# ENCRYPTED IMAGE VISUAL SECURITY INDEX VIA NON-LOCAL RECOGNIZABLE DEGREE EVALUATION

*Ran Shi*[a] *Jian Xiong*[b] *Tong Qiao*[c]

[a] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China
[b] College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China
[c] School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China

**ABSTRACT**

With the development of perceptual image encryption techniques, visual security evaluations of perceptually encrypted images have gained much attention. Current visual security indices isolate neither global nor local visual security evaluations. They ignore the fact that humans can reorganize partial local information to infer global information and local information can possibly be leaked in any position of the encrypted image. To address this problem, we propose a block-based non-local recognizable degree measure with a global structure similarity measure as a visual security index. In our index, the non-local searching strategy is utilized to capture leaked local information in any position of an encrypted image. The recognizable degree is evaluated by appearance recognizability and spatial structural recognizability involving human visual properties. In addition, weighted Minkowski pooling is adopted to evaluate the overall recognizable degree of all blocks depending on highly recognizable blocks. Furthermore, this overall recognizable degree is adjusted by global structure similarity, which is used to alleviate the global region structure distortion problem induced by the block partition. Experimental results demonstrate the sharpness and good robustness of our proposed index on different databases and various encryption types.

***Index Terms***— Encrypted Images, Visual Security

## 1. INTRODUCTION

Perceptual image encryption [1] aims to protect the visual content of an image by encrypting its information. Its performance is determined by the encrypted image's visual security degree, which represents the perceptually unrecognizable degree of the encrypted image compared with its plain image. Since the human viewer is the end recipient of the encrypted image, the most reliable method of visual security degree evaluation is the subjective assessment. However, this is impractical due to the high labor cost and cumbersome of the subjective assessment. Therefore, there is a great demand for effective objective indices that can evaluate the visual security degree in good agreement with subjective judgment.

The visual security index is different from the traditional image quality assessment metric [7]. For example, an image with poor visual quality may not mean that it maintains high visual security. The content of this image can also be leaked. Generally, visual security indices can be classified into two categories: local-based indices [2, 3] and global-based indices [4, 5, 6, 7]. For local-based indices, the plain and the encrypted image are divided into several non-overlapped blocks, and then each block in the plain image can obtain a visual security score by comparing it with its corresponding block in the same position of the encrypted image. The overall visual security degree of the encrypted image is estimated by pooling the visual security degrees of all blocks. In [2], an edge similarity score (ESS) and a luminance similarity score (LSS) were proposed between the plain image and perceptually encrypted image to indicate the visual security degree. In [3], the similarities of luminance and local gradient were used to evaluate one encrypted block's visual security degree. Different from local-based indices, global-based indices directly extract features of the whole image to measure the visual security degree. Xiang et al. [4] proposed a VSI-Canny by calculating the weighted edge and texture similarities between the plain and encrypted images. In [5], the wavelet-based frequency information was further considered to improve the performance of the VSI-Canny. Yue et al. [6] adopt multiple quality-sensitive image attributes, such as naturalness, structure and texture to assess the visual quality of an encrypted image as its visual security degree. In [7], an image visual importance pooling method was considered to combine spatial contrast and texture similarity maps in addition to features of gradient magnitude and texture.

In current visual security indices, their evaluation strategies isolate the relationship between global visual security and local visual security. They ignore that even if humans cannot obtain the global information of an image, global information can still be inferred by re-organizing partial local information. This means that the leakage of the local information can heavily degrade the whole visual security degree. Meanwhile, local information in the plain image can actually be leaked in any position rather than corresponding positions in the encrypted image so that the current adopted evaluation strategy is not as effective. Moreover, these indices do not fully involve human visual properties when the visual security degree is evaluated. Another side effect of block-based indices is that the block partition may distort an image's own region structure. For example, if one part of an object and background are partitioned into one block, it does not conform to humans understanding of the region structure. This may reduce the accuracy of the visual security evaluation. Therefore, inspired by non-local means filter [8] which bridges global and local information, we propose a block-based non-local recognizable degree measure with a global structure similarity measure as our visual security index. Compared with previous related works, the main contributions of our work are summarized as follows:

1. A novel overall recognizability evaluation strategy is proposed that captures highly recognizable local information in the encrypted image by the non-local searching. Thus, the overall recognizable degree can be estimated by mostly

Jian Xiong is the corresponding author. This work was supported by the National Natural Science Foundation of China under Grants 61801219 and 61701258, and the Fundamental Research Funds for the Provincial Universities of Zhejiang under grant No.GK219909299001-007.

