© ACM. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published by ACM, see http://portal.acm.org/dl.cfm.

# Image Segmentation Based Visual Security Evaluation

Christof Kauba Department of Computer Sciences University of Salzburg 5020 Salzburg, AUSTRIA ckauba@cosy.sbg.ac.at Stefan Mayer Department of Computer Sciences University of Salzburg 5020 Salzburg, AUSTRIA mail@stefan-mayer.at

Andreas Uhl Department of Computer Sciences University of Salzburg 5020 Salzburg, AUSTRIA uhll@cosy.sbg.ac.at

## ABSTRACT

In this paper we present a metric for visual security evaluation of encrypted images, also known as visual security metric. Such a metric should be able to assess whether an image encryption method is secure or not. In order to consider intelligibility of objects in encrypted images our metric is based on image segmentation and applying a measure designed to evaluate the segmentation result. The visual security metrics' performance is evaluated using a selective encryption approach and compared to some general image quality metrics like PSNR, metrics suggested for encrypted images like Irregular Deviation and two metrics specifically designed for visual security evaluation. Our visual security metric performs better than all of the other tested metrics on the dataset and encryption algorithm we used during our experiments in terms of different correlation measures.

### Keywords

visual security metric, selective encryption, image segmentation, confidence, correlation

## **1. INTRODUCTION**

Today a number of (format compliant) image encryption techniques exist which allow the encrypted content to be decoded and viewed. To determine the level of security offered by these techniques it is not enough to simply evaluate the cryptographic strength of the encryption cipher used. For some methods the decoded encrypted image is a low quality version of the original image and certain image features can still be recognised. So beside evaluating the encryption cipher also the visual security of the result has to be assessed. Visual security metrics are designed to be able to assess the security of an image encryption method based on the visual output. In this context they need to deal with the remaining image information left behind by the encryption process and the recognizability and intelligibility of the encrypted image content.

In order to be able to discuss the exact notion of visual

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

IH&MMSec 2016, June 20 - 23, 2016, Vigo, Spain

© 2016 Copyright held by the owner/author(s). Publication rights licensed to ACM. ISBN 978-1-4503-4290-2/16/06...\$15.00

DOI: http://dx.doi.org/10.1145/2909827.2930806

security, we need to distinguish distinct application scenarios of media encryption schemes [9]:

**Confidentiality Encryption**: means MP security (message privacy). The formal notion is that if a system is MP-secure an attacker cannot efficiently compute any property of the plain text from the cipher text. This can only be achieved by the conventional encryption approach, i.e. applying a cryptographically strong cipher to compressed (redundancy-free) image data.

**Content Confidentiality**: is a relaxation of confidential encryption. Side channel information may be reconstructed or left in plaintext, e.g. header information, packet length, but the actual visual content must be secure in the sense that the image content must not be intelligible / discernible.

**Sufficient Encryption**: means we do not require full security, just enough security to prevent abuse of the data. The content must not be consumable due to high distortion (e.g. for DRM systems) by destroying visual quality to a degree which prevents a pleasant viewing experience or destroys the commercial value. This implicitly refers to message quality security (MQ), which requires that an adversary cannot reconstruct a higher quality version of the encrypted material than specified for the application scenario.

Given these different application scenarios it is clear that depending on the goal, a security metric has to fulfil different roles. For example, under the assumption of sufficient encryption a given security metric would have to evaluate which quality is low enough to prevent a pleasant viewing experience.

When it comes to content confidentiality the question of quality is no longer applicable. Content confidentiality requires that image content must not be identified by human or automated recognition. This requirement also has to be maintained for any part of the image. Image metrics, in general, do not deal with such questions but rate the overall image quality, the question of intelligibility is usually not covered at all. Thus, it seems to be clear that a general purpose metric covering all application scenarios is probably very hard or impossible to design.

Additionally we have to face the fact that different encryption methods introduce different kind of distortions. While some methods shift and morph the images (i.e. chaotic encryption which is mainly based on permutations) others introduce noise and noise like patterns. An ideal metric for assessment of visual security has to be able to deal with those different kind of distortions.

