Subjective and Objective Quality Assessment of Transparently Encrypted JPEG2000 Images

Thomas Stutz, Vinod Pankajakshan, Florent Autrusseau, Andreas Uhl, Heinz Hofbauer

Cover Page

1) Title of the paper:

Subjective and Objective Quality Assessment of Transparently Encrypted JPEG2000 Images

2) authors' affiliation and address:

IRCCyN-IVC, (UMR CNRS 6597), Polytech' Nantes
Rue Christian Pauc, La Chantrerie, 44306 NANTES, France.
Tel : 02.40.68.30.52
Fax : 02.40.68.32.32

3) e_mail address:

Florent.Autrusseau@univ-nantes.fr

4) Conference & Publisher information:

ACM Workshop on Multimedia and Security
http://www.mmsec10.com/

5) bibtex entry:

```
@misc{ivcselectencrypt,
  author = {Autrusseau, Florent, and Stutz, Thomas, and
Pankajakshan, Vinod},
  title = {Subjective quality assessment of selective encryption
techniques},
  year = {2010},
  url = {http://www.irccyn.ec-nantes.fr/~autrusse/Databases/
SelectiveEncryption/}
}
```

Subjective and Objective Quality Assessment of Transparently Encrypted JPEG2000 Images

Thomas Stütz
University of Salzburg
Jakob Haringer Str. 2
5020 Salzburg, AUSTRIA
tstuetz@cosy.sbg.ac.at

Vinod Pankajakshan
IRCCyN lab., Polytech'Nantes
Rue Ch. Pauc, BP 50609
44306 Nantes, FRANCE
Vinod.Pankajakshan@univ-nantes.fr

Florent Autrusseau
IRCCyN lab., Polytech'Nantes
Rue Ch. Pauc, BP 50609
44306 Nantes, FRANCE
Florent.Autrusseau@univ-nantes.fr

Andreas Uhl
University of Salzburg
Jakob Haringer Str. 2
5020 Salzburg, AUSTRIA
uhl@cosy.sbg.ac.at

Heinz Hofbauer
University of Salzburg
Jakob Haringer Str. 2
5020 Salzburg, AUSTRIA
hhofbaue@cosy.sbg.ac.at

ABSTRACT

Transparent encryption has two main requirements, i.e. security and perceived quality. The perceptual quality aspect has never been thoroughly investigated. In this work, three variants to transparently encrypt JPEG2000 images are compared from a perceptual quality viewpoint. The assessment is based on subjective and objective quality assessment of the transparently encrypted images and if the requirements with respect to desired functionalities can be met by the respective techniques. In particular, we focus on the question if it is possible to predict the subjective quality of the encrypted (and attacked) images as given by the Mean Opinion Score (MOS) with state-of-the-art objective quality metrics. Additionally, we answer the question which objective quality measure is suited best to determine an image quality for which a certain subjective quality is required.

Categories and Subject Descriptors

I.4.9 [**Computing Methodologies**]: Image Processing and Computer Vision—*Applications*

General Terms

Experimentation, human factors, measurement, performance, security

Keywords

Subjective quality assessment, image quality, image encryption, transparent encryption, JPEG2000

MM&Sec'10, September 9–10, 2010, Roma, Italy.

1. INTRODUCTION

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the application requirements for a particular multimedia environment [1]. In the context of multimedia applications, encryption commonly has a different aim as opposed to full confidentiality and privacy. One well-known example is the application scenario of transparent encryption. Authors in [2] introduce the term "transparent encryption" in the context of digital TV broadcasting: a broadcaster of pay TV does not always intend to prevent unauthorized viewers from receiving and watching their program, but rather intends to promote a contract with nonpaying watchers. Therefore, two major requirements have to be met concurrently:

- Prevention of access to a high quality image (security requirement).
- Enabling access to a low quality image (quality requirement).

