Contribution of Non-scrambled Chroma Information in Privacy-Protected Face Images to Privacy Leakage

Hosik Sohn[1], Dohyoung Lee[2], Wesley De Neve[1],
Konstantinos N. Plataniotis[2], and Yong Man Ro[1]

[1] Image and Video Systems Lab, Department of Electrical Engineering,
Korea Advanced Institute of Science and Technology
{sohnhosik,wesley.deneve}@kaist.ac.kr, ymro@ee.kaist.ac.kr
[2] Multimedia Lab, The Edward S. Rogers Sr.,
Department of Electrical and Computer Engineering, University of Toronto
dohyoung.lee@utoronto.ca, kostas@comm.utoronto.ca

Abstract. To mitigate privacy concerns, scrambling can be used to conceal face regions present in surveillance video content. Given that lightweight scrambling tools may not protect chroma information in order to limit bit rate overhead in heterogeneous usage environments, this paper investigates how the presence of non-scrambled chroma information in face regions influences the effectiveness of automatic and human face recognition (FR). To that end, we apply three automatic FR techniques to face images that have been privacy-protected by means of a layered scrambling technique developed for Motion JPEG XR, testing the effectiveness of automatic FR and layered scrambling using various experimental conditions. In addition, we investigate whether agreement exists between the judgments of 32 human observers and the output of automatic FR. Our experimental results demonstrate that human observers are not able to successfully recognize face images when simultaneously visualizing scrambled luma and non-scrambled chroma information. However, when an adversary has access to the coded bit stream structure, the presence of non-scrambled chroma information may significantly contribute to privacy leakage. By additionally applying layered scrambling to chroma information, our experimental results show that the amount of privacy leakage can be substantially decreased at the cost of an increase in bit rate overhead, and with the increase in bit rate overhead dependent on the number of scalability layers used.

Keywords: Chroma information, face recognition, Motion JPEG XR, privacy protection, scalability, scrambling, video surveillance.

1 Introduction

Present-day video surveillance systems often come with high-quality video capture capabilities and plenty of computational resources, making it possible to detect and recognize human faces with increasing rates of success. This ability has recently raised privacy concerns [1]. To mitigate these privacy concerns, scrambling can be

Y.Q. Shi, H.J. Kim, and F. Perez-Gonzalez (Eds.): IWDW 2011, LNCS 7128, pp. 453–467, 2012.

leveraged to conceal the identity of face images in video content originating from surveillance cameras.

The past few years have witnessed the development of a wide range of content-based tools for protecting privacy in video surveillance systems. The authors of [2] propose two scrambling techniques to conceal regions-of-interest (ROIs) in video sequences compliant with MPEG-4 Visual: a transform-domain technique that pseudo-randomly flips the sign of selected transform coefficients and a codestream-domain technique that inverts selected bits of codewords in a compressed bit stream. Descrambling privacy-protected ROIs can only be done by authorized users (*i.e.*, users in possession of a secret key), thus ensuring privacy preservation. To hide identity revealing features (e.g., faces or vehicle tags), the authors of [3] propose and evaluate a format-independent encryption scheme that randomly permutes pixel values in each macroblock before compression. The permutation-based encryption scheme tolerates lossy compression and is also robust to transcoding (without requiring access to secret keys). In [4], we introduce a layered scrambling technique that aims at concealing the identity of face images in video sequences scalably encoded with Motion JPEG XR. To that end, we make use of Random Sign Inversion (RSI), Random Permutation (RP), and Random Level Shift (RLS) to scramble the different types of luma subbands that make up face regions. Also, in [5], we present a video surveillance system that makes use of the Scalable Video Coding (SVC) extension of H.264/AVC. To ensure privacy protection, we detect face regions and scramble these regions by means of RSI, making use of a different secret key for each layer in the SVC bit stream. Finally, it is worth mentioning that the authors of [6] introduce a framework for joint encryption and compression for the purpose of content access control. To that end, video data are modified in the frequency domain by means of selective bit scrambling, block shuffling, and block rotation of the transform coefficients and motion vectors.

In general, content-based tools for privacy protection alter the visual information present in privacy-sensitive regions. However, altering visual information typically breaks the effectiveness of coding tools such as entropy coding, thus leading to bit rate overhead. Consequently, content-based tools for privacy protection need to find a proper balance between the level of security offered on the one hand and the amount of bit rate overhead on the other hand. As a result, to limit bit rate overhead, content-based tools for privacy protection may only scramble luma information, leaving chroma information unprotected [4, 7-11].

In this paper, we study and quantify the influence of the presence of non-scrambled chroma information on the effectiveness of automatic and human FR. To that end, following the objective evaluation methodology of [12], we apply three automatic FR techniques to face images that have been privacy-protected in the luma domain by means of a layered scrambling technique developed for Motion JPEG XR [4], testing the effectiveness of automatic FR and layered scrambling using various experimental conditions. In addition, we extend the objective evaluation methodology of [12] in order to investigate whether agreement exists between the judgments of 32 human observers and the output of automatic FR. Note that the objective evaluation methodology of [12] was not available yet at the time of designing and testing the layered scrambling technique for Motion JPEG XR presented in [4].