While PSNR, SSIM, and the more more specific measures developed in the context of visual encryption do a reasonable job to rate the visual security of a ciphered image for particular image encryption techniques, for many encryption methods these metrics tend to have troubles in the correct assessment of visual security in correspondence to visual perception especially for higher levels of encryption. Hofbauer and Uhl showed that general visual image quality metrics have difficulties assessing low quality images [7].

Since most of these metrics compare the plain and the cipher images pixel by pixel or region by region (fundamental principles of the Human Vision System (HVS) in terms of luminance and edge perception are considered) a warped image may still be recognisable while the metric rates the image as secure due to large dissimilarities in terms of pixel or local region differences. Also, noise patterns tend to decrease the score rather quickly but leave the content of the image still intelligible. Thus, answering the question if an encryption of this type results in a content confidential image, i.e. an image without any intelligible content, can become quite challenging with those metrics.

An important aspect if it comes to content intelligibility is the ability to recognise objects in the images both for humans and automated detection. One way to detect objects inside an image is to use image segmentation methods trying to automatically detect and segment the objects from the background and each other. If the segmentation succeeds this indicates that there are still some objects visible (or at least partially visible). Our approach is based on image segmentation and evaluating the segmentation result in order to design a metric for visual security assessment which is able to handle the issue of content recognition and intelligibility in a more appropriate manner. The basic idea is to first segment the reference and cipher image and then compare the segmentation results. By doing so our approach should be able to capture parts of the image content (i.e. contours) which are still visible despite the warping and noise introduced by the encryption approach. Thus the overall metric is termed "Segmentation Based Similarity Score" (SBSS).

The rest of the paper is divided into four parts. In section 2 an overview of existing visual security metrics is given. Section 3 explains the segmentation based similarity score. Section 4 describes the experimental setup, including the dataset and the encryption approach used to test the metrics performance and lists the other metrics which are evaluated. This is followed by the presentation and discussion of the experimental results in section 5. Finally section 6 concludes this paper and gives an outlook on future work.

#### 2. VISUAL SECURITY METRICS

To evaluate the visual security of an encrypted image in an objective manner, several different kinds of metrics have been proposed in the literature. This section gives a short overview of these metrics where the ones we used during our experiments are described in more detail.

Despite the fact that PSNR and SSIM originally have been developed for image quality assessment, they have also been used for the assessment of encrypted images [2, 11, 3].

Besides that several attempts have been made to develop metrics specifically for the task of measuring the encryption quality. Luminance variance (LV) [5] simply measures the variance in the luminance values in the encrypted images. High variance should indicate a higher level of encryption and thus higher visual security.

The irregular deviation [1] measures how much the statis-

tical distribution of histogram deviation is close to uniform distribution. For perfectly encrypted images the deviation should be close to uniform distribution, thus the smaller the value of irregular deviation (ID) the better the encryption quality. ID is calculated as follows:

- 1. Absolute difference of reference image (R) and encrypted image (C): D = |R C|
- 2. Calculate the histogram of D: H = histogram(D)
- 3. Let  $h_i$  be the amplitude of histogram at index i. Then the average value of H is

$$M_H = \frac{1}{256} \sum_{i=0}^{255} h_i$$

- 4. Absolute value of the histogram deviations from this mean value as follows:  $H_{D_i} = |h_i M_H|$
- 5. Irregular deviation  $I_D$ :  $I_D = \sum_{i=0}^{255} H_{D_i}$

Another similar measure is the deviation from uniform histogram [1]. An ideal image encryption leads to images having uniform histogram distribution. Thus the lower the deviation from uniform histogram (DFUH) is, the higher should be the encryption quality. DFUH is calculated as follows:

• Let  $H_C$  be the histogram of the encrypted image and let  $H_{C_i}$  be the value of the frequency of occurrence at index *i* then the uniform histogram is defined as

$$H_{C_i} = \begin{cases} \frac{M \cdot N}{256} & 0 \le C_i \le 255\\ 0 & otherwise \end{cases}$$

• Deviation from uniform histogram is calculated as follows

$$D_P = \frac{\sum_{C_i=0}^{255} |H_{C_i} - H_C|}{M \cdot N}$$

The Edge Similarity Score was introduced by Mao and Wu [14] and uses localized edge information. The image is divided into blocks and a Sobel edge detection filter is used on each block to find the most prominent edge direction on which the final score calculation is based.

