0.691
	RMSE	1.056	0.999	**0.645**	1.061	1.065	1.248	0.984	0.866

selective encrypted images are typically in the low- or moderate-quality ranges, it is more important to evaluate the performance of VSAs in the low and moderate image quality ranges than in the high-quality ranges [21, 26].

The comparison results of different VSAs in different image quality ranges on the two test databases are shown in Table 5. We can find that our proposed VSA has better performance compared with the other VSAs in the low and moderate image quality ranges. In the low image quality range, on the IVC-SelectEncrypt database, VIF shows superior performance in $\max_D$, LSS shows the best performance on PLCC, SRCC, KRCC, and RMSE, our proposed VSA achieves the best value on μ_D and σ_D, and other values are very close to the best one. On the PEID database, VIF shows superior performance in confidence evaluation (lowest μ_D, σ_D, and $\max_D$), and our proposed VSA achieves the best performance on PLCC, SRCC, KRCC, and RMSE. In the moderate image quality range, our proposed VSA achieves the best performance on monotonicity, linearity, and accuracy evaluation on the two databases. In the high image quality range, SSIM obtains the best performance on IVC-SelectEncrypt database; on the PEID database, various VSAs exhibit satisfactory performance in different aspects. In summary, our proposed VSA exhibits better performance in low and moderate image quality ranges on the two databases. In the low and moderate image quality ranges, the structure and orientation changes caused by selective encryption are more obvious. And the saliency of the original image can extract the more important areas of the images which is important for the visual security assessment of the selective encrypted images. Therefore, it is rational that our proposed VSA shows the better performance in low and moderate image quality ranges.

4.2.3. Evaluation on Different Encryption Types. We also evaluated the different VSAs on various types of encryption on the two test databases to more comprehensively evaluate

Table 5: Overall performance comparison on different ranges.

	Database	Evaluation	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-Canny	Proposed
IVC-SelectEncrypt	Low	μ_D	0.216	0.367	0.283	0.311	0.218	0.179	0.183	**0.155**
		σ_D	0.112	0.199	0.137	0.211	0.307	0.256	0.099	**0.092**
		$\max_D$	0.394	0.689	**0.283**	0.876	0.312	0.479	0.353	0.306
		PLCC	0.684	0.680	0.900	**0.935**	0.760	0.586	0.900	0.912
		SRCC	0.703	0.528	0.889	**0.902**	0.673	0.662	0.826	0.899
		KRCC	0.524	0.389	0.711	**0.746**	0.582	0.479	0.635	0.733
		RMSE	0.381	0.384	0.228	**0.185**	0.574	0.620	0.228	0.246
	Moderate	μ_D	**0.129**	0.168	0.222	0.290	0.136	0.141	0.183	0.154
		σ_D	0.174	0.125	0.138	0.116	0.258	0.273	**0.090**	0.094
		$\max_D$	**0.255**	0.393	0.404	0.423	0.376	0.312	0.277	0.306
		PLCC	0.514	0.474	0.583	0.503	0.602	0.388	0.503	**0.713**
		SRCC	0.531	0.348	0.521	0.495	0.577	0.321	0.473	**0.629**
		KRCC	0.367	0.244	0.367	0.345	0.324	0.253	0.324	**0.422**
		RMSE	0.286	0.294	0.271	0.289	0.602	0.639	0.288	**0.234**
	High	μ_D	0.130	**0.038**	0.186	0.114	0.220	0.198	0.119	0.164
		σ_D	0.076	**0.044**	0.093	0.117	0.331	0.277	0.068	0.080
		$\max_D$	0.301	**0.178**	0.368	0.424	0.399	0.309	0.259	0.334
		PLCC	0.694	**0.740**	0.596	0.253	0.588	0.646	0.605	0.650
		SRCC	0.694	**0.732**	0.606	0.494	0.599	0.646	0.606	0.638
		KRCC	0.520	**0.558**	0.445	0.360	0.442	0.466	0.437	0.469
		RMSE	0.316	**0.295**	0.353	0.425	0.564	0.549	0.352	0.333
PEID	Low	μ_D	0.152	0.300	**0.030**	0.389	0.170	0.049	0.197	0.097
		σ_D	0.170	0.159	**0.019**	0.152	0.095	0.039	0.105	0.041
		$\max_D$	0.527	0.716	**0.142**	0.753	0.376	0.283	0.643	0.225
		PLCC	0.593	0.577	0.793	0.641	0.573	0.315	0.432	**0.804**
		SRCC	0.574	0.617	0.698	0.531	0.484	0.287	0.196	**0.711**
		KRCC	0.405	0.452	0.532	0.380	0.355	0.204	0.135	**0.533**
		RMSE	0.534	0.542	0.449	0.510	0.573	0.619	0.599	**0.403**
	Moderate	μ_D	0.187	0.527	**0.091**	0.432	0.398	0.116	0.441	0.290
		σ_D	0.145	0.161	0.054	0.192	0.195	**0.038**	0.161	0.127
		$\max_D$	0.499	0.850	0.387	0.771	0.394	**0.276**	0.725	0.565
		PLCC	0.355	0.407	0.617	0.295	0.387	0.376	0.474	**0.623**
		SRCC	0.320	0.368	**0.604**	0.418	0.289	0.257	0.475	0.601
		KRCC	0.221	0.256	0.418	0.288	0.198	0.170	0.333	**0.430**
		RMSE	0.531	0.519	0.503	0.543	0.534	0.539	**0.500**	0.519
	High	μ_D	0.210	0.511	**0.159**	0.295	0.278	0.286	0.393	0.317
		σ_D	0.172	0.321	**0.133**	0.180	0.163	0.172	0.264	0.198
		$\max_D$	0.538	0.853	0.534	0.628	**0.479**	0.530	0.882	0.774
		PLCC	0.850	0.849	0.838	0.518	0.840	0.693	**0.860**	0.480
		SRCC	0.795	0.781	0.785	0.632	0.766	0.629	**0.820**	0.459
		KRCC	0.608	0.593	0.584	0.466	0.568	0.433	**0.639**	0.321
		RMSE	0.473	0.329	0.312	0.532	**0.310**	0.412	0.317	0.498