Note that, besides FR, perception-based security metrics such as Luminance Similarity Score (LSS) and Edge Similarity Score (ESS) can be used to assess the level of privacy protection offered by scrambling [13], as well as more advanced visual security metrics (e.g., the metric outlined in [7], making use of local features). However, these metrics are general in nature and are thus not able to take advantage of domain-specific information (e.g., face information). As a result, these general security metrics may overestimate the level of protection offered by privacy-preserving tools. Therefore, when a privacy-threatening tool such as (automatic) FR can be applied, we believe it is better to make use of face recognition rates in order to assess the level of protection offered by a particular tool for privacy protection.

Our experiments demonstrate that human observers are not able to successfully recognize face images when simultaneously visualizing scrambled luma and non-scrambled chroma information. However, when an adversary has access to the coded bit stream structure, the presence of non-scrambled chroma information may significantly contribute to privacy leakage. By additionally applying layered scrambling to chroma information, our experiments show that the amount of privacy leakage can be substantially decreased at the cost of an increase in bit rate overhead, and with the increase in bit rate overhead dependent on the number of scalability layers used.

This paper is organized as follows. In Section 2, we briefly review layered scrambling for Motion JPEG XR. In Section 3, we describe our experimental setup. We subsequently present and discuss experimental results in Section 4. In Section 5, we detail the costs and benefits of layered scrambling of chroma information. Finally, we provide concluding remarks and directions for future research in Section 6.

2 Layered Scrambling for Motion JPEG XR

The video surveillance system studied in this paper makes use of Motion JPEG XR to encode video content captured by surveillance cameras. Motion JPEG XR offers a low-complexity solution for the intra coding of high-resolution video content, while at the same time offering quality and scalability provisions that are similar to the quality and scalability provisions of Motion JPEG 2000 and the Scalable High Intra Profile of H.264/AVC SVC [14-15]. The aforementioned features allow designing video surveillance systems that are able to facilitate real-time monitoring in diverse usage environments, ranging from desktop PCs connected to a wired network to mobile devices connected to a wireless network.

In [4], to facilitate privacy protection, we apply a layered scrambling technique to the luma subbands that make up face regions [4]. Specifically, we apply RLS, RP, and RSI to the DC, LP, and HP luma subbands of face regions, respectively. That way, it is possible to trade-off the visual importance of subbands against the amount of coded data in the subbands, the level of security offered by a particular scrambling tool, the impact of a particular scrambling tool on the coding efficiency, and the computational complexity of a particular scrambling tool. For more details regarding layered scrambling for Motion JPEG XR, we would like to refer the reader to [4]. Note that the layered scrambling technique under consideration can be applied to any coding format that allows organizing its transform coefficients in subbands (layered scrambling in H.264/AVC could for instance be realized by taking advantage of data partitioning).

3 Experimental Setup

To construct sets of training, gallery, and probe face images, we collected 3070 frontal face images of 68 subjects from the 'talking' image set of CMU PIE [16]. This resulted in the use of 68 gallery, 340 training, and 2662 probe face images. Further, assuming that an adversary does not have access to an implementation of layered scrambling for Motion JPEG XR, we only scrambled the probe face images. Consequently, the probe face images represent privacy-protected face images that appear in video content originating from surveillance cameras.

To encode face images, we inherited the settings previously used in [4] for the "ATM" video sequence [17]. This implies that we encoded face images with a spatial resolution of 192×192 and with a quantization parameter (QP) value set to 20.

To investigate the privacy-preserving nature of layered scrambling for Motion JPEG XR, we made use of the following automatic FR techniques: Principal Component Analysis (PCA) [18] and Fisher's Linear Discriminant Analysis (FLDA) [19], which both make use of global features, and Local Binary Patterns (LBP) [20], which makes use of local features. When using PCA- and FLDA-based FR, we followed the recommendations made by the FERET protocol to normalize face images [21]. When using LBP-based FR, we followed the preprocessing method of [20]. Also, when using LBP-based FR, we sampled eight binary patterns on a circle of radius two for each 16×16 region. Further, we applied layered scrambling after geometrical alignment, assuming that face detection is accurate and that eye coordinates are known.

We plotted FR results on a Cumulative Match Characteristic (CMC) curve [21]. To facilitate a fair comparison, we adopted the best found correct recognition rate (BstCRR) for PCA- and FLDA-based FR [22]. BstCRR reports the highest true positive recognition rate by means of an exhaustive search, varying the dimension of the feature vectors. On the other hand, we obtained the recognition rate for LBP-based FR for feature vectors with a maximum dimensionality of 8496 (the 144 blocks are represented by 59 features each).