The Luminance Similarity Score was also introduced by Mao and Wu [14] and is based on localized luminosity information. Again the image is divided into blocks, the average luminance of each block is calculated. The final score depends on the per block luminance difference of the blocks and two additional thresholds.

Yao et al. introduced the Neighbourhood Similarity Degree metric [19] which utilizes local pixel similarity correlation. The difference of the centre pixel and its neighbouring pixels inside a window is calculated for each pixel, then the average these pixel differences over the whole image is taken. The final score is the absolute difference between these average values for the reference and the encrypted image.

Sun et al. [17] proposed a metric based on an entropy measure called Local Entropy. The encrypted image is partitioned into blocks. Then the probability of a pixel inside a block is calculated by histogram normalization. Based on this probability the block entropy for each block is calculated and the final score is the average of the block-wise entropy values divided by the log of the maximum pixel.

The Local Feature Based Visual Security metric was introduced by Tong et al. [18] and utilizes localized edge and luminance features which are combined and weighted according to error magnitude. Again the image is divided into blocks at first. For each block the average and standard deviation of the luminance values is calculated and combined to the local luminance feature. For each pixel inside a block the luminance edge direction is determined and a histogram calculated of these edge directions forms the local edge density feature. Final score calculation is based on a weighting of an ordered combination of the local luminance and edge density values.

Yongjie and Wengang [21] proposed a visual security metric based on grey relation analysis (abbreviated as Yongjie10):

- 1. First divide the image into  $32 \times 32$  pixel blocks
- 2. Calculate a grey level histogram for each blocks, divided into 6 bins
- 3. Apply grey relation analysis for each of the histograms
  - (a) Determine the reference sequence  $(X_0)$  and compared sequence  $(X_i)$

$$X_0 = \{X_0(k) | k = 1, 2, ..., n\}$$

$$X_i = \{X_i(k) | k = 1, 2, ..., n\} (i = 1, 2, ..., m)$$

- (b) Calculate the correlation coefficients (*Cor*) between reference sequence and all relative sequences
- (c) Calculate the mean of all correlations

$$\mu = \frac{1}{N} \sum_{k=1}^{n} Cor(k)$$

4. Calculate the average of all correlation factors

Xiongjun Li [12] also proposed an approach based on grey level analysis in combination with information entropy (abbreviated as Li08):

- 1. Create a variance image G with respect to the evaluated image  $F=\{f(i,j)|1\leq i\leq M, 1\leq j\leq N\}$
- 2. Calculate the average of the absolute differences between each pixel and its 8-neighbors pixel by pixel

$$G = \{g(i,j) | 1 \le i \le M, 1 \le j \le N\}$$

$$g(i,j) = \sum_{k=-1}^{1} \sum_{l=-1}^{1} \frac{|f(i,j) - f(i+k,j+l)|}{8}$$

3. Assuming m is the mean of the values in G, s is the standard deviation of the values in G

$$m_f = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{g(i,j)}{M \cdot N} \quad s_f = \sqrt{\frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (g(i,j) - m_f)^2}{(M \cdot N - 1)}}$$

 $m_f$ ,  $s_f$  are less than the grey level range of the image (256 grey levels for a 8 Bit image)

4.  $H_f$  is the general information entropy of the image

$$H_f = -\sum_{l=0}^{L-1} p_f(l) \cdot \log_2(p_f(l))$$

 $p_f(l)$  represents the probability of grey level l. (max. entropy value is 8Bit)

5. The basic scrambling degree measure is

$$B_f = \frac{\frac{H_f}{8} \cdot \frac{m_f}{256}}{\left(\frac{s_f}{256}\right)} = \frac{H_f \cdot m_f}{8 \cdot s_f}$$

Jenisch and Uhl [10] proposed an approach which relies on object recognition based on SIFT, called SIFT Similarity Score. At first the SIFT key points are extracted in both images and then matched against each other, returning an array of matching key points along with their corresponding Euclidean distances. The final score is number of matching key points divided by the maximum possible number of matches, taken to the power of the average Euclidean distance divided by the  $L_2$ -norm of Euclidean matching distances.

