MIPRO 2014, 26-30 May 2014, Opatija, Croatia

An Experimental Tattoo De-identification System for Privacy Protection in Still Images

Darijan Marčetić, Slobodan Ribarić
Faculty of Electrical Engineering and Computing
University of Zagreb
Unska 3, 10000 Zagreb, Croatia
Email: {darijan.marcetic, slobodan.ribaric}@fer.hr

Vitomir Štruc and Nikola Pavešić
Faculty of Electrical Engineering
University of Ljubljana
Tržaška 25, SI-1000 Ljubljana, Slovenia
Email: {vitomir.struc, nikola.pavesic}@fe.uni-lj.si

***Abstract*—An experimental tattoo de-identification system for privacy protection in still images is described in the paper. The system consists of the following modules: skin detection, region of interest detection, feature extraction, tattoo database, matching, tattoo detection, skin swapping, and quality evaluation. Two methods for tattoo localization are presented. The first is a simple ad-hoc method based only on skin colour. The second is based on skin colour, texture and SIFT features. The appearance of each tattoo area is de-identified in such a way that its skin colour and skin texture are similar to the surrounding skin area. Experimental results for still images in which tattoo location, distance, size, illumination, and motion blur have large variability are presented. The system is subjectively evaluated based on the results of tattoo localization, the level of privacy protection and the naturalness of the de-identified still images. The level of privacy protection is estimated based on the quality of the removal of the tattoo appearance and the concealment of its location.**

Keywords—tattoo de-identification, privacy protection, SIFT.

I. INTRODUCTION

In general, privacy protection for multimedia contents is a prerequisite for public/private surveillance systems [1], the storing and exchange of medical records [2], court interrogations of protected witnesses, and web services, such as social networks [3], image sharing [4], news portals, and Google Street View [5]. Person identification can be performed in still images and/or on video based on hard and soft biometric identifiers. Soft-biometric identifiers, such as gait, gesture, silhouette, skin marks, tattoos, hairstyle, height, weight, age and gender, may be used as valuable additional information for the identification of individuals in combination with other cues.

The current state of the art of personal recognition systems based on soft-biometric identifiers, such as birthmarks and tattoos [6], could enable the automatic personal identification of individuals in still images or on video even if face de-identification methods have been applied. For example, systems based on scars, marks and tattoos are being increasingly used for suspect and victim identification in forensics and law enforcement agencies [6], [7]. Furthermore, tattoos, as a soft biometric trait, are becoming ever more present in the wider population; for example, 24% of people aged 18 to 50 in the USA have at least one tattoo, and their number is increasing [8].

The visual appearance of a tattoo and its location on the body vary greatly, which makes it suitable for personal identification. The ANSI/NIST-ITL.1-2011 standard classifies tattoos based on visual appearance into 8 classes (i.e. human, animal, plant...) and 70 subclasses (i.e. male face, female face...) [9]. In addition, tattoos are indexed based on their position on the body into 33 main categories (i.e. abdomen, ankle, arm…) and 71 subcategories (i.e. forehead, finger(s) left hand, finger(s) right hand…) [9].

Tattoo-ID [6] and FASTID [7] are two well-known systems for tattoo identification. They both use SIFT features [10] for tattoo identification. Although these systems rely on human labelling, Lee et al. [11] presented a content-based image retrieval system for matching tattoo images. A methodology for detecting scars, marks and tattoos found in unconstrained imagery typical of forensics scenarios is described in [12]. The matching and retrieval of tattoo images based on active contour content-based image retrieval and global-local image features is described in [13]. All of this raises the need for tattoo de-identification for privacy protection. Additionally, tattoo de-identification can increase the privacy protection level of naive or k-Same based approaches to face de-identification [14] in still images because even if the visual appearance of a tattoo is removed from the face, the tattoo location may still be present as an artefact. As far as we know, currently there are no papers related to tattoo de-identification for privacy protection.

In this paper we focus on tattoo localization and de-identification for privacy protection in still images. An experimental tattoo de-identification system for still images is proposed, and the preliminary results of de-identification are presented.

II. SYSTEM DESCRIPTION

The proposed system for tattoo de-identification is depicted in Fig. 1. The system consists of the following modules: skin detection, region of interest (ROI) detection, feature extraction, tattoo database, matching, tattoo detection, skin swapping, and quality evaluation. Detailed descriptions of the modules follow.