The first requirement states that an adversary shall not be able to compute a reconstruction with a higher quality than targeted. The second requirement, namely to explicitly demand a certain image quality, is completely different from scenarios where confidentiality or privacy are the primary aims. These requirements can be facilitated by providing a low quality version of the broadcast program for everyone, only legitimate (paying) users get access to the full quality visual data. This is also what is meant by the term "try and buy" scenario. Also in image databases, the availability of a thumbnail is of advantage as an incentive for buying the full-quality version. A similar application scenario is "sufficient encryption"; here the aim is to sufficiently reduce the quality of the content, such that all of its business value is lost. Thus sufficient encryption is relevant in the context of commercial content distribution as well.

The integration of multimedia encryption into standardized multimedia formats (such as JPEG2000) in a format-compliant way has the great benefit that the deployment costs are greatly reduced. Format-compliant encryption guarantees that the encrypted multimedia file still complies with

the format specifications, therefore operations that can be performed on the JPEG2000 stream can also be transparently conducted on the encrypted stream. Consequently, format-compliant encryption can be easily integrated into existing media distribution frameworks. Concerning the application scenario of transparent encryption and sufficient encryption, the property of format-compliance preservation is beneficial as the entire distribution chain can remain unchanged and the potential customers obtain the promotional low quality versions in exactly the same way as usual.

For the application scenarios of transparent and sufficient encryption, the notion of security is based on quality, i.e., the security goal is to prevent an attacker from computing a "high quality" reconstruction of the original content. Thus quality is the key-defining property in the definition of security, but it has not yet been investigated whether quality in the context of transparent/perceptual encryption can be effectively determined. There are two alternative ways of assessing the perceived quality of digital images, one can either run a subjective experiment, where human observers are asked to judge the quality of displayed images, or use specific algorithms (named Objective Quality Metrics and abbreviated OQM in the following) in order to predict the scores given by the observers. Subjective experiments are time consuming and require a very specific setup [3]. Thus, in order to avoid running tedious subjective tests, many OQMs have been proposed during the last few decades. However, designing an efficient objective quality metric is complex and OQMs may have a different behavior when tested on different kind of distortions. When using an OQM for a given type of artifact (coding, watermarking, encryption...) it is crucial to evaluate the ability of the metric to accurately predict the subjective scores for the specific distortion. The distortion introduced by multimedia encryption schemes has not yet been evaluated or discussed, neither for JPEG2000 encryption nor for any other scheme (at least as far as the authors are aware of). It is thus interesting to investigate whether the state-of-the-art OQMs are suitable for assessing the distortions introduced by transparent encryption. Furthermore, unlike the conventional usage of OQM to predict the score provided by human observers, an important need for a transparent encryption framework is to use OQMs for a quality threshold detection scenario, i.e., being able to determine if the perceived quality of a given distorted image is above/below a quality target. This ability is of great importance in a transparent encryption scenario, as a quality level is required in order to distribute properly encrypted images.

The rest of the paper is organized as follows. Section 2 gives an overview of JPEG2000 encryption schemes, with a focus on transparent encryption. The subjective and objective quality assessments are briefly summarized in section 3. The experimental setup is described in section 4, detailed analysis of results is presented in section 5 and finally section 6 concludes the paper.

2. TRANSPARENT JPEG2000 ENCRYPTION

The application scenario of transparent encryption requires the availability of a low quality public version and the protection of the high quality version of the content. We distinguish two cases; in the first case format-compliant encryption enables the fully transparent implementation of transparent encryption and in the second, additional measures need to be taken to signal the public low quality version and the encrypted data; specific file formats can be used for that end, e.g., in the case of JPEG2000 the application of JPSEC [4] would be obvious.

In this work three JPEG2000 transparent encryption scenarios are considered.

2.1 Traditional Approach

The traditional approach to implement transparent encryption on-top of a scalable bitstream is to encrypt all the enhancement layers [5]. In the case of JPEG2000 this approach is straightforward: in the compressed JPEG2000 file the position at which the desired low quality is achieved is determined and all the successive packet body data in the file (enhancement layers) are encrypted.

However, the encrypted portions introduce distortion in the image, which can be removed by an attacker. As all enhancement layers are encrypted, an optimal adversary strategy is to remove all the encrypted data, i.e., truncate the codestream at the start of encryption.