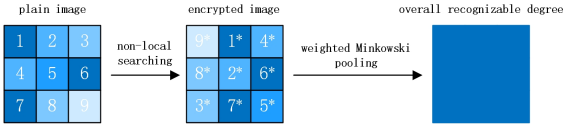
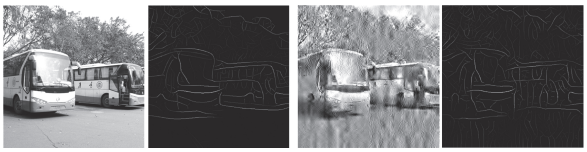



**Fig. 1**: The legend of our proposed overall recognizability evaluation strategy. The number and "$*$" indicate the corresponding positions of matching blocks. A deeper color corresponds to a higher recognizable degree.



(a) (b)

**Fig. 2**: One plain image, its poorly encrypted image in the PEID database [10] and their edge maps. (a) One plain image with its edge map (b) one poorly encrypted image with its edge map.

depending on highly recognizable local information from weighted Minkowski pooling, which conforms more with human perception.

2. We design Minkowski pooling based appearance recognizability measure and fuzzy Jaccard Index based spatial structural recognizability measure to properly evaluate the recognizable degree of two compared blocks involving human visual properties.
3. Our index can not only overcome ineffectiveness on special encryption type but also achieve better average evaluation accuracy on various encryption types compared with the state-of-art indices.

This paper is organized as follows. Section II describes our visual security index in detail. Experimental results are presented in Section III. We conclude our paper in Section IV.

## 2. THE PROPOSED METHOD

Given a plain image $P$ and its encrypted image $E$, our goal is to develop an index to evaluate the visual security degree of this encrypted image. The overall recognizability evaluation strategy of our index is illustrated in Fig. 1. Since humans can infer one encrypted image's global information from its local information leaked in any position, our index adopts a "block" as a basic local unit in the plain image and each block can match one block with its highest recognizable degree in the encrypted image by the non-local searching. Then, the overall recognizable degree is mainly inferred from these highly recognizable blocks using weighted Minkowski pooling. Both of $P$ and $E$ are divided into $M \times N$ non-overlapped blocks whose sizes are $l \times l$, where $M$ and $N$ are the numbers of blocks along the row and the column respectively. $l$ is estimated as $\lfloor \alpha L \rfloor + 1$, where $L$ is the length of the shorter side of $P$, $\alpha$ is a constant and $\lfloor \cdot \rfloor$ is the round-down operator. For one block $b_p$ in the plain image, its non-local recognizable degree $RD(b_p)$ is evaluated as:

$$RD(b_p) = MAX_{b_e \in B_E}(sim(b_p, b_e)) \quad (1)$$

where $b_e$ is one block belonging to the block set $B_E$ of all blocks in the encrypted image and $sim$ is the recognizable degree measure. Therefore, "non-local" is embodied in that each $b_p$ can match a $b_e^*$ with its highest recognizable degree by comparison with all blocks in the encrypted image rather than the block in $b_p$'s corresponding position only.