Besides objective assessments, we also conducted subjective assessments with 32 human observers. For each of the experimental settings used, we presented three scrambled probe face images of different subjects to the human observers. Given a probe face image and a set of twelve gallery face images, we subsequently asked the human observers to select the gallery face image that is most similar to the given probe face image. The human observers were also able to indicate that a suitable match could not be found. Further, we allowed the human observers to study the probe face images at different zoom levels. In addition, we enhanced the contrast of the probe face images. This reflects a real-world scenario in which an attacker has complete control over the scrambled probe face images.

4 Assessment of Chroma-Induced Privacy Leakage

In this section, we present our objective and subjective assessments, studying and quantifying privacy leakage induced by the presence of non-scrambled chroma information in face images.

4.1 Notations

Table 1 introduces a number of notations used throughout the remainder of this paper. *DC*, *LP*, and *HP* denote a DC, LP, and HP subband, respectively. A first subscript is used to denote the incremental use of several subbands. Specifically, S_1, S_2, and S_3 represent the use of *DC*, *DC+LP*, and *DC+LP+HP*, respectively. A second subscript is used to denote the presence of luma and/or chroma channels. Finally, a prime is used to indicate the use of scrambling. As an overall example, $S'_{3,Y}$ indicates that the DC, LP, and HP subbands of the luma channel have been scrambled: $S'_{3,Y} = DC'_Y + LP'_Y + HP'_Y$.

Table 1. Summary of notations used

Notation	**Explanation**
DC, LP, and *HP*	DC, LP, and HP subband
S_3, S_2, and S_1	*DC+LP+HP, DC+LP,* and *DC*
Subscripts (Y, Co, and Cg)	Luma and chroma channels (Y, Co, and Cg)
Prime (′)	Scrambled image data

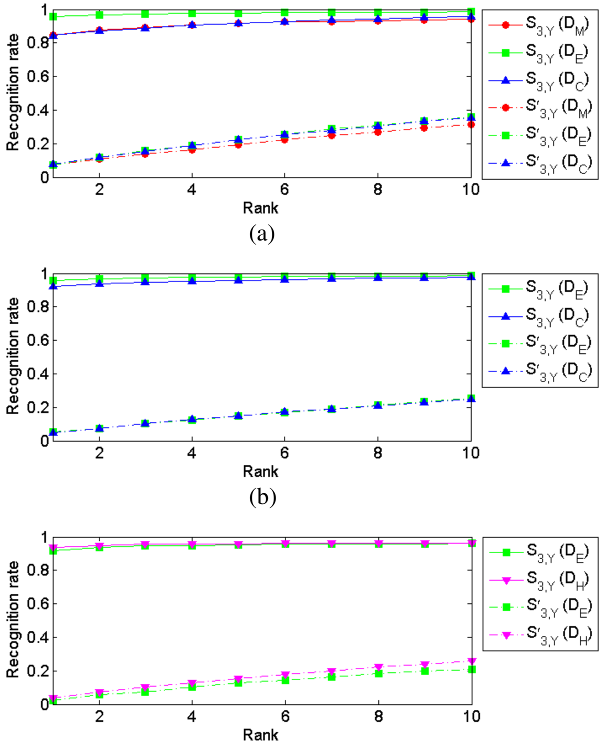
4.2 Objective Assessments

Our objective assessments consist of four experiments: 1) distance measurement for automatic FR applied to privacy-protected probe face images; 2) automatic FR applied to scrambled luma information; 3) automatic FR applied to scrambled luma and non-scrambled chroma information; and 4) automatic FR applied to non-scrambled chroma information.

Distance Measurement – The effectiveness of automatic FR depends on the metric used for measuring the distance between the feature vector of a probe face image and the feature vectors of the gallery face images. In this experiment, we investigate the influence of the following distance metrics on the effectiveness of automatic FR: Euclidean distance, Mahalanobis distance, Cosine distance, and Chi-square distance (denoted as D_E, D_M, D_C, and D_H, respectively).

When making use of non-scrambled probe face images, Fig. 1 shows that PCA-, FLDA-, and LBP-based FR are most effective when the Mahalanobis, Euclidean, and Chi-square distance metric are used, respectively (PCA-, FLDA-, and LBP-based FR achieve a rank 1 recognition rate of 84%, 96%, and 95%, respectively). These observations independently confirm results previously presented in the scientific literature [19],[20],[24]. However, when making use of scrambled probe face images, our experimental results indicate that PCA-based FR is most effective when making use of the Euclidean distance metric. Consequently, in the remainder of our experiments, we make use of the Euclidean distance metric for PCA- and FLDA-based FR, and we make use of the Chi-square distance metric for LBP-based FR. Note that, hereinafter, the grey-shaded area in each figure represents the set of recognition rates that yield an ideal or asymptotical level of privacy protection, which is the probability of success of random guessing.

Scrambled Luma Information – Fig. 2 allows studying the effectiveness of FR when only protecting the luma subbands of probe face images, assuming that an adversary is not able to take advantage of the possible presence of non-scrambled chroma information in the privacy-protected probe face images.