2.2 Window Encryption Approach

The window encryption approach is an umbrella term for all schemes that format-compliantly encrypt only a fraction of the packet body data at a certain position in the file [5]. The main advantages are firstly that the encrypted portion can be efficiently signalled with JPEG2000 error concealment tools and secondly the reduced encryption effort.

As only a small fraction of the codestream is encrypted, the encrypted parts can be effectively signalled by taking advantage of the JPEG2000 error concealment options [5]. Thus a decoder, taking benefit of the error concealment information, produces the same quality reconstruction as an adversary trying to conceal the encrypted portions of the codestream. Given the current state-of-the-art this error-concealment attack is the best known attack [5].

2.3 Wavelet Packets

The application of secret wavelet packet bases for encryption has been proposed in [6] and specifically discussed for JPEG2000 [7]. Transparent encryption can be implemented with secret wavelet packet bases by stopping the further decomposition of the approximation subband at a certain depth (and correspondingly at a certain resolution). The image can be reconstructed on the basis of the LL coefficients at the corresponding resolution.

Given the current state-of-the-art the approximation subband is the best quality an attacker can achieve.

3. PERCEPTUAL QUALITY ASSESSMENT

As previously explained, image quality assessment may be performed either during a subjective experiment, or using objective quality metrics. On one hand, subjective experiments involves human observers who will rate the perceived quality of the displayed images. For a given distorted image, the scores provided by the observers are averaged to form the Mean Opinion Score (MOS). On the other hand, OQMs are computational models predicting the perceived quality. They can be classified into two main categories, the statistical metrics (such as the PSNR) basically checks for either local or global statistical differences between two images, whereas advanced OQMs take into account some Human Visual System properties for computing a predicted MOS

(named MOSP). Several human visual properties are commonly considered: spatial frequency sensitivity, luminance level, masking or facilitation effects.

Although a large number of OQMs exist in the literature, they may exhibit varying levels of performances when tested on different subjective datasets. The Video Quality Experts Group (VQEG) issued some recommendations [8] to assess the efficiency of the objective quality metrics. The most commonly used tool to evaluate the efficiency of a given OQM is the correlation coefficient between the MOS and the MOSP. A high correlation ensures that the metric can accurately predict the observers scores. However the correlation may not be sufficient in all cases. The outlier ratio or RMSE can be also used to ensure that the metric's prediction (MOSP) form a narrow MOS versus MOSP distribution. Apart from the quality assessment task, OQM can also be used for a (in-)visibility threshold detection. In such a framework, the most important feature required from the metrics would be to present a very compact MOS versus MOSP distribution near the target MOS threshold.

4. EXPERIMENTAL SETUP

In this section, we first describe the transparent encryption image database which has been used, as well as the subjective experiment setup and we briefly mention the OQMs which will be tested for benchmarking (see sect. 5.2).

4.1 Subjective Data Set

The image test set contains five different distortion types, i.e., encryption schemes and corresponding attacks at five different quality levels, i.e., different parameter settings. The different distortion types are traditional encryption (trad), truncation of the codestream (trunc), window encryption and no error concealment (iwind_nec), window encryption with error concealment (iwind_ec), and wavelet packet encryption (res). The images have been compressed with JJ2000 default parameters (version 5.1), which include layer progression, the application of the 9/7 reversible filter and no rate limitation. The start of encryption has been 1%, 7%, 14%, 21%, and 29% for the distortion types, trad, trunc, iwind_nec, and iwind_ec. A window with a size of 1% of the overall codestream length has been encrypted at different positions in the codestream (iwind_nec and iwind_ec). A format-compliant packet body encryption algorithm [9] has been employed. For wavelet packet encryption the decomposition depth of the approximation subband has been 1 (res-4), 2 (res-3), 3 (res-2), 4 (res-1), and 5 (res-0).

The image data set is generated from 8 gray-scale input images of size 720×480 pixels. Each image is encrypted using the 5 different methods with 5 different parameter settings, thereby generating 200 distorted images[1].