For the recognizable degree measure $sim$ of two compared blocks, we consider two factors: appearance recognizability $sim_A$ and spatial structural recognizability $sim_S$. On the one hand, the appearance recognizability directly correlates with the visual perceptual similarity of two compared blocks; on the other hand, the spatial structural recognizability represents similar understanding of two compared blocks' spatial structures. For $sim_A$, it can be estimated by four steps:

1. Since the human visual system is sensitive to the changes in various frequency components of an image especially to the low frequency components, $b_p$ and $b_e$ are first transformed into the frequency domain by the Discrete Cosine Transform (DCT).
2. Then, their DCT coefficients of subbands are weighted by a low-pass filter, where we use the exponential function $exp(-r/\sigma)$ to approximate this filter. $r$ is a certain subband's rank following the zigzag order, and $\sigma$ is the bandwidth controlled by $\beta l$, where $\beta$ is a ratio constant.
3. After the weighting in the frequency domain, $b_p$ and $b_e$ are transformed back to the spatial domain as $\tilde{b_p}$ and $\tilde{b_e}$.
4. Finally, their $sim_A$ is estimated by Minkowski pooling as [9]:

$$sim_A(b_p, b_e) = \sqrt[\gamma]{\frac{1}{l*l}\sum_i (1 - \frac{|\tilde{b_p}(i) - \tilde{b_e}(i)|}{255})^\gamma} \quad (2)$$

where $i$ represents a certain pixel and $\gamma$ is a constant. The core property of the Minkowski pooling is that higher $\gamma$ makes the pooling result be more dependent on larger components.

We can see that $sim_A$ is more dependent on the most similar pixels in the $b_p$ and $b_e$. This also reflects the importance of the local recognizability as well as in the block.

If $sim_A(b_p, b_e)$ is higher, $b_p$ should be easily recognized in the encrypted image. However, even if $sim_A(b_p, b_e)$ is lower, humans can still recognize the partial content of $b_p$ by spatial structure similarity. Therefore, we design a spatial structural recognizability $sim_S$. We use a Fourier-Argand filter [11] which has a strong noise suppression ability to extract the main edges of the plain image and encrypted image as shown in Fig. 2. Accordingly, $b_p$ and $b_e$ can obtain their own edge maps $EM_{b_p}$ and $EM_{b_e}$. The edge map is used to describe one block's structural information which can assist humans in recognizing this block. Although encryption processes may displace or distort edges to some extent, they may not overly impede human ability to understand the structural information. Therefore, we develop a fuzzy Jaccard Index (i.e. IoU) to evaluate $sim_S$. It assigns different weights to edges in the encrypted block which is represented as a weight map $WEM_{b_p}$ of $EM_{b_p}$. Closer to edges in the plain block, edges in its encrypted block can obtain higher weights. For $sim_S$, it can be estimated following three steps:

1. Firstly, $EM_{b_p}$ is converted into its binary map $BEM_{b_p}$ by a threshold 0.5. By performing the distance transform on $BEM_{b_p}$, we obtain a distance map $DSM_{b_p}$ where each pixel's value indicates its shortest distance to the edges in $BEM_{b_p}$.
2. Then, the weight map $WEM_{b_p}$ is calculated as $(1 - DEM_{b_p}/d_{b_p})$. $d_{b_p}$ is the diagonal length of $b_p$ as a reference length to perform normalization.

3. Finally, $sim_S(b_p, b_e)$ follows the formulation of the Jaccard Index:

$$sim_S(b_p, b_e) = \frac{|WEM_{b_p} \cdot BEM_{b_e}|}{|BEM_{b_p}| + |BEM_{b_e}| - |BEM_{b_p} \cdot BEM_{b_e}|} \tag{3}$$

where $|\cdot|$ is the norm and $BEM_{b_e}$ is the binary map of $EM_{b_e}$. The weight map allows $sim_S$ to tolerate slight structural distortion.

As discussed above, $sim_S$ plays an auxiliary role in $sim$. Therefore, $sim$ is estimated as:

$$sim(b_p, b_e) = sim_A(b_p, b_e) \cdot sim_S(b_p, b_e)^{1-sim_A(b_p,b_e)} \tag{4}$$

where $sim$ is mainly determined by $sim_A$ and complemented by $sim_S$.