the performance of all VSAs. There are 15 different encryption types in the test on the two databases. Tables 6 and 7 report the performance results of all encryption types that appear in the test databases, respectively.

From Table 6, we can find that our proposed VSA has better monotonicity performance (the higher SRCC and KRCC values) than other IQAs and VSAs on the two databases. More specifically, our proposed VSA achieves the highest SRCC hit-count (8 times) and KRCC hit-count (7 times), and this value is higher than those of the other metrics. We can also find that our proposed VSA still has the highest PLCC hit-count (7 times) and RMSE hit-count (7 times) from Table 7.

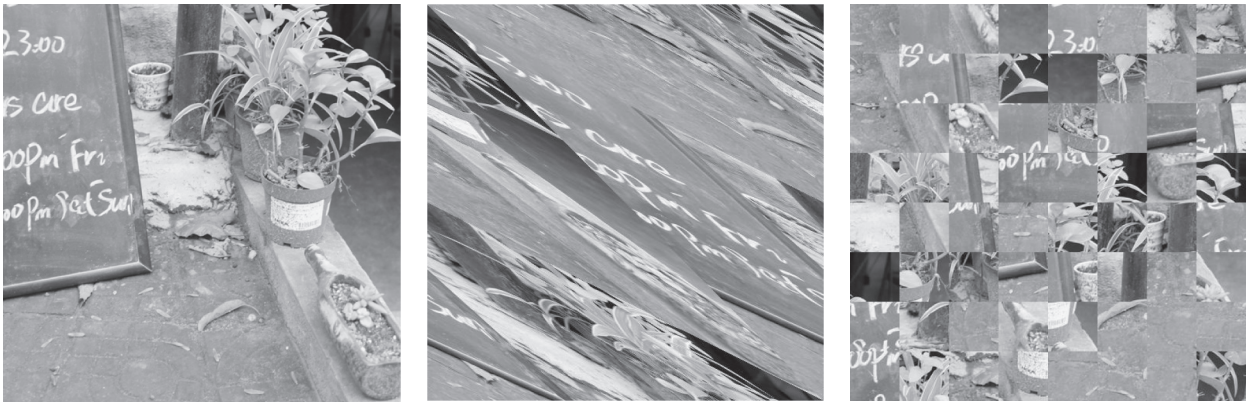
From Tables 6 and 7, we can see that all of the involved VSAs obtain relatively inferior performance on encryption types enc08 and enc09 in the PEID database, and our proposed VSA is still relatively great on enc09 but relatively poor on enc08. As shown in Figure 5, the distortions caused by these two encryption methods are different from other methods that they make the images warping. Therefore, the features extracted from these encrypted images cannot match the features of the original images and these VSAs and IQAs have not good performance on the two encryption methods. This situation also results the overall performance of our method at PEID being worse than IVC-SelectEncrypt. Except for enc08 and enc09, other encryption methods cause

Table 6: Overall performance comparison (SRCC and KRCC) on different encryptions.