(a)

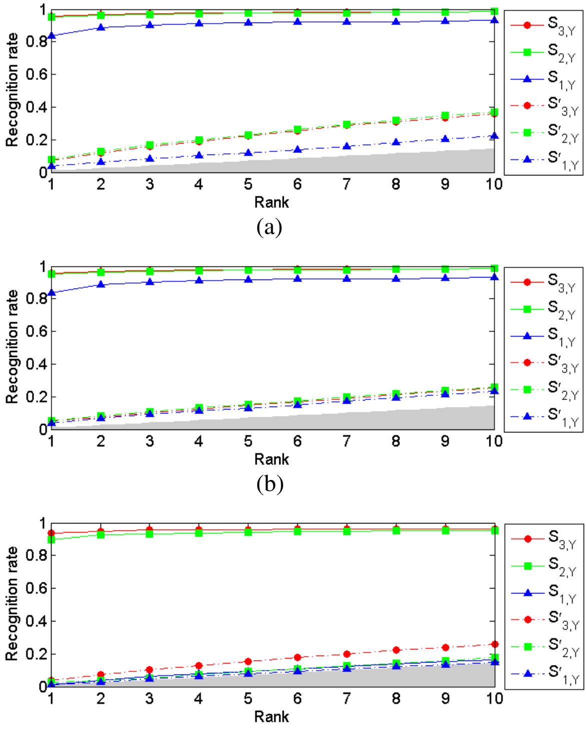
(b)

(c)

Fig. 1. Influence of distance measurement on FR effectiveness: (a) PCA, (b) FLDA, and (c) LBP

When making use of non-scrambled probe face images, all rank 1 recognition rates are higher than 83%, except when LBP-based FR is applied to $S_{1,Y}$, (*i.e.*, when LBP-based FR is applied to the luma information stored in the DC subbands of a face region). Specifically, for LBP-based FR, the rank 1 recognition rate decreases from 94% for $S_{1,Y}$ to 1.2% for $S_{1,Y}$. The substantial decrease in effectiveness of LBP-based

FR can be attributed to the fact that distinctive pixel information in local regions is almost completely eliminated in DC subbands. When scrambling the luma subbands of probe face images, the overall effectiveness of FR decreases significantly. The rank 1 recognition rates obtained for PCA-, FLDA-, and LBP-based FR are lower than 7.6%, 6.1%, and 3.8%, respectively. Consequently, the results presented in Fig. 2 show that layered scrambling is for instance highly effective in preserving privacy when making use of grayscale video surveillance.



(a)

(b)

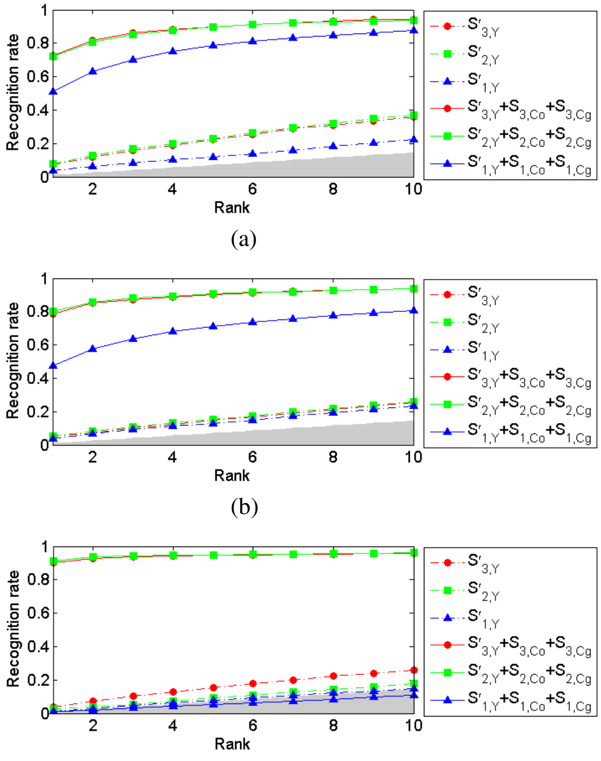
(c)

Fig. 2. Influence of layered scrambling on FR effectiveness: (a) PCA, (b) FLDA, and (c) LBP. Note that FR only makes use of luma information.

Scrambled Luma and Non-scrambled Chroma Information – To limit bit rate overhead in heterogeneous usage environments, the layered scrambling technique proposed in [4] only protects the luma subbands of face regions. In this experiment, we investigate whether layered scrambling is still effective when the scrambled luma channel and the non-scrambled chroma channels are simultaneously used for the purpose of automatic FR, assuming that an adversary has access to the compressed bit stream structure, and thus to the non-scrambled chroma information. Indeed, previous research has demonstrated that the additional use of chroma information is capable of increasing the overall effectiveness of FR [25].

To take advantage of non-scrambled chroma information, we adopted feature-level fusion [23]. Specifically, we fused feature vectors extracted from the scrambled luma and the non-scrambled chroma channels of face images by means of concatenation. Note that JPEG XR by default makes use of the YCoCg color space. Also, note that we did not subsample the chroma channels during encoding (*i.e.*, we made use of the YCoCg 4:4:4 color format).