# 3. SEGMENTATION BASED SIMILARITY SCORE

Image segmentation describes the process of partitioning an image into multiple segments. This can be regarded as a kind of clustering process. Image segmentation is done for several reasons, including content-based image retrieval, object detection and recognition tasks. There are many different image segmentation approaches [13] from simple thresholding based ones over watershed segmentation to more advanced ones like mean shift segmentation, graph based segmentation and statistical region merging. Advanced image segmentation approaches are robust against noise and other image distortions. Images having similar image content should lead to similar segmentation results. Thus one would assume that also an image and its encrypted versions result in similar segmentation results (depending on the strength of the encryption). This is the main idea behind our proposed visual security metric based on image segmentation.

Simple thresholding based segmentation and watershed segmentation is not suitable for this task as it is too sensitive to noise. We tested a mean shift segmentation approach, a statistical region merging based one and a graph based one and decided to use the graph based segmentation method proposed by Felzenszwalb and Huttenlocher [6] as it lead to the most promising segmentation results. Their graph-based segmentation approach works directly on the data points in the feature space (no filtering is performed). It uses a variation of single-linkage clustering. The traditional singlelinkage clustering works as follows:

- 1. Generate a minimum spanning tree of the data points
- 2. Remove edges with a length greater than a given hard threshold
- 3. Remaining connected components become clusters

Felzenszwalb and Huttenlocher's method uses adaptive thresholding instead of a fixed threshold. For more details the interested reader is referred to their original work [6].

After segmenting the reference and the encrypted image a method to compare the segmentation results is needed. Again there is a bunch of metrics proposed in the literature for this purpose [8, 20, 22]. The simplest ones are set based metrics like the Jaccard Coefficient. They work well for binary segmentations (only foreground and background) but are not suitable for general segmentations with more than 2 resulting image segments as it is not obvious how the two corresponding sets are found. To overcome this problem coefficients based on the confusion matrix are used. In addition there are also methods based on the Hausdorff distance and gradient based coefficients. All these coefficients have one problem in common: they are quite sensitive to refinement (due to oversegmentation). The distortions introduced in the images due to selective encryption lead to oversegmentation especially for higher encryption levels as it can be seen in figure 2. Thus all these coefficients are not appropriate for our visual security metric approach. Huang and Dom [8] presented two measures to evaluate the results of image segmentation which should overcome this problem (i.e. their measures ignore refinement), one that works without a reference image and one that needs a reference image. We decided to use their measure which is designed to work if a reference (ground-truth) image is available. This measure (abbreviated as HD in the following) is based on the Hamming distance and calculated as follows:

$$HD = 1 - \frac{D_H(GT \to S) + D_H(S \to GT)}{2A}$$

where GT is the ground-truth image (reference image in our case), S is the segmented image (encrypted image in our case), A is the area of the image (number of pixels) and  $D_H$ is the Hamming distance defined as follows:

$$D_H(GT \to S) = \sum_i \sum_{j \neq max(i)} |GT_i \cap S_j|$$
$$D_H(S \to GT) = \sum_i \sum_{j \neq max(i)} |S_i \cap GT_j|$$

where  $GT_i$  or  $S_i$  is the *i*-th segment in the ground-truth or segmented image, respectively. The range of HD values is between 0 and 1 where values close to 1 indicate that the segmentation result is close to the ground-truth segmentation result. For our SBSS metric we use the HD value directly and interpret values close to 0 as images having a better visual security and a value of 1 indicates identical images.