4.2 Subjective and Objective quality assessment

The subjective experiment was conducted in normalized viewing conditions following the ITU recommendations R BT.500-11 [3]. A standard double stimulus impairment scale (DSIS) protocol was used for the subjective test. Both the original and distorted images were displayed side-by-side on an monitor and the viewing distance was set to 6 times the image height. The viewing monitor had respectively 0.26 and 213 Cd/m^2 minimum and maximum Luminance, with a 1920x1200 resolution. The original and distorted images were respectively displayed on the left and right side of the screen. These locations were known to the observers, who were asked to rate the quality of the distorted image (with respect to the original) in a 5 point scale: 1 - "very annoying", 2 - "annoying", 3 - "slightly annoying", 4 - "perceptible but not annoying" and 5 - "imperceptible" distortions.

Twenty one observers were enrolled and were screened for correct vision before running the test. Every session ran for about 20 minutes. The display sequence for the 200 test images was randomized, this process is typically used in order to avoid displaying the same images at the end of the test, when the observers' attention tend to be reduced.

Fifteen objective quality metrics were tested on the subjective data set. This includes the 12 OQMs included in the 'MeTriX MuX' package[2] and, in addition to these, we used the ESS and LSS metrics [10], which have been specifically designed for security evaluation of encrypted data. Finally, we also considered a modified version of the CPA [11], an HVS-based OQM proposed recently for evaluating the quality of watermarked images. The CPA metric was modified by incorporating the contrast masking property of the HVS, implemented as a threshold elevation step after a perceptual subband decomposition.

5. EVALUATION AND ANALYSIS

5.1 Transparent JPEG2000 Encryption Schemes

In the following we give a precise definition of the presented statistics, which are employed in the assessment of the transparent JPEG2000 encryption schemes. Let o_i^s be the subjective score for an image i of subject s. Let $\mathcal{I}_m$ be the set of images obtained with a distinct encryption algorithm and set of parameters denoted by m. AVG and SD determine the average and empirical standard deviation.

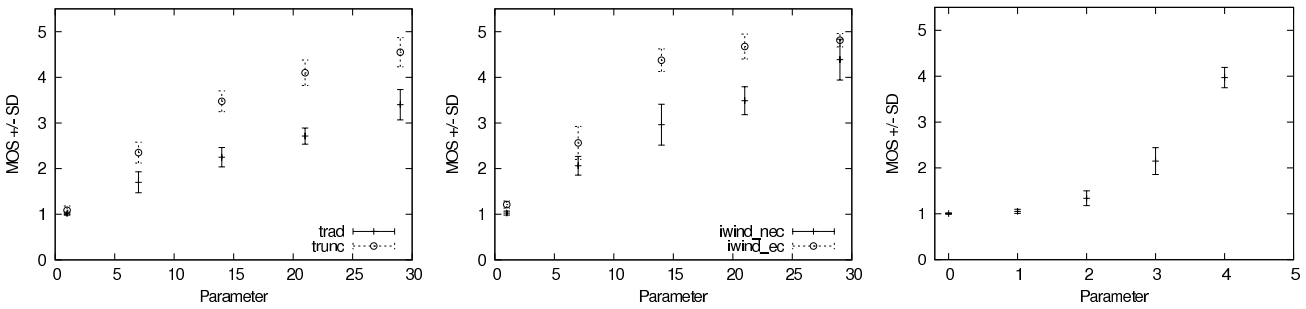
$$MOS(i) = \mathrm{AVG}_{s \in \mathcal{S}}(o_i^s)$$
$$A\_MOS_m = \mathrm{AVG}_{i \in \mathcal{I}_m}(MOS(i))$$
$$SD\_MOS_m = \mathrm{SD}_{i \in \mathcal{I}_m}(MOS(i))$$

Are the encryption algorithms configurable and which subjective quality can be achieved?