As shown in Fig. 3, the recognition rates significantly increase when automatic FR is able to make use of both scrambled luma information and non-scrambled chroma information, compared to the recognition rates obtained when automatic FR is only able to make use of scrambled luma information. In particular, the rank 1 recognition rate is at least 44% for all FR techniques used, except when LBP-based FR is applied to DC subbands. This implies that the presence of non-scrambled chroma information can significantly decrease the effectiveness of scrambling when an adversary has access to the compressed bit stream structure.



(a)

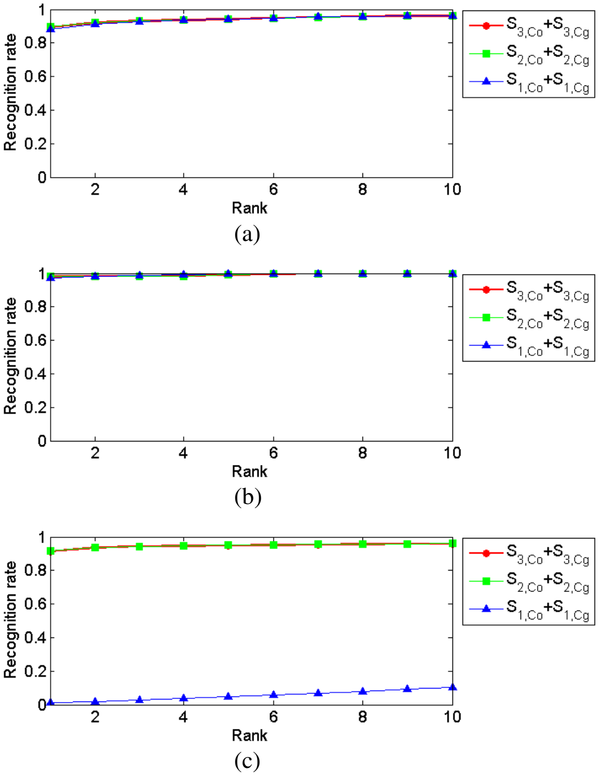
(b)

(c)

Fig. 3. Influence of scrambled luma information and non-scrambled chroma information on FR effectiveness: (a) PCA, (b) FLDA, and (c) LBP

Non-scrambled Chroma Information – Since non-scrambled chroma information is available to an adversary aware of the compressed bit stream structure, it is also important to investigate the effectiveness of automatic FR when only making use of non-scrambled chroma information. Fig. 4 plots the recognition rates obtained for automatic FR only making use of non-scrambled chroma information. We can observe that the rank 1 recognition rate is always higher than 88% for all FR techniques used, except when LBP-based FR is applied to DC subbands. This again implies that the presence of non-scrambled chroma information can significantly decrease the effectiveness of scrambling when an adversary has access to the compressed bit stream structure.

To summarize, for video surveillance applications requiring a high level of privacy protection, the results presented in Fig. 3 and Fig. 4 indicate that both luma and chroma information needs to be scrambled.



(a)

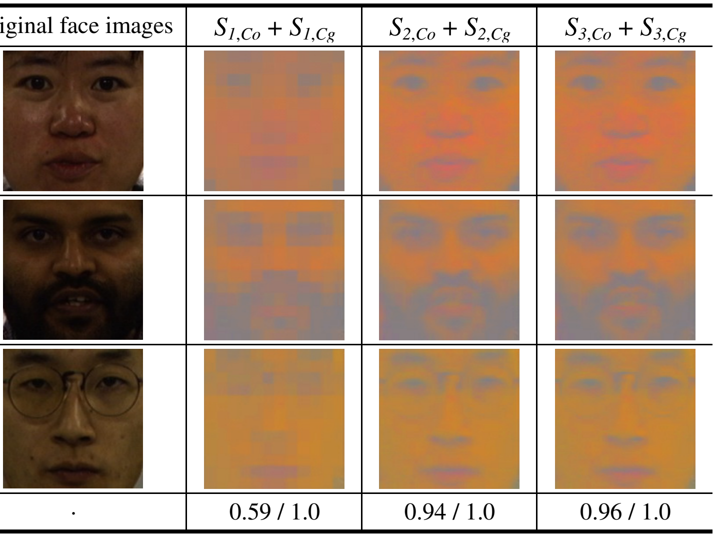
(b)

(c)

Fig. 4. FR effectiveness when only making use of non-scrambled chroma information: (a) PCA, (b) FLDA, and (c) LBP

4.3 Subjective Assessments

Our subjective assessments consist of two experiments: 1) human FR applied to non-scrambled chroma information and 2) human FR applied to scrambled luma and non-scrambled chroma information. In addition, we make use of complementary objective assessments to study whether agreement exists between 32 human observers and the output of automatic FR. The complementary objective assessments make use of experimental settings that are identical to the experimental settings used in our subjective assessments (for each of the subjective experiments, we used three probe face images and twelve gallery face images). Consequently, we report experimental results by means of example face images, Subjective Recognition Rates (SRR), and Objective Recognition Rates (ORR). Subjective recognition rates are obtained by counting the number of human observers reporting a correct identification over the total number of trials (since three probe face images are used for each parameter setting, the total number of trials for each parameter setting is three times the total number of human observers), while objective recognition rates are obtained by counting the number of correctly identified probe face images over the total number of probe face images at rank 1. Note that objective recognition rates are obtained for PCA-based FR (PCA-based FR had the highest overall effectiveness in Section 4.2).