		SRCC								KRCC							
Database	Metric	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-Canny	Proposed	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-Canny	Proposed
IVC-SelectEncrypt	trad	0.965	**0.968**	0.964	0.948	0.933	0.960	0.951	**0.968**	0.864	**0.864**	0.854	0.820	0.799	0.852	0.818	0.854
	trunc	0.888	0.879	**0.953**	0.948	0.913	0.907	0.953	0.921	0.731	0.710	0.803	**0.829**	0.801	0.798	0.826	0.764
	iwind_ec	0.909	0.924	0.941	0.887	0.859	0.886	0.927	**0.965**	0.738	0.766	0.800	0.751	0.724	0.753	0.779	**0.811**
	iwind_nec	0.910	0.953	0.951	0.907	0.946	0.946	0.934	**0.953**	0.770	0.837	0.829	0.820	0.827	0.822	0.798	**0.837**
	res	0.915	0.886	**0.955**	0.955	0.926	0.916	0.944	**0.960**	0.778	0.717	0.839	**0.842**	0.787	0.765	0.825	**0.846**
PEID	enc01	0.906	0.927	0.897	**0.951**	0.540	0.452	0.864	0.937	0.735	0.774	0.759	**0.807**	0.473	0.386	0.709	0.759
	enc02	0.951	0.911	**0.963**	0.835	0.846	0.627	0.887	0.938	**0.809**	0.760	0.785	0.650	0.668	0.453	0.711	0.764
	enc03	0.923	0.898	0.977	0.944	0.966	0.862	0.975	**0.978**	0.749	0.741	0.825	0.795	0.813	0.724	0.872	**0.873**
	enc04	0.911	0.916	0.916	0.908	0.828	0.907	0.738	**0.962**	0.742	0.750	0.741	0.736	0.694	0.713	0.538	**0.769**
	enc05	0.929	0.936	0.940	0.924	0.789	0.821	0.927	**0.946**	0.774	0.790	0.783	0.767	0.613	0.689	0.783	**0.830**
	enc06	0.970	0.965	0.972	0.968	0.961	0.914	0.972	**0.976**	0.847	0.833	0.852	0.845	0.844	0.825	0.853	**0.853**
	enc07	0.956	0.977	**0.983**	0.958	0.975	0.959	0.982	0.971	0.805	0.869	**0.885**	0.818	0.876	0.859	0.884	0.862
	enc08	0.083	0.666	0.191	0.200	0.325	0.360	**0.710**	0.246	0.066	0.528	0.144	0.145	0.256	0.259	**0.558**	0.184
	enc09	0.235	**0.760**	0.582	0.187	0.364	0.339	0.155	0.521	0.162	**0.582**	0.493	0.126	0.289	0.276	0.082	0.380
	enc10	0.760	0.943	**0.980**	0.631	0.846	0.678	0.632	0.930	0.589	0.807	**0.823**	0.473	0.723	0.649	0.468	0.788

Table 7: Overall performance comparison (PLCC and RMSE) on different encryptions.