All the encryption algorithms are capable to produce severe to almost imperceptible distortions, although not all qualities are achieved with the evaluated parameters of encryption for all algorithms (truncation gives the best distribution of qualities for the evaluated parameters). The wavelet packet encryption approach has the drawback that it is already evaluated with the finest possible granularity, but there is an enormous quality gain from res-3 (approximation subband of depth 2) to res-4 (approximation subband of depth 3) of almost two MOS points. The other algorithms can be adjusted at much finer granularity. The relationship between encryption parameter and perceived quality is further illustrated in figure 1 where the A_MOS and SD_MOS are plotted for a varying encryption parameter. Encryption schemes and corresponding attacks are grouped together.

[1] `http://www.irccyn.ec-nantes.fr/~autrusse/Databases/SelectiveEncryption/`

[2] `http://foulard.ece.cornell.edu/gaubatz/metrix_mux/`



(a) "trad" and "trunc" encryption (b) Window encryption (c) Wavelet packet encryption ("res")

Figure 1: Plot of mean opinion score and standard deviation in dependency of the encryption parameter.

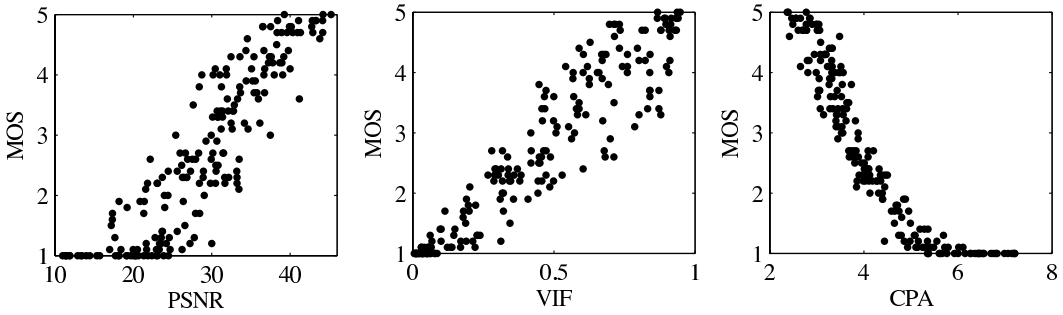


Figure 2: MOS vs. MOSP plots for selected OQMs.

Which application scenarios can be met?

As previously discussed, the application scenario of sufficient encryption can be met by all. All algorithms, except wavelet packet encryption, can be adjusted to a finer granularity than evaluated. If the plaintext portion of the JPEG2000 codestream is explicitly signalled (format-compliance of the entire encrypted codestream is not required), the traditional approach is equivalent to truncation and the proposed method to determine the truncation points performs well. However, if fully transparent application is targeted, the gap between the direct reconstruction of the traditional approach and truncation is considerable (up to 1.4 MOS points, figure 1(a)), i.e., the noise introduced by encrypted data, which can be efficiently removed, is severe. For the window encryption approach without error concealment it is also advised to signal the preceding plaintext portion, as the truncation yields superior MOS results compared to the direct reconstruction of the format-compliant encrypted codestream. However, the scheme without error concealment is susceptible to an attack, which obtains the same results as the window encryption approach with error concealment. This attack efficiently removes the noise introduced by encryption, which is reflected by significant MOS improvements (up to 1.42 MOS points, figure 1(b)). However, the improvements are far less pronounced in the low-quality range (at a MOS of ≈ 1 the improvement is only 0.178 MOS points). Thus for medium to high quality the transparent application of the window encryption approach without error concealment is not advisable, while for low quality it can be employed (MOS ≈ 1). For the window encryption approach with error concealment the explicit signalling of the leading plaintext data is not recommended, as the error concealed reconstruction results in higher MOS values. The window encryption approach with error concealment is optimally suited for transparent application, as the best known attack is the same as the concealed reconstruction (only available if the decoder is able to perform error concealment). The granularity of the encryption is limited to the adjustment of the decomposition depth of the approximation subband, which results in a MOS gap of ≈ 2 and ≈ 4.

Which encryption algorithm performs best?

If explicit signalling of the plaintext data is employed the traditional approach is recommended. The selection of the start of encryption relative to uncompressed codestream delivers quite consistent MOS results (considering different images). The window encryption approach with error concealment is the only approach which can be recommended for the application in a fully transparent fashion (no signalling of the encrypted data).