Subbands used	Original face images	$S_{1,Co} + S_{1,Cg}$	$S_{2,Co} + S_{2,Cg}$	$S_{3,Co} + S_{3,Cg}$
Example face images				
SRR / ORR	·	0.59 / 1.0	0.94 / 1.0	0.96 / 1.0

Fig. 5. Subjective and objective results for non-scrambled chroma information

Non-scrambled Chroma Information – This experiment assumes that an adversary has access to the compressed bit stream structure. Fig. 5 shows the subjective recognition rates obtained for probe face images only consisting of non-scrambled chroma information (this is, we did not visualize luma information for the probe face images shown in Fig. 5). We can observe that the subjective recognition rate is equal to 96% for S_3, 94% for S_2, and 59% for S_1. When not scrambling chroma information, the 32 human observers were able to correctly identify the face images by means of visual clues such as skin color information, the shape of a face, the presence of four corners in the face images, and even slight differences in face orientation. In addition, we can observe that PCA-based FR is able to achieve perfect objective recognition rates, regardless of the different types of subbands used.

Scrambled Luma and Non-scrambled Chroma Information – Again assuming that an adversary has access to the compressed bit stream structure, Fig. 6 shows the subjective recognition rates obtained for probe face images with scrambled luma and non-scrambled chroma information. From both the subjective recognition rates and the example face images shown, we can observe that scrambled luma information significantly hampers the identification of probe face images when simultaneously visualizing scrambled luma and non-scrambled chroma information. On the other hand, we can observe that PCA-based FR is able to achieve perfect recognition rates (see ORR in Fig. 6). The latter can be attributed to the presence of non-scrambled chroma information and the use of a limited number of gallery face images.

To summarize, the experimental results presented in Fig. 5 and Fig. 6 indicate that, when an adversary has access to the compressed bit stream structure, non-scrambled chroma information can be successfully used to identify probe face images that have only been privacy-protected in the luma domain.

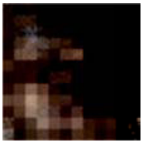
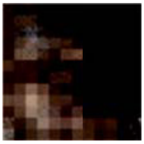
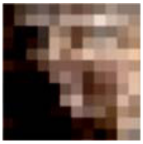
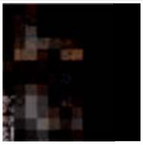
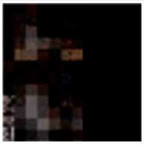
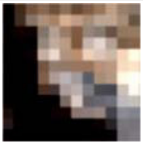
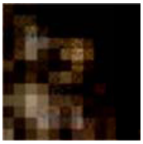
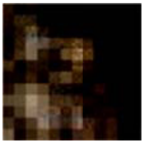
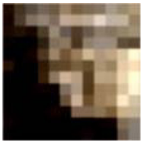
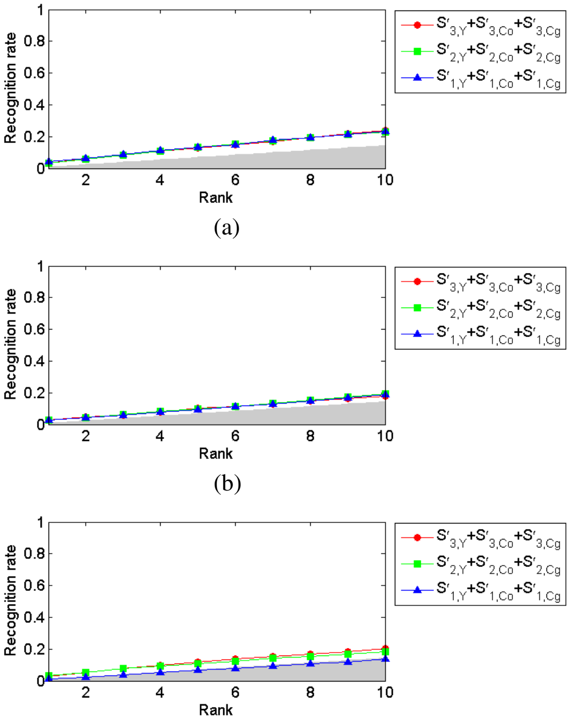
Subbands used	Original face images	$S'_{1,Y}+S_{1,Co}+S_{1,Cg}$	$S'_{2,Y}+S_{2,Co}+S_{2,Cg}$	$S'_{3,Y}+S_{3,Co}+S_{3,Cg}$
Example face images				
				