		PLCC								RMSE							
Database	Metric	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-canny	Proposed	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-canny	Proposed
IVC-SelectEncrypt	trad	0.955	**0.969**	0.969	0.955	0.922	0.957	0.955	0.968	0.250	0.208	**0.207**	0.250	0.264	0.248	0.249	0.211
	trunc	0.916	0.907	**0.980**	0.970	0.946	0.949	0.974	0.958	0.510	0.536	**0.246**	0.308	0.316	0.293	0.287	0.365
	iwind_ec	0.957	0.981	0.983	0.941	0.916	0.967	0.982	**0.984**	0.434	0.280	0.264	0.483	0.512	0.491	0.274	**0.258**
	iwind_nec	0.931	0.965	0.960	0.907	0.924	0.948	0.950	**0.971**	0.435	**0.312**	0.334	0.502	0.493	0.375	0.370	**0.312**
	res	0.905	0.931	**0.978**	0.955	0.949	0.939	0.961	0.961	0.480	0.412	0.234	**0.211**	0.501	0.487	0.198	0.311
PEID	enc01	0.904	**0.957**	0.948	0.952	0.796	0.583	0.944	0.946	0.509	0.346	**0.328**	0.363	0.716	0.903	0.393	0.418
	enc02	0.967	0.950	**0.970**	0.888	0.861	0.636	0.888	0.939	0.424	0.516	**0.410**	0.760	0.749	0.856	0.762	0.517
	enc03	0.964	0.956	**0.985**	0.970	0.979	0.917	0.984	**0.985**	0.481	0.533	0.326	0.442	0.383	0.412	0.324	**0.312**
	enc04	0.940	0.928	0.950	0.939	0.816	0.911	0.883	**0.967**	0.526	0.573	0.442	0.531	0.473	0.459	0.722	**0.419**
	enc05	0.917	0.947	0.955	0.921	0.812	0.853	0.956	**0.956**	0.520	0.420	**0.402**	0.508	0.529	0.513	0.385	**0.402**
	enc06	0.982	0.979	0.988	0.982	0.978	0.926	0.984	**0.989**	0.363	0.391	0.362	0.358	0.371	0.402	0.345	**0.339**
	enc07	0.980	0.982	**0.987**	0.968	0.982	0.964	0.979	**0.987**	0.386	0.366	**0.367**	0.483	0.375	0.396	0.391	0.415
	enc08	0.108	0.610	0.272	0.273	0.387	0.364	**0.717**	0.229	0.428	0.341	0.796	0.414	0.369	0.483	**0.230**	0.418
	enc09	0.426	**0.760**	0.715	0.296	0.619	0.475	0.656	0.698	1.408	**1.011**	1.129	1.487	1.245	1.378	1.174	1.115
	enc10	0.824	0.966	**0.987**	0.750	0.933	0.809	0.804	0.969	1.067	0.489	**0.463**	1.246	0.574	0.796	1.121	**0.463**



(a) (b) (c)

Figure 5: The encrypted images by enc08 and enc09 from the PEID (29) database. (a) Original image. (b) Encrypted image of (a) by enc08. (c) Encrypted image of (a) by enc09.

Table 8: Computational cost of all involved metrics.

Metric	PSNR	SSIM	VIF	LSS	ESS	LFBVS	VSI-Canny	Proposed
Time(s)	**0.034**	0.136	1.983	0.173	0.518	0.789	0.778	0.476

obvious structure and orientation changes of images. Therefore, it is reasonable that our proposed method shows the better performance because the features of our proposed VSA are more relevant to the content leakage caused by most encryption methods.

4.3. Computational Complexity. Finally, considering that the running time is important in many practical applications, we analyze the computational cost of all VSAs. In our test, we measure the computational cost of a VSA on 512×512 images. We perform experiments using the original code in the MATLAB R2016b on a 64-bit Windows 7 operating system at 16 GB memory and 3.20 GHz frequency of Intel processors. To avoid the possible bias caused by selecting the specific images, we randomly choose 100 images from the PEID database and then calculate the average running time as the computation cost of each VSA.

It is known from Table 8 that most of the metrics are fast to compute. By contrast, PSNR and SSIM are the fastest methods but they are mainly used for image quality assessment, and their performance is not excellent. VIF is also an IQA method which has a relatively good performance, but its running time is much higher than other methods because its computational model is more complex. Compared with other VSAs, our proposed VSA has a faster running speed. In implementation, our method takes up most of the time in feature extraction procedure. In the future, we will try to explore more efficient feature extraction techniques to reduce the computational cost of the proposed method.

5. Conclusions

In this paper, we have presented a novel visual security assessment (VSA) that makes use of the structure and orientation information. First, we extract the structure of the original and the encrypted images by combining PC and GM. Then, we extract the orientation information by the GM, and we can obtain similarity measurements by calculating the structure and orientation similarity maps. Meanwhile, we compute the saliency map of original image. Then, we utilize a saliency-based polling strategy to combine these two similarity maps and generate the final VSA score. We conduct extensive experiments to evaluate the performance of our proposed VSA and compare it with other IQAs and VSAs which are widely used for the visual security assessment for encrypted images on two encryption image databases. The experimental results show that our proposed VSA has better performance and stronger robustness than all existing IQAs and VSAs, especially in the range of low and moderate image quality.