5.2 Objective Quality Metrics

Although 15 OQMs were tested, due to space limitation we only present the results for 8 OQMs, including the best performing metrics and the most commonly used (PSNR and SSIM) ones. Figure 2 shows the MOS versus MOSP plot for three selected OQMs. The effectiveness of an OQM in predicting the subjective quality is indicated by a narrow and compact distribution of points in the MOS-MOSP plot. The performance of the OQMs are evaluated using standard measures: the root mean square error (RMSE), outlier ratio (OR), linear correlation coefficient (CC) measuring the prediction accuracy, and the Spearman rank-ordered correlation coefficient (SROCC), measuring the monotonicity.

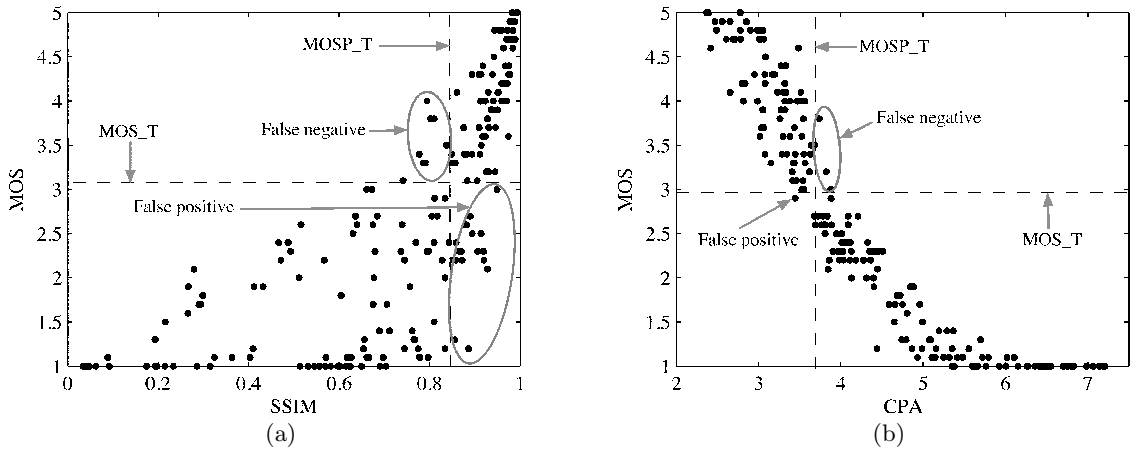


Figure 3: Threshold selection on MOSP

Efficient OQMs are characterized by low RMSE and outlier ratio and high correlations. Before comparing the OQM performances, the MOSP given by each OQM need to be mapped into the range of MOS values [8]. A least-square fitting function was used for mapping the MOSP values. Among the 8 selected metrics, 4 were mostly designed and tested for coding distortions (SSIM, MSSIM, VSNR and VIF), two were specifically designed for encryption artifacts (LSS and ESS), one was mostly tested in a watermarking framework (CPA), and finally, the PSNR is commonly used on any kind of distortion. The SSIM, ESS, and MSSIM metrics provide a MOSP in the range $[0, 1]$, VIF was designed to predict slight quality enhancements (slightly above 1). The CPA metric does not have any strictly defined boundaries (as for the PSNR). An important observation for the CPA metric is the reversed MOSP distribution. Effectively unlike others, CPA does not provide a similarity measurement, but rather a measure of the differences between images. Thus, the higher is the CPA score, the lower is the image quality. Among the 15 tested metrics, except VSNR and CPA, all metrics are statistical metrics. The Visual Signal to Noise Ratio (VSNR) is based on near-threshold and suprathreshold properties of human vision, and the modified CPA metric tested here uses a perceptual sub-band decomposition and models both contrast masking and threshold elevation.

Which objective quality metric performs best?