When each $b_p$ can find its $b_e^*$ with the highest recognizable degree, we can pool them to estimate the overall recognizable degree of $E$. For each $b_p$, we also consider its weight for the overall recognizable degree. On the one hand, a higher structural complexity of one block means it involves more recognizable information; on the other hand, one block's information can also be inferred from those of its neighboring blocks due to their high correlations. Therefore, one block with high structural complexity should be assigned a large weight while the weight can be reduced if its neighboring blocks have high recognizable degrees. Therefore, $b_p$'s weight $w(b_p)$ is estimated as:

$$w(b_p) = (1 - NRD_{avg}(b_p))\sqrt{\frac{1}{l*l}\sum_i (EM_{b_p}(i))^2 - (\frac{1}{l*l}\sum_i EM_{b_p}(i))^2} \tag{5}$$

where $NRD_{avg}(b_p)$ is the average recognizable degree of $b_p$'s four-neighboring blocks. The latter term about the structural complexity refers to [12].

Based on the non-local recognizable degree and the weight of each block, we also adopt Minkowski pooling to measure the recognizability degree of $E$:

$$RD(P, E) = \sqrt[\gamma]{\frac{1}{\sum_{b_p} w(b_p)} \sum_{b_p} (w(b_p) \cdot RD(b_p)^\gamma)} \tag{6}$$

We can see that $RD(P, E)$ are mainly dependent on those blocks with high recognizable degrees. It follows that humans can recognize one encrypted image by inferring it from the most recognizable local information.

In addition, one side effect of block-based indices is that the block partition may distort an image's own region structure. For example, if one part of an object and background are partitioned into one block, it does not conform to human's understanding of the region structure. This may influence the visual security evaluation. To alleviate this problem, we also introduce a global structural similarity measure $GS$ between $P$ and $E$:

$$GS(P, E) = B(H(EM_P), H(EM_E)) \tag{7}$$

where $B(\cdot)$ calculates the Bhattacharyya distance [13] between histograms $H(\cdot)$ of $P$'s edge map $EM_P$ and $E$'s edge map $EM_E$ to indicate their global structural similarity. A higher $GS(P, E)$ indicates a higher similarity. Finally, our visual security index is formulated as:

$$VSI(P, E) = RD(P, E)(1 + GS(P, E)) \tag{8}$$

In our index, a higher $VSI$ indicates a lower visual security. The proposed $VSI$ is mainly determined by the block based non-local recognizable degree measure $RD$ and $GS$ is treated as a coefficient to adjust our index by measuring the global structural similarity.

## 3. EXPERIMENTS

### 3.1. Dataset

In order to evaluate the performance of our proposed index, we tested it on two widely used encrypted image databases, IVC-SelectEncrypt [14] and PEID [10]. The IVC-SelectEncrypt database includes 200 encrypted images generated from eight plain images by exploiting five different encrypted algorithms based on five different security degrees. The PEID database comprises 1080 encrypted images of 20 plain images using ten perceptual encryption schemes. Using a subjective survey, each encrypted image in these two databases can obtain a Mean Opinion Score (MOS) to indicate its visual security score. Thus, MOS can be treated as the ground truth of the visual security score predicted by our index. Following the work of [15], each predicted score $x$ is first mapped to $Q(x)$ to obtain a linear relationship with MOS.

### 3.2. Overall performance

In the experiments, $\alpha$ and $\beta$ in our index are empirically set to 0.1 and 40. $\gamma$ is set to 5 referred to [9]. Our index is also compared against seven encrypted image visual security score indices which are LSS [2], ESS [2], LFBVS [3], VSI-Canny [4], NQIQAPEI [6], NMVSI [5] and IIBVSI [7]. Four common performance evaluation criteria, i.e. the Spearman Rank-Order Correlation Coefficients (SROCC), the Kendall rank correlation coefficient (KRCC),the Linear Correlation Coefficient (LCC) and the root mean squared error (RMSE) are used to evaluate the performance. Higher values of the first three criteria indicate better subjective agreement achieved by the proposed index, while the last criterion is the reverse. The comparison results are shown in Table. 1. We can see that our index can achieve the second highest SROCC and LCC, the third highest KRCC, and the lowest RMSE in the IVC-SelectEncrypt database. For the PEID database, our index outperforms other indices in terms of all four criteria. Overall, it shows that the performance of our index is competitive and demonstrates that our strategy of the block based non-local recognizability matching combined with the global structure similarity evaluation is effective.