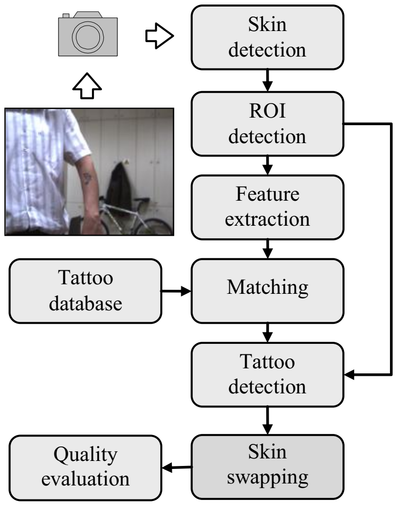

Fig. 1. The tattoo de-identification system.

A still image obtained by a colour camera is an input (Fig. 2) to the *skin detection* module. Uncovered body parts like head, neck, hands, legs or torso are detected in two phases.

Fig. 2. An example of a still image obtained by a colour camera.

In the first phase, skin colour cluster boundaries (Fig. 3) are obtained by a pixel-based method through a series of decision rules in the RGB colour space [15].

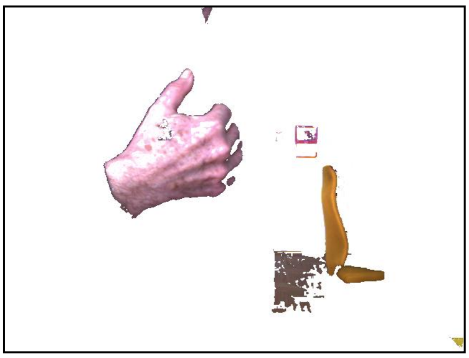

Fig. 3. A skin colour area.

In the second phase, geometrical constraints are used to eliminate skin-like colour regions that do not belong to the uncovered body part areas. A skin-like colour region is declared as a non-uncovered body part area based on its size and shape. The parameters of the size filter and the shape are determined experimentally based on a set of training still images.

In the *region of interest (ROI) detection* module, the potential tattoo regions are located. The ROI consists of skin colour regions, holes and cutout regions which are inside or close to an uncovered body part area. Tattoos can also have skin-like colours and this is the reason why skin colour regions are also included in the ROIs. Typically, tattoos have colours that are not classified as a skin colour, which results in holes and cutouts. Holes are fully surrounded by an uncovered body part area. Cutout regions have a non-skin colour and the distances of their pixels to the nearest pixels belonging to an uncovered body part area are below some predefined threshold. The cutout regions are obtained by the morphological operation of closing. Fig. 4 depicts holes and cutouts. The corresponding ROI is shown in Fig. 5.

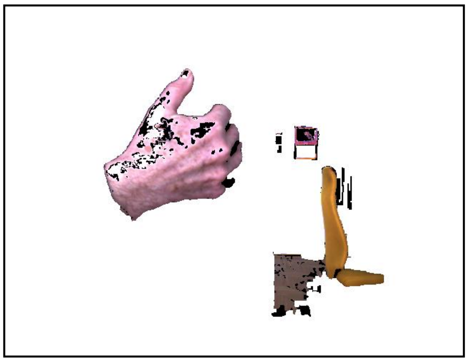

Fig. 4. A skin colour area with holes and cutout regions depicted in black.

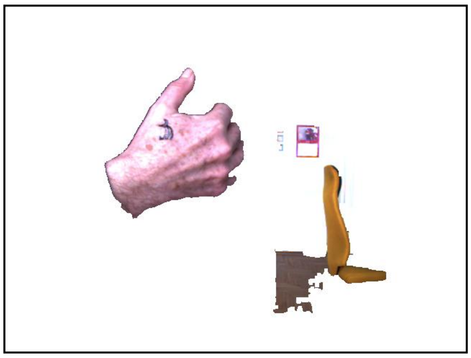

Fig. 5. The ROI – a candidate for SIFT feature extraction

The SIFT features are extracted from a ROI in the *feature extraction* module. SIFT features are commonly used for tattoo identification [6], [7], [11], and this is the main reason why we have selected them for tattoo localization in the proposed system. Note that in the process of tattoo de-identification, the tattoo SIFT features are removed. Additionally, by introducing the suspects' tattoo database and by using the results of SIFT feature matching it is possible to refuse tattoo de-identification and to alert authorities that the owner of a tattoo is on the screening list. Fig. 6 illustrates the SIFT features extracted from the ROI (Fig. 5).