From the results given in table 1, it is clear that the SSIM presents the worst performance among the selected OQMs whereas the CPA presents the best performance for all measures. The wide distribution of points in the MOS-MOSP plot of the SSIM is reflected by the high RMSE and Outlier ratio. The PSNR on the other hand performs better than the SSIM but still has significant RMSE and outlier ratio. Besides the CPA metric, VIF also has reasonable performance in predicting the subjective scores.

Which metric is best suited in a quality threshold detection scenario?

As mentioned in section 1, in a practical scenario it is desirable to know whether the quality of an encrypted image is above or below a particular MOS. For instance, a content provider would like to make sure that the encrypted image is not of high visual quality and at the same time it has an acceptable quality. A straightforward way is to set a threshold on the MOSP value such that a MOSP value above/below the threshold detects the image as having a desired quality in terms of the MOS. However, from the spread of MOS-MOSP plots given in figure 2, it is evident that such a detection based on the MOSP threshold will result in some error. For example, consider the MOS-MOSP plot for SSIM shown if figure 3(a). If we consider a target MOS value (MOS_T) of 3, whatever threshold we choose for the MOSP value (MOSP_T), there will be some false positive detection where the MOS value is less than the target but the MOSP value greater than the threshold on SSIM. Similarly, for some images the MOSP values indicate low visual quality while the MOS is above the target value, resulting in false negative detection. Note that due to the negative slope of the MOS-MOSP plot in figure 3(b), an image is detected as having quality above the target MOS value if the corresponding MOSP is less than MOSP_T and vice versa.

Metric	RMSE	OR	CC	SROCC
PSNR	0.555	0.460	0.909	0.912
SSIM	0.730	0.640	0.840	0.869
MSSIM	0.634	0.485	0.901	0.952
VSNR	0.540	0.445	0.914	0.918
VIF	0.459	0.345	0.939	0.940
CPA	0.372	0.300	0.961	0.970
ESS	0.53	0.400	0.912	0.93
LSS	0.54	0.400	0.914	0.927

Table 1: Comparative performance of OQMs

In order to find the best OQM for the threshold-based detection, we consider the following threshold selection method[3]. Let $MOS(i)$ and $MOSP(i)$ be the MOS value and the predicted MOS value corresponding to the i^{th} image, where $i = 1, 2, \cdots, N$. Consider a target MOS value, MOS_T and

[3]This method is for the OQMs with a positive slope in the MOS-MOSP plot

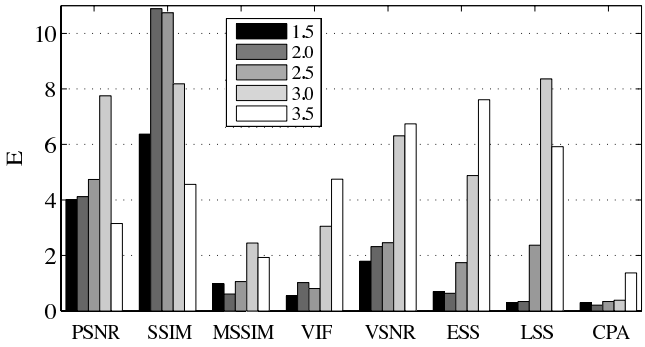


Figure 4: Detection performance of OQMs for different target MOS values

let T be a threshold on the MOSP such that:

$$\begin{aligned}
\mathcal{I}_{\mathrm{TP}}^{T} &= \{i \mid MOS(i) \geqslant MOS_T \text{ and } MOSP(i) \geqslant T\} \\
\mathcal{I}_{\mathrm{TN}}^{T} &= \{i \mid MOS(i) < MOS_T \text{ and } MOSP(i) < T\} \\
\mathcal{I}_{\mathrm{FP}}^{T} &= \{i \mid MOS(i) < MOS_T \text{ and } MOSP(i) \geqslant T\} \\
\mathcal{I}_{\mathrm{FN}}^{T} &= \{i \mid MOS(i) \geqslant MOS_T \text{ and } MOSP(i) < T\}
\end{aligned}$$

are the index sets corresponding to the true positive, true negative, false positive and false negative detections, respectively. The important factor which needs to be considered while choosing an optimal threshold is not the number of false positive and false negative detection, but the significance of wrong detection. So we consider detection error corresponding to the threshold T, defined as:

$$E(T) = \sum_{i \in (\mathcal{I}_{\mathrm{FP}}^{T} \bigcup \mathcal{I}_{\mathrm{FN}}^{T})} \mid MOS(i) - MOS\_T \mid^2 \qquad (1)$$

such that the farther the MOS value corresponding to a wrong detection from MOS_T , the more impact it has on the error. The optimal threshold $MOSP\_T$ is given by:

$$MOSP\_T = \underset{T}{\operatorname{argmin}}\, E(T) \ . \qquad (2)$$

Note that MOSP_T is optimal in the sense that it minimizes the error function (Eq. 1) and it is possible to use a different error function to get a different threshold. The detection performance of selected OQMs at the optimal thresholds corresponding to different target MOS values ($MOS\_T = 1.5, 2.0, 2.5, 3.0, 3.5$) is shown in figure 4. It can be observed that the commonly used metrics like PSNR and SSIM results in significant errors. The CPA and MSSIM metrics give the best performance for all the considered target MOS values.

6. CONCLUSIONS AND OUTLOOK

A subjective experiment was conducted on a set of transparently encrypted JPEG2000 images and the performances of state-of-the-art OQMs were evaluated. The goal of this work was to evaluate the perceptual quality of 3 selected transparent encryption techniques. Based of the subjective test analysis we conclude that all three variants for transparent encryption are suitable for sufficient encryption (severe quality reduction). Only the window encryption approach with error concealment meets all the requirements of transparent encryption. If the encrypted parts are signalled, the other variants are applicable as well. The evaluation of state-of-the-art OQMs shows that CPA and VIF are the best performing metrics in a quality assessment framework, whereas in a threshold selection scenario, the CPA and MSSIM metrics performs best.

7. REFERENCES

[1] A. Uhl and A. Pommer. *Image and Video Encryption. From Digital Rights Management to Secured Personal Communication*, volume 15 of *Advances in Information Security*. Springer-Verlag, 2005.

[2] B. M. Macq and J-J. Quisquater. Cryptology for digital TV broadcasting. *Proceedings of the IEEE*, 83(6):944–957, June 1995.

[3] ITU-R-BT.500-11. Methodology for the subjective assessment of the quality of television pictures question itu-r 211/11, g. Technical report, Intl Telecom. Union, 2004.

[4] ISO/IEC 15444-8. Information technology – JPEG2000 image coding system, Part 8: Secure JPEG2000, April 2007.

[5] T. Stütz and A. Uhl. On efficient transparent JPEG2000 encryption. In *Pro. of ACM Multimedia and Security Workshop, MM-SEC '07*, pages 97–108, New York, NY, USA, September 2007. ACM Press.

[6] A. Pommer and A. Uhl. Selective encryption of wavelet-packet encoded image data — efficiency and security. *ACM Multimedia Systems (Special issue on Multimedia Security)*, 9(3):279–287, 2003.

[7] D. Engel and A. Uhl. Secret wavelet packet decompositions for JPEG2000 lightweight encryption. In *Intl. Conf. on Acoustics, Speech, and Signal Processing, ICASSP*, volume V, pages 465–468, 2006.

[8] VQEG MM. Final report from the video quality experts group on the validation of objective models of multimedia quality assessment, 2008.

[9] H. Wu and D. Ma. Efficient and secure encryption schemes for JPEG2000. In *Proc. of the 2004 Intl. Conf. on Acoustics, Speech and Signal Processing (ICASSP 2004)*, pages 869–872, May 2004.

[10] Y. Mao and M. Wu. A joint signal processing and cryptographic approach to multimedia encryption. *IEEE Transactions on Image Processing*, 15(7):2061–2075, July 2006.

[11] M. Carosi, V. Pankajakshan, and F. Autrusseau. Toward a simplified perceptual quality metric for watermarking applications. In *Proc. of the SPIE conf. on Electronic Imaging*, volume 7542, San Jose, CA, USA, January 2010. SPIE.