### 3.3. Performance on Different Types of Encryption

In our opinion, a visual security index with wider usage should be available for different encryption methods as many as possible. To more comprehensively evaluate the performance of our index on different encryption types, we further perform experiments on each encryption type on two test databases. For brevity, we only present the SROCC results of all indices.

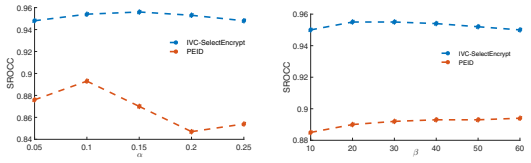
In Table. 2, our proposed index can achieve the highest average SROCC (increased 3.3%) and the smallest standard deviation (decreased 7.2%) of all encryption types in the two databases. Specifically, by the non-local searching, our index achieves significant improvement on the enc09 "Chaos Psudoramdom Generator" encryption algorithm [16] which divides one image into many blocks and shuffles their positions. As Buckets effect reveals, the capacity of a bucket depends on the shortest board. The SROCC of our index on enc09 is 0.889, however other indices are completely invalid on this type where the second best performance is only 0.457 by the IIBVSI. It means that if we use other compared indices to evaluate visual security of images encrypted by enc09, their results should be far away from subjective perception. Therefore, the effectiveness of these indices is limited by this special encryption type enc09. Furthermore, if we recalculate the average SROCC of each index by

**Table 1**: Performance comparison of different visual security indices.

| Database | Evaluation | LSS | ESS | LFBVS | VSI-Canny | NQIQAPEI | NMVSI | IIBVSI | Our |
|---|---|---|---|---|---|---|---|---|---|
| IVC-SelectEncrypt | SROCC | 0.932 | 0.909 | 0.891 | 0.949 | 0.894 | 0.948 | **0.968** | 0.954 |
| | KRCC | 0.786 | 0.747 | 0.712 | 0.819 | **0.892** | 0.817 | 0.848 | 0.820 |
| | LCC | 0.920 | 0.901 | 0.891 | 0.950 | 0.726 | 0.949 | **0.966** | 0.953 |
| | RMSE | 0.520 | 0.576 | 0.601 | 0.887 | 0.598 | 0.417 | 0.405 | **0.402** |
| PEID | SROCC | 0.749 | 0.772 | 0.618 | 0.799 | 0.813 | 0.802 | 0.878 | **0.893** |
| | KRCC | 0.575 | 0.592 | 0.458 | 0.632 | 0.676 | 0.634 | 0.719 | **0.820** |
| | LCC | 0.803 | 0.808 | 0.724 | 0.884 | 0.818 | 0.845 | 0.893 | **0.897** |
| | RMSE | 1.078 | 1.065 | 1.248 | 0.845 | 0.834 | 0.843 | 0.816 | **0.801** |