Data Availability

Previously reported IVC-SelectEncrypt and PEID data were used to support this study and are available at http://www.polytech.univ-nantes.fr/autrusseau-f/Databases/SelectiveEncryption/ and https://sites.google.com/site/xiangtaooo/, respectively. These prior studies (and datasets) are cited at relevant places within the text as references.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding publication of this paper.

Acknowledgments

This work was supported in part by the Natural Science Foundation of China under grant nos. 61601268, 61803237, 61901246, and U1736122; in part by the Natural Science Foundation for Distinguished Young Scholars of Shandong Province under grant no. JQ201718; and in part by the Shandong Provincial Key Research and Development Plan under grant no. 2017CXGC1504.

References

[1] F. Shang, H. Zhang, L. Zhu, and J. Sun, "Adversarial cross-modal retrieval based on dictionary learning," *Neurocomputing*, vol. 355, pp. 93–104, 2019.

[2] E. Yu, J. Sun, J. Li, X. Chang, X.-H. Han, and A. G. Hauptmann, "Adaptive semi-supervised feature selection for cross-modal retrieval," *IEEE Transactions on Multimedia*, vol. 21, no. 5, pp. 1276–1288, 2019.

[3] H. Liu, B. Xu, D. Lu, and G. Zhang, "A path planning approach for crowd evacuation in buildings based on improved artificial bee colony algorithm," *Applied Soft Computing*, vol. 68, pp. 360–376, 2018.

[4] H. Wu, H. Zhang, L. Cui, and X. Wang, "A heuristic model for supporting users' decision-making in privacy disclosure for recommendation," *Security and Communication Networks*, vol. 2018, Article ID 2790373, 13 pages, 2018.

[5] Y. X. Yan, L. Wu, W. Y. Xu, H. Wang, and Z. M. Liu, "Integrity audit of shared cloud data with identity tracking," *Security and Communication Networks*, vol. 2019, Article ID 1354346, 11 pages, 2019.

[6] W. Wan, J. Wang, and J. Li, "Hybrid JND model-guided watermarking method for screen content im-ages," *Multimedia Tools and Applications*, vol. 79, no. 7-8, pp. 4907–4930, 2018.

[7] J. Wang and W. Wan, "A novel attention-guided JND model for improving robust image watermarking," *Multimedia Tools and Applications*, vol. 79, no. 33-34, pp. 24057–24073, 2020.

[8] W. Wan, J. Wang, J. Li et al., "Pattern complexity-based JND estimation for quantization watermarking," *Pattern Recognition Letters*, vol. 130, pp. 157–164, 2020.

[9] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7965–7980, 2019.

[10] Y. Song, H. Wang, X. Wei, and L. Wu, "Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud," *Security and Communication Networks*, vol. 2019, Article ID 3249726, 9 pages, 2019.

[11] X. Xiao, X. Zheng, and Y. Zhang, "A multidomain survivable virtual network mapping algorithm," *Security and Communication Networks*, vol. 2017, Article ID 5258010, 12 pages, 2017.

[12] H. Liu, B. Liu, H. Zhang, L. Li, X. Qin, and G. Zhang, "Crowd evacuation simulation approach based on navigation knowledge and two-layer control mechanism," *Information Sciences*, vol. 436-437, pp. 247–267, 2018.

[13] G. Han and W. Zhang, "Improved biclique cryptanalysis of the lightweight block cipher piccolo," *Security and Communication Networks*, vol. 2017, Article ID 7589306, 12 pages, 2017.

[14] X. Zheng, J. Tian, X. Xiao, X. Cui, and X. Yu, "A heuristic survivable virtual network mapping algorithm," *Soft Computing*, vol. 23, no. 5, pp. 1453–1463, 2019.

[15] H. Wang, D. He, J. Shen, Z. Zheng, X. Yang, and M. H. Au, "Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps," *Soft Computing*, vol. 22, no. 7, pp. 2267–2274, 2018.

[16] W. Zhang and V. Rijmen, "Division cryptanalysis of block ciphers with a binary diffusion layer," *IET Information Security*, vol. 13, no. 2, pp. 87–95, 2019.