### 4. EXPERIMENTAL SETTINGS

To establish a standard of comparison and to show the performance of our SBSS metric in comparison with other metrics we evaluated them on the Berkeley Segmentation Dataset BSDS300<sup>1</sup> [15]. For these images a segmentation ground truth exists and they lead to reasonable results. We use the test image set of the BSDS300 which contains 100 images. The images are true colour images having a resolution of  $481 \times 321$  or  $321 \times 481$  pixels. We convert the images to greyscale which is necessary for the encryption method we use. This encryption method is briefly described below.



Figure 1: Encryption example (left original image, right encrypted image)

### 4.1 Encryption Method

We decided for a format compliant, bitstream oriented JPEG2000 encryption scheme during our evaluations. The encryption is applied to the JPEG2000 compressed data and in order to achieve format compliance only the packet data is encrypted without the headers. The encryption software is based on JJ2000. Encryption is done by replacing the packet data with generated encrypted bytes. Basically, the JPEG2000 packet body data is encrypted in a format compliant manner using the iterative approach proposed in [16]. The encryption level grows with the amount of bytes in the bitstream that are being replaced by encrypted ones [4], starting right after the JPEG2000 main header. This encryption introduces noise-type distortion into the data which kind of overlay the visual information still present in the data. An example can be seen in figure 1. When assessing the security of format compliantly encrypted visual data, the data can simply be decoded with the encrypted parts (called "direct decoding"). Due to format compliance, this is possible with any given decoding scheme.

For the SBSS approach we utilize the efficient graph-based segmentation implementation<sup>2</sup> provided by the authors [6]. We tested different parameters and found out that sigma = 0.5, K = 250 and min = 50 works best. Figure 2 and figure 3 show some encrypted images (starting from unencrypted towards increasing encryption strength) and their corresponding segmentation results for a well working example (contours remain visible in the segmentation results) and a badly working example (contours disappear in the segmentation results), respectively.

#### 4.2 Evaluation Methodology

We evaluated the PSNR, LV, IR, DFUH, Yongjie10, Li08 and our SBSS metric. To reproduce our results or get comparable ones the following procedure should be used:

- Use the test images of the BSDS300 data set including the segmentation ground truth
- Encrypt the images with the approach to be tested
- Segment the encrypted images according to our approach and evaluate the results using the suggested metric described in section 3

#### 5. EXPERIMENTAL RESULTS

The visual security evaluation results for different metrics tested on the BSDS300 images encrypted using our selective encryption can be seen in figure 4. The figure shows the

<sup>&</sup>lt;sup>1</sup>http://www.eecs.berkeley.edu/Research/Projects/CS/ vision/bsds/

<sup>&</sup>lt;sup>2</sup>http://cs.brown.edu/~pff/segment/



Figure 2: Segmentation well working example



**Original Image** 

Encrypt. Level 2 Encrypt. Level 4 Encrypt. Level 13

Figure 3: Segmentation badly working example

average (mean) values over all images. All values in the diagrams are scaled by its maximum value to fit them in the interval [0;1]. The values on the horizontal axis represent the encryption level, where 0 is the uncompressed (original) image, level 1 corresponds to JPEG2000 compression without any encryption and higher values indicate stronger encryption and thus higher visual security.

At lower encryption levels the images do show some resemblance of the original images but with higher encryption levels recognizability and intelligibility of the images decreases as it can be seen in figures 2 and 3. Therefore the desired behaviour of a metric on this set of images would be a monotonically rising or falling curve.

Our proposed metric SBSS shows this desired behaviour as it shows a monotonically falling curve. The slope is steep up to encryption level 6 and gets flatter then which can be explained by the fact that starting from this encryption level only very small parts of the original image remain visible in the encrypted images. Nevertheless there is a continuous decrease up to level 21, i.e. it is able to quantify differences in the encryption strength.