Each SIFT feature is paired with the location of a centre of a region from which it was extracted. These SIFT features are matched with template SIFT features from the *tattoo database* (Fig. 7). The template SIFT features in the *tattoo database* are obtained from still images with tattoos during the learning phase. Experimentally, we used 24 tattoos (Fig. 7) with at least two tattoos from each of the eight classes of tattoos [9]. Each tattoo in the tattoo database has an average of 56 template SIFT features. The *tattoo database* consists of 1338 SIFT features.

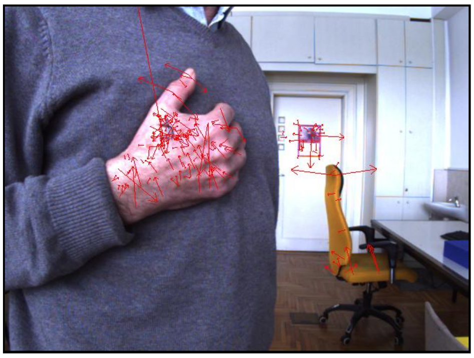

Fig. 6. Extracted SIFT features.

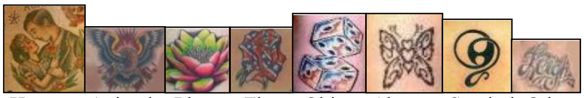

Fig. 7. Examples of tattoos used for forming the template SIFT features in the *tattoo database*.

Matching is performed in the *matching* module as described in [10]. If there are SIFT features that have matched with some template SIFT features from the *tattoo database* (Fig. 8), then these SIFT feature locations are declared as seeds of a tattoo region(s).

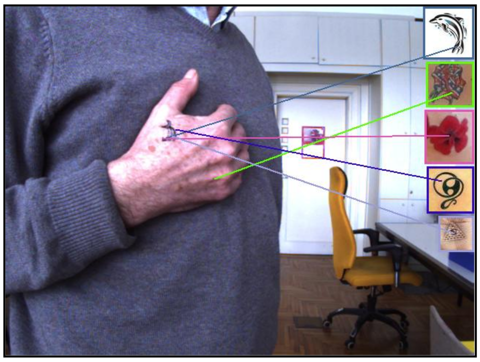

Fig. 8. The result of matching SIFT features to the template SIFT features.

The suitability of each template SIFT feature for tattoo localization and alternative matching schemes have not been analyzed so far in the experimental system, but this is planned as part of future work. In general, SIFT features common for many tattoos are more desirable, thus leading to a smaller *tattoo database* and faster matching times. A lower matching threshold would lead to fewer false negative tattoo detections and more false positive tattoo detections.

Tattoo regions are obtained by segmentation in the *tattoo detection* module. Two methods are presented. In the first ad-hoc method, all holes in the skin colour regions, obtained in the *ROI detection* module, are declared as tattoo regions (Fig. 4). This surprisingly simple yet effective ad-hoc method is based on the observation that tattoos in still images are typically fully surrounded by a skin colour region. In the second method, segmentation starts from the matched SIFT feature locations obtained in the *matching* module. Consequently, the initial tattoo region consists only of seed pixels corresponding to these locations (Fig. 9 b). The surrounding area is iteratively analysed for tattoo presence as follows. Each analyzed pixel is declared as an element of a tattoo region if its distance to the nearest tattoo pixel is below some predefined threshold and if at least one of the two additional conditions is also fulfilled (Fig. 9 a). The first condition is that a pixel has a non-skin colour. The optional second condition is evaluated if the first condition is not fulfilled. The second condition is that entropy, determined on a neighbourhood around this analyzed pixel, has a non-skin value. The value of entropy for a non-skin area is determined experimentally. This texture-based condition is used to obtain tattoo pixels which have a skin-like colour, which reduces false negative tattoo detections. Consequently, a ROI can be segmented as part of a tattoo region based on its colour or texture even if this ROI part has SIFT features that have not been matched with any SIFT feature from the tattoo database, or even if it has no SIFT features. The described procedure of tattoo region growing is iteratively performed until no new pixels can be declared as a member of a tattoo region. The obtained tattoo region is dilated to its surrounding area by a relatively small circular structuring element. The output of the *tattoo detection* module is a segmented ROI image consisting of tattoo regions and a non-tattoo area (Fig. 9).