[17] H. Hofbauer and A. Uhl, "Identifying deficits of visual security metrics for images," *Signal Processing: Image Communication*, vol. 46, pp. 60–75, 2016.

[18] Z. Tang, Z. Huang, H. Yao, X. Zhang, L. Chen, and C. Yu, "Perceptual image hashing with weighted DWT features for reduced-reference image quality assessment," *The Computer Journal*, vol. 61, no. 11, pp. 1695–1709, 2018.

[19] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[20] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430–444, 2006.

[21] T. Xiang, S. Guo, and X. Li, "Perceptual visual security index based on edge and texture similarities," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 951–963, 2016.

[22] Y. Mao and M. Wu, "Security evaluation for communication-friendly encryption of multimedia," in *Proceedings of IEEE International Conference on Image Processing (ICIP)*, vol. 1, pp. 569–572, Singapore, October 2004.

[23] L. Tong, F. Dai, Y. Zhang, and J. Li, "Visual security evaluation for video encryption," in *Proceedings of ACM International Conference on Multimedia*, pp. 835–838, Firenze, Italy, October 2010.

[24] J. Sun, X. Liu, W. Wan, J. Li, D. Zhao, and H. Zhang, "Video hashing based on appearance and attention features fusion via DBN," *Neurocomputing*, vol. 213, pp. 84–94, 2016.

[25] J. Zong, L. Meng, H. Zhang, and W. Wan, "JND-based multiple description image coding," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 8, pp. 3935–3949, 2017.

[26] T. Xiang, Y. Yang, H. Liu, and S. Guo, "Visual security evaluation of perceptually encrypted images based on image importance," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 11, pp. 4129–4142, 2020.

[27] P. Kovesi, "Image features from phase congruency," *Videre: Journal of Computer Vision Research*, vol. 1, no. 3, pp. 1–26, 1999.

[28] Y. Liu, k. Gu, Y. Zhang et al., "Unsupervised blind image quality evaluation via statistical measurements of structure, naturalness, and perception," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 4, pp. 929–943, 2020.

[29] J. Wu, W. Lin, G. Shi, Y. Zhang, W. Dong, and Z. Chen, "Visual orientation selectivity based structure description," *IEEE Transactions on Image Processing*, vol. 24, no. 11, pp. 4602–4613, 2015.

[30] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[31] J. Zhou, O. C. Au, G. Zhai, Y. Y. Tang, and X. Liu, "Scalable compression of stream cipher encrypted images through context-adaptive sampling," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1857–1868, 2014.

[32] F. Autrusseau, T. Stutz, and V. Pankajakshan, "Subjective quality assessment of selective encryption techniques," 2010.

[33] S. Guo, T. Xiang, X. Li, Y. Yang, and P. E. I. D. ", "A perceptually encrypted image database for visual sec-urity evaluation," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 99, pp. 1151–1163, 2019.

[34] L. Zhang, Y. Shen, and H. Li, "VSI: VSI: a visual saliency-induced index for perceptual image quality assessment," *IEEE Transactions on Image Processing*, vol. 23, no. 10, pp. 4270–4281, 2014.

[35] J. Wu, W. Lin, G. Shi, L. Li, and Y. Fang, "Orientation selectivity based visual pattern for reduced-reference image quality assessment," *Information Sciences*, vol. 351, pp. 18–29, 2016.

[36] J. Harel, C. Koch, and P. Perona, "Graph-based visual saliency," in *Proceedings of International Conference on Neural Information Processing Systems (NIPS)*, pp. 545–552, Columbia, Canada, December 2006.

[37] S. Goferman, L. Zelnik-Manor, and A. Tal, "Context-aware saliency detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 10, pp. 1915–1926, 2012.

[38] E. Erdem and A. Erdem, "Visual saliency estimation by nonlinearly integrating features using region covariances," *Journal of Vision*, vol. 13, no. 4, pp. 1–11, 2013.

[39] A. Garcia-Diaz, X. R. Fdez-Vidal, X. M. Pardo, and R. Dosil, "Saliency from hierarchical adaptation through decorrelation and variance normalization," *Image and Vision Computing*, vol. 30, no. 1, pp. 51–64, 2012.

[40] J. Zhang and S. Sclaroff, "Saliency detection: a boolean map approach," in *Proceedings of the 2013 IEEE International Conference on Computer Vision*, Sydney, NSW, Australia, December 2013.