				
SRR / ORR	·	0.03 / 1.0	0.0 / 1.0	0.0 / 1.0

Fig. 6. Subjective and objective results for scrambled luma and non-scrambled chroma information

5 Discussion

Given that the mere scrambling of luma information already results in significant distortion of the facial information present in a face region, human observers were not able to correctly recognize face images when simultaneously visualizing scrambled luma and non-scrambled chroma information. However, as shown by our objective and subjective assessments (see Fig. 4 and Fig. 5), an adversary aware of the compressed bit stream structure can take advantage of the presence of non-scrambled chroma information in probe face images. Consequently, for video surveillance applications requiring a high level of privacy protection, both the luma and the chroma channels need to be scrambled at the cost of a higher bit rate overhead. In this paper, we therefore propose to apply layered scrambling to both the luma (Y) and the chroma channels (Co and Cg).



(a)

(b)

(c)

Fig. 7. FR effectiveness when making use of scrambled luma and chroma information: (a) PCA, (b) FLDA, and (c) LBP.

Fig. 7 allows studying the effectiveness of automatic FR applied to probe face images with scrambled luma and chroma channels. The resolution of the probe face images used was fixed to 192×192 and the QP value was set to 20. For all FR techniques used, we can observe that the rank 1 recognition rates obtained are lower than 4.1%, demonstrating that a high level of privacy protection can be achieved by scrambling both the luma and the chroma channels.

Fig. 8 shows that scrambling both the luma and chroma channels results in a total bit rate overhead of 7.0%, 18.1%, and 46.4% for S_3, S_2, and S_1, respectively, using a value of 8 for the RLS parameter L (see [4]). Compared to the case in which only luma information is scrambled, the increase in bit rate overhead is 5.4%, 14.1%, and 36.9% for S_3, S_2, and S_1, respectively. Note that we measured the overhead relative to the size of the face image (and not to the size of the whole image, which includes both the face image and background information), thus assuming a worst case scenario (dependent on the scenario, face regions may make up a large part of the video content). Further, Fig. 8 also presents bit rate overhead numbers when using 4:2:0 sub-sampling. Note that sub-sampling decreases the level of privacy protection, given the lesser amount of data available for scrambling. For instance, in the ideal case where all transform coefficients are non-zero and where the RLS parameter L is set to 8, the use of chroma sub-sampling reduces the total number of combinations required to break the protection of 10 MBs from 3.6×10^{722} to 1.7×10^{360}.

The results above show that, although scrambling chroma information increases the level of privacy protection, it comes with a higher bit rate overhead. The latter may be of concern when multiple video streams need to be simultaneously delivered in diverse usage environments.

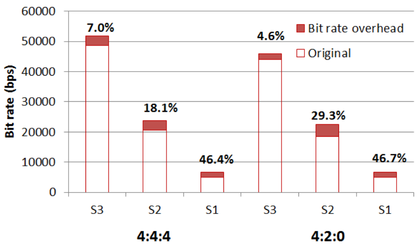


Fig. 8. Bit rate overhead when making use of scrambled luma and chroma information: (a) 4:4:4 color format and (b) 4:2:0 color format

6 Conclusions and Directions for Future Research

This paper studied and quantified the influence of non-scrambled chroma information on the effectiveness of automatic and human FR. To that end, we made use of three automatic FR techniques to test the effectiveness of a layered scrambling technique developed for Motion JPEG XR, taking into account the following four experimental conditions: 1) distance measurement for automatic FR applied to privacy-protected probe face images; 2) automatic FR applied to scrambled luma information; 3) automatic FR applied to scrambled luma and non-scrambled chroma information; and 4) automatic FR applied to non-scrambled chroma information. In addition, we investigated whether agreement exists between the judgments of 32 human observers and the output of automatic FR for the following two experimental conditions: 1) human

FR applied to non-scrambled chroma information and 2) human FR applied to scrambled luma and non-scrambled chroma information.

Our results show that human observers were not able to successfully recognize face images when simultaneously visualizing scrambled luma and non-scrambled chroma information. However, when an adversary has access to the coded bit stream structure, the presence of non-scrambled chroma information may significantly contribute to privacy leakage (rank 1 recognition rates > 88% when applying automatic FR to non-scrambled chroma information). Consequently, for video surveillance applications requiring a high level of privacy protection, our results indicate that both luma and chroma information needs to be scrambled. We therefore applied layered scrambling to both luma and chroma information, showing that a higher level of privacy protection can be achieved (rank 1 recognition rates < 4.1%) at the cost of an increase in bit rate overhead of 36.9% (DC), 14.1% (DC+LP), and 5.4% (DC+LP+HP), measuring overhead relative to the case where only luma information is scrambled.

In order to compile a benchmark for tools for privacy protection, future research will focus on identifying additional worst case scenarios. This benchmark could for instance be used to design a more effective evaluation framework for privacy preservation. This benchmark could also be used to design more effective tools for privacy protection. Finally, we plan to evaluate the use of layered scrambling in coding formats other than Motion JPEG XR.