**Table 2**: Performance comparison (SROCC) of different visual security indices on each encryption type.

| Database | Type | LSS | ESS | LFBVS | VSI-Canny | NQIQAPEI | NMVSI | IIBVSI | Our |
|---|---|---|---|---|---|---|---|---|---|
| IVC-SelectEncrypt | trad | 0.948 | 0.933 | 0.960 | 0.964 | 0.963 | 0.776 | 0.962 | **0.972** |
| | trunc | 0.948 | 0.913 | 0.907 | **0.966** | **0.966** | 0.595 | 0.939 | 0.884 |
| | iwind_ec | 0.887 | 0.858 | 0.866 | 0.928 | 0.927 | 0.433 | **0.942** | 0.912 |
| | iwind_nec | 0.907 | 0.922 | 0.946 | 0.925 | 0.924 | 0.672 | **0.974** | 0.969 |
| | res | **0.955** | 0.926 | 0.919 | 0.954 | 0.953 | 0.742 | **0.955** | 0.954 |
| PEID | enc01 | 0.950 | 0.540 | 0.451 | 0.951 | **0.952** | 0.866 | 0.784 | 0.893 |
| | enc02 | 0.834 | 0.846 | 0.627 | **0.963** | **0.963** | 0.917 | 0.886 | 0.936 |
| | enc03 | 0.943 | 0.966 | 0.862 | **0.977** | 0.976 | 0.899 | 0.939 | 0.901 |
| | enc04 | 0.908 | 0.828 | 0.906 | 0.923 | 0.923 | 0.876 | **0.944** | 0.901 |
| | enc05 | 0.924 | 0.789 | 0.821 | **0.959** | 0.958 | 0.893 | 0.798 | 0.913 |
| | enc06 | 0.968 | 0.961 | 0.914 | **0.975** | **0.975** | 0.896 | 0.939 | 0.951 |
| | enc07 | 0.958 | 0.975 | 0.958 | **0.981** | **0.981** | 0.967 | 0.954 | 0.948 |
| | enc08 | 0.199 | 0.325 | 0.360 | 0.682 | 0.682 | 0.733 | **0.745** | 0.715 |
| | enc09 | 0.187 | 0.364 | 0.339 | 0.307 | 0.307 | 0.257 | 0.457 | **0.889** |
| | enc10 | 0.630 | 0.846 | 0.677 | 0.596 | 0.586 | **0.933** | 0.859 | 0.834 |
| Avg | | 0.810 | 0.799 | 0.768 | 0.870 | 0.869 | 0.764 | 0.872 | **0.905** |
| Std | | 0.264 | 0.213 | 0.222 | 0.193 | 0.194 | 0.202 | 0.136 | **0.064** |




(a) (b)

**Fig. 3**: SROCC of our proposed index with different parameters settings. (a) parameter $\alpha$, (b) parameter $\beta$.

**Table 3**: SROCC of our proposed index with four different configurations.

| | $sim_A$ | $sim_S$ | $w$ | $GS$ | IVC-SelectEncrypt | PEID |
|---|---|---|---|---|---|---|
| C1 | √ | | | | 0.935 | 0.825 |
| C2 | √ | √ | | | 0.940 | 0.885 |
| C3 | √ | √ | √ | | 0.956 | 0.885 |
| C4 | √ | √ | √ | √ | 0.954 | 0.893 |

excluding biases of its highest and lowest SROCC values, our index can also obtain the best performance of 0.914 and the second best one is VSI-Canny with 0.905. The results demonstrate that our index can not only overcome ineffectiveness on special encryption type but also have stronger robustness on different encryption types compared with other indices.

### 3.4. Parameterizations

In our index, there are two main parameters: one is $\alpha$ to determine the block size; the other is $\beta$ to estimate the bandwidth $\sigma$ in $sim_A$. In above experiments, $\alpha$ and $\beta$ are set to 40 and 0.1 respectively. In order to assess their influences for our index, we evaluate our index's performance in terms of SROCC using different $\alpha$ and $\beta$. $\beta$ is first fixed as 40 and $\alpha$ is sampled from 0.05 to 0.25 with step 0.05. Then, we fix $\alpha$ as 0.1 and test different $\beta$ ranging from 10 to 60. As illustrated in Fig. 3, compared with $\beta$, SROCC is with fluctuation by varying $\alpha$ especially tested on PEID database. Since "non-local" is a relative concept, too small block may lost its own recognizability and too large block makes the matching tend to be global. Therefore, larger or smaller $\alpha$ may degrade the effectiveness of the non-local recognizability matching.