The two quite simple metrics, LV and IR are also able to quantify the difference in encryption levels as IR shows a monotonically falling curve and LV shows a rising curve, but not monotonically though. The curves are not as smooth as the one of SBSS. They also have their steepest slope until encryption level 6. PSNR shows only a flat slope, especially starting from encryption level 6 the values do not change to



Figure 4: Average metric values

Metric/Correlation	Pearson	Spearman	Kendall Tau
PSNR	-0.4419	-0.6657	-0.5103
LV	0.6449	0.6203	0.4939
IR	-0.5858	-0.6554	-0.5047
DFUH	-0.2759	-0.2059	-0.1526
Yongjie10	0.0189	0.0524	0.0397
Li08	0.5709	0.5282	0.3998
SBSS	-0.7936	-0.8441	-0.6822

Table 1: Correlation values for the tested metrics

a considerable extent any longer and thus it is not suitable for visual security evaluation.

DFUH works quite well up to encryption level 6 but then its return values for higher encryption levels are fluctuating and it is thus no longer able to capture the increase in encryption strength correctly.

Li08 shows a nearly monotonically rising curve towards higher encryption levels with a few exceptions at level 4, 8, 11 and 17. It is able to represent the increase in encryption strength to a certain extent but it performs worse than the two much simpler metrics LV and IR.

Yongjie10 is the worst performing metric. It can be clearly seen that its return values are fluctuating across the whole tested range and there is no clear trend towards rising or falling return values with an increasing encryption level. Thus it is unusable for this kind of images in combination with this kind of visual encryption.

To quantify the differences between the tested visual security evaluation metrics we calculated the simple Pearson correlation coefficient, the Spearman rank correlation coefficient and Kendall Tau (Beta) correlation coefficient, measuring the correlation between the metrics' return values and the encryption level. Table 1 shows the average results over all the images in the test set. The results from the visual inspection of the graph in figure 4 is confirmed by the correlation values. Our proposed method, SBSS, clearly shows the highest correlation, followed by the two simple metrics, LV and IR. Li08 performs worse than IR but better than PSNR. The worst performing metrics are DFUH and Yongjie10. Note that we tested these metrics only with one specific selective encryption approach. They might be more suitable for another approach and thus perform better if utilized for visual security evaluation there.

# 6. CONCLUSION

The ability to recognise objects inside encrypted images is an important aspect in visual security evaluation. Our aim was to test if it is possible to detect objects inside the images using image segmentation to assess visual security. Thus we developed a new visual security metric based on image segmentation, SBSS. Our experimental results show that SBSS is well suited for that task. We evaluated our approach on the test images of the BSDS300 dataset which is specifically made for image segmentation (there exists a segmentation ground truth). Our results clearly show that is possible to evaluate the visual security of encrypted images based on image segmentation. Throughout the entire test set used it turned out that SBSS, LV and IR performed best. But it also became apparent that there are always some outliers for which one or several of the metrics did not perform well. It showed that the tested metrics are most reliable for small encryption strengths.

The results presented in this paper are a basis for further research on image segmentation based visual security metrics. Our future work will include tests with different kinds of visual encryption algorithms.

## 7. ACKNOWLEDGMENTS

This work was partially funded by the Austrian Science Fund (FWF), project nr. P27776.

## 8. REFERENCES

- J. Ahmad and F. Ahmed. Efficiency analysis and security evaluation of image encryption schemes. International Journal of Video & Image Processing and Network Security, 12(4):18–31, 2012.
- [2] S.-K. Au Yeung, S. Zhu, and B. Zeng. Quality assessment for a perceptual video encryption system. In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, pages 102–106, June 2010.
- [3] M. V. Droogenbroeck and R. Benedett. Techniques for a selective encryption of uncompressed and compressed images. In *Proceedings of ACIVS* (Advanced Concepts for Intelligent Vision Systems), pages 90–97, Ghent University, Belgium, Sept. 2002.
- [4] F. Dufaux, S. Wee, J. Apostolopoulos, and T. Ebrahimi. JPSEC for secure imaging in JPEG2000. In A. G. Tescher, editor, *Applications of Digital Image Processing XXVII*, volume 5558, pages 319–330. SPIE, Aug. 2004.
- [5] H. M. Elkamchouchi and M. Makar. Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers. In *Radio science* conference, 2005. NRSC 2005. Proceedings of the twenty-second national, pages 277–284. IEEE, 2005.
- [6] P. F. Felzenszwalb and D. P. Huttenlocher. Efficient graph-based image segmentation. Int. J. Comput. Vision, 59(2):167–181, Sept. 2004.
- [7] H. Hofbauer and A. Uhl. Visual quality indices and low quality images. In *IEEE 2nd European Workshop* on Visual Information Processing, pages 171–176, Paris, France, July 2010.
- [8] Q. Huang and B. Dom. Quantitative methods of evaluating image segmentation. In *Image Processing*,