Acknowledgement. This research was supported by the National Research Foundation (NRF) of Korea (grant: NRF-D00070).

References

1. Bowyer, K.W.: Face recognition technology: security versus privacy. IEEE Society on Social Implications of Technology 23, 9–19 (2004)
2. Dufaux, F., Ebrahimi, T.: Scrambling for Privacy Protection in Video Surveillance Systems. IEEE Transactions on Circuits and Systems for Video Technology 18, 1168–1174 (2008)
3. Carrillo, P., Kalva, H., Magliveras, S.: Compression Independent Reversible Encryption for Privacy in Video Surveillance. EURASIP Journal on Information Security 2009, Article ID 429581, 13 pages (2009)
4. Sohn, H., De Neve, W., Ro, Y.M.: Privacy Protection in Video Surveillance Systems: Analysis of Subband-Adaptive Scrambling in JPEG XR. IEEE Transactions on Circuits and Systems for Video Technology 21, 170–177 (2011)
5. Sohn, H., Anzaku, E.T., De Neve, W., Ro, Y.M., Plataniotis, K.N.: Privacy Protection in Video Surveillance Systems Using Scalable Video Coding. In: IEEE International Conference on Advanced Video and Signal Based Surveillance, pp. 424–429 (2009)
6. Zeng, W., Lei, S.: Efficient frequency domain video scrambling for content access control. In: Proceedings of ACM International Conference on Multimedia, pp. 285–294 (1999)
7. Tong, L., Dai, F., Zhang, Y., Li, J.: Visual security evaluation for video encryption. In: Proceedings of ACM International Conference on Multimedia, pp. 835–838 (2010)
8. Dufaux, F., Ebrahimi, T.: H.264/AVC video scrambling for privacy protection. In: Proceedings of IEEE International Conference on Image Processing, pp. 1688–1691 (2008)

9. Sohn, H., De Neve, W., Ro, Y.M.: Region-of-Interest Scrambling for Scalable Surveillance Video using JPEG XR. In: Proceedings of ACM International Conference on Multimedia, pp. 861–864 (2009)
10. Rodrigues, J.-M., Puech, W., Bors, A.: A Selective Encryption for Heterogeneous Color JPEG Images Based on VLC and AES Stream Cipher. In: Proceedings of European Conference on Colour in Graphics, Imaging and Vision, pp. 34–39 (2006)
11. Zou, J., Ward, R.K., Qi, D.: A new digital image scrambling method based on Fibonacci numbers. In: Proceedings of International Symposium on Circuits and Systems, III-965-8 (2004)
12. Dufaux, F., Ebrahimi, T.: A Framework for the Validation of Privacy Protection Solutions in Video Surveillance. In: IEEE International Conference on Multimedia & Expo., pp. 66–71 (2010)
13. Mao, Y., Wu, M.: A joint signal processing and cryptographic approach to multimedia encryption. IEEE Transactions on Image Processing 15(7), 2061–2075 (2006)
14. Tran, T.D., Liu, T., Topiwala, P.: Performance comparison of leading image codecs: H.264/AVC Intra, JPEG2000, and Microsoft HD Photo. In: Proceedings of SPIE, pp. 66960B.1–66960B.14 (2007)
15. Srinivasan, S., Tu, C., Regunathan, S.L., Sullivan, G.J.: HD Photo: A new image coding technology for digital photography. In: Proceedings of SPIE, pp. 66960A.1–66960A.19 (2007)
16. Sim, T., Baker, S., Bsat, M.: The CMU pose, illumination, and expression database. IEEE Transactions on Pattern Analysis and Machine Intelligence 25, 1615–1618 (2003)
17. IVY Lab Video Surveillance Dataset, `http://ivylab.kaist.ac.kr/demo/vs/dataset.htm`
18. Turk, M.A., Pentland, A.P.: Eigenfaces for recognition. Journal of Cognitive Neuroscience 3, 71–86 (1991)
19. Belhumeur, P.N., Hesphanha, J.P., Kriegman, D.J.: Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence 9, 711–720 (1997)
20. Ahonen, T., Hadid, A., Pietikainen, M.: Face description with local binary patterns: Application to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 28, 2037–2041 (2006)
21. Phillips, P.J., Wechsler, H., Huang, J., Rauss, P.: The FERET database and evaluation procedure for face recognition algorithms. Image and Vision Computing Journal 16, 295–306 (1998)
22. Wang, J., Plataniotis, K.N., Lu, J., Venetsanopoulos, A.N.: On solving the face recognition problem with one training sample per subject. Pattern Recognition 39, 1746–1762 (2006)
23. Jain, A.K., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recognition 38, 2270–2285 (2005)
24. Perlibakas, V.: Distance measures for PCA-based face recognition. Pattern Recognition Letters 25, 1421–1430 (2004)
25. Choi, J.Y., Ro, Y.M., Plataniotis, K.N.: Color face recognition for degraded face images. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 39, 1217–1230 (2009)