### 3.5. Ablation study and limitations

In order to further analyze the contribution and limitation of each component in our index, we perform an ablation study with four configurations and test them on the IVC-SelectEncrypt database and PEID database. SROCC is used to indicate their performances as shown in Table 3. Therein, $C1$ can be treated as a basic strategy of our index which has $sim_A$ only and there is no weighting $w$ in the pooling and no global similarity $GS$. However, the basic strategy $C1$ already outperforms all block-based indices on these two databases. From $C1$ and $C2$, we can see that the combination of $sim_A$ and $sim_S$ is reasonable to measure the block's recognizable degree. Compared with $C2$ and $C3$, $w$ can improve the performance of our index on the IVC-SelectEncrypt database. However, it cannot influence the performance on the PEID database. By the adjustment of $GS$, our index can achieve better performance on the PEID database but worse performance on the IVC-SelectEncrypt database. This reflects the limitations of $w$ and $GS$ which may not be suitable for all cases. The reason might be that different correlation degrees of neighboring blocks in $w$ are not involved. For $GS$, our index may benefit from a more adaptive way to integrate it with $RD$. In our future work, we can optimize $w$ and $GS$ to further improve our index.

## 4. CONCLUSION

In this paper, we evaluate encrypted image visual security by integrating the block-based non-local recognizable degree evaluation and the global structure similarity. The merit of our proposed visual security index is that it can infer the overall recognizable degree from those highly recognizable blocks that appear in any position, which better agrees with human perception. Experimental results demonstrate the superiority and robustness of our proposed index.

## 5. REFERENCES


[1] T. Lookabaugh and D. C. Sicker, "Selective encryption for consumer applications," *IEEE Communications Magazine*, vol. 42, no. 5, pp. 124–129, 2004.

[2] Min Wu Yinian Mao, "Security evaluation for communication-friendly encryption of multimedia," in *Image Processing, 2004. ICIP '04. 2004 International Conference on*, 2004.

[3] Lingling Tong, Feng Dai, Yongdong Zhang, and Jintao Li, "Visual security evaluation for video encryption," in *Proceedings of the 18th International Conference on Multimedea 2010, Firenze, Italy, October 25-29, 2010*, 2010.

[4] Tao Xiang, Shangwei Guo, and Xiaoguo 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.

[5] Aansu Sara Abraham, Lekha R Nair, and MS Deepa, "A novel method for evaluation of visual security of images," in *2017 International Conference on Networks and Advances in Computational Technologies (NetACT)*. IEEE, 2017, pp. 387–391.

[6] Guanghui Yue, Chunping Hou, Ke Gu, Tianwei Zhou, and Hantao Liu, "No-reference quality evaluator of transparently encrypted images," *IEEE Transactions on Multimedia*, vol. PP, no. 99, pp. 1–1, 2019.

[7] Tao Xiang, Ying Yang, Hangcheng Liu, and Shangwei Guo, "Visual security evaluation of perceptually encrypted images based on image importance," *IEEE Transactions on Circuits and Systems for Video Technology*, 2019.

[8] Antoni Buades, Bartomeu Coll, and J. M. Morel, "A non-local algorithm for image denoising," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2005.

[9] Maurizio Carosi, Vinod Pankajakshan, and Florent Autrusseau, "Towards a simpli?ed perceptual quality metric for watermarking applications," *Proceedings of Spie the International Society for Optical Engineering*, vol. 7542, 2010.

[10] Shangwei Guo, Tao Xiang, Xiaoguo Li, and Ying Yang, "Peid: A perceptually encrypted image database for visual security evaluation," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, pp. 1–1, 2019.

[11] Tianle Zhao and Thierry Blu, "The fourier-argand representation: An optimal basis of steerable patterns," *IEEE Transactions on Image Processing*, vol. PP, no. 99, pp. 1–1, 2020.

[12] P. L. Correia and F. Pereira, "Objective evaluation of video segmentation quality," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 186–200, 2003.

[13] Jifeng Ning, Lei Zhang, David Zhang, and Chengke Wu, "Interactive image segmentation by maximal similarity based region merging," *Pattern Recognition*, vol. 43, no. 2, pp. 445–456, 2010.

[14] Tao Xiang, Kwok-wo Wong, and Xiaofeng Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, pp. 023115, 2007.

[15] VQEG, "Final report from the video quality experts group on the validation of objective models of video quality assessment," 2003.

[16] T Xiang, K. W. Wong, and X Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, no. 2, pp. 1–10, 2007.