1995. Proceedings., International Conference on, volume 3, pages 53–56. IEEE, 1995.

- [9] S. Jenisch and A. Uhl. A detailed evaluation of format-compliant encryption methods for JPEG XR-compressed images. *EURASIP Journal on Information Security*, 2014(6), 2014.
- [10] S. Jenisch and A. Uhl. Visual security evaluation based on SIFT object recognition. In L. Iliadis et al., editors, *Proceedings of the 10th Artificial Intelligence Applications and Innovations Conference (AIAI* 2014), volume 436 of Springer IFIP AICT, pages 624–633, Rhodes, GR, Sept. 2014.
- [11] M. I. Khan, V. Jeoti, and A. S. Malik. On perceptual encryption: Variants of DCT block scrambling scheme for JPEG compressed images. In T.-H. Kim, S. K. Pal, W. I. Grosky, N. Pissinou, T. K. Shih, and D. Slezak, editors, *FGIT-SIP/MulGraB*, volume 123 of *Communications in Computer and Information Science*, pages 212–223. Springer, 2010.
- [12] X. Li. A new measure of image scrambling degree based on grey level difference and information entropy. In Computational Intelligence and Security, 2008. CIS '08. International Conference on, volume 1, pages 350 -354, dec. 2008.
- [13] L. Luccheseyz and S. Mitray. Color image segmentation: A state-of-the-art survey. Proceedings of the Indian National Science Academy (INSA-A), 67(2):207-221, 2001.
- [14] Y. Mao and M. Wu. Security evaluation for communication-friendly encryption of multimedia. Singapore, Oct. 2004. IEEE Signal Processing Society.
- [15] D. Martin, C. Fowlkes, D. Tal, and J. Malik. A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics. In Proc. 8th Int'l Conf. Computer Vision, volume 2, pages 416–423, July 2001.
- [16] T. Stütz and A. Uhl. On format-compliant iterative encryption of JPEG2000. In *Proceedings of the Eighth IEEE International Symposium on Multimedia* (*ISM'06*), pages 985–990, San Diego, CA, USA, Dec. 2006. IEEE Computer Society.
- [17] J. Sun, Z. Xu, J. Liu, and Y. Yao. An objective visual security assessment for cipher-images based on local entropy. *Multimedia Tools and Applications*, Mar. 2010. online publication.
- [18] L. Tong, F. Dai, Y. Zhang, and J. Li. Visual security evaluation for video encryption. In *Proceedings of the International Conference on Multimedia*, MM '10, pages 835–838, New York, NY, USA, 2010. ACM.
- [19] Y. Yao, Z. Xu, and J. Sun. Visual security assessment for cipher-images based on neighborhood similarity. *Informatica*, 33:69–76, 2009.
- [20] G. L.-E. W. Yong. Evaluation measures for segmentation. *matrix*, 1(1):5.
- [21] T. Yongjie and Z. Wengang. Image scrambling degree evaluation algorithm based on grey relation analysis. In Computational and Information Sciences (ICCIS), 2010 International Conference on, pages 511–514, dec. 2010.
- [22] Y. J. Zhang. A survey on evaluation methods for image segmentation. *Pattern recognition*, 29(8):1335–1346, 1996.