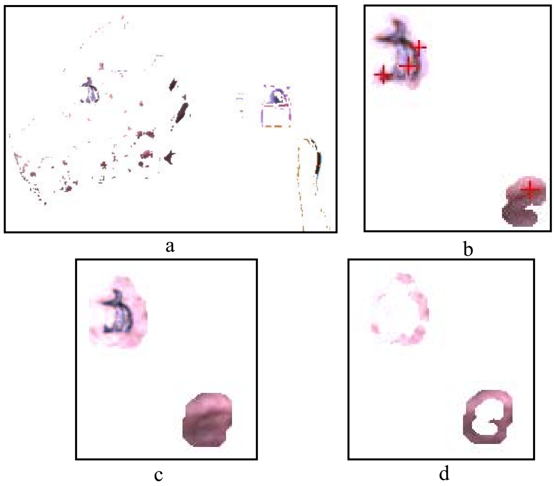

Fig. 9. Tattoo area segmentation process: a) an area of an ROI that has a non-skin colour or non-skin texture; b) segmented tattoo regions with seeds depicted as red crosses; c) a ROIs used in the process of de-identification; d) skin non-tattoo areas used for swapping the tattoo region in b).

Each tattoo region is de-identified in the *skin swapping* module. In the process of tattoo de-identification, these tattoo regions are replaced with skin patches obtained from their surrounding skin area. Consequently, the colour and texture of de-identified tattoo regions are the same as those of the surrounding skin area. The problem of replacing tattoo regions with skin patches is similar to the problem of face swapping [16]. Issues regarding colour transfer and colour matching between images in the process of face swapping are described in [16], [17]. Similar procedures can be used for face and tattoo de-identification.

In our experimental system we use a simple method to replace a tattoo region with skin-like patches obtained from its surrounding skin area.

The de-identification process is performed in the *skin swapping* module as follows. First, an area used in the process of de-identification (Fig. 9 c), obtained in the *tattoo detection* module, which consists of a tattoo region (Fig. 9 b), and its surrounding area (Fig. 9 d), is divided into squares. There are two types of squares: squares that have at least one tattoo region pixel (marked in red in Fig. 10) and squares that have only skin colour pixels, and these squares enclose groups of red squares (marked in green in Fig. 10).

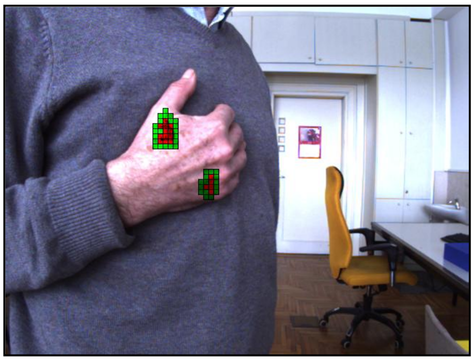

Fig. 10. Two types of squares used in the process of de-identification.

For each one of these red squares, the nearest green square of a skin non-tattoo region is selected. Tattoo region pixels in the red square are replaced with corresponding pixels from its nearest green square (Fig. 10). The size of the squares (5×5 pixels) is experimentally determined. Larger squares result in more natural skin texture; however, in this case, the de-identification process may result in artefacts in de-identified tattoo areas. After replacement, a median filter is applied on the de-identified area. With this method, we try to hide the tattoo location and its visual appearance, and preserve the naturalness of the de-identified image (Fig. 11).

In the *quality estimation* module, the privacy protection level and naturalness of de-identified tattoo regions are evaluated. The privacy protection level is subjectively evaluated based on two criteria: the first criterion is that the SIFT features are removed from the de-identified tattoo regions, and the second one is that both tattoo location and its visual appearance are hidden. The naturalness of the de-identified tattoo regions is also subjectively evaluated.

Fig. 11. De-identified tattoo still frame.

III. EXPERIMENTAL RESULTS

Two experiments were performed on still images of people with and without tattoos collected by a colour video camera placed in our laboratory. A total of 204 video frames with a resolution of 640×480 pixels, of which 148 contained a tattoo, as still images taken from 8 video sequences of three persons walking in front of the camera were selected for the evaluation. Examples of the still images are shown in Fig. 12. In the future, we plan to develop a tattoo de-identification system for surveillance applications and for this reason still images, used in the experiments, are taken as frames from the video. The distance of persons from the camera was in the range of 1 to 5 meters. The tattoos were from 5 to 35 pixels in diameter, which is small relative to the image size, they cover below 15% of the uncovered body part area, have motion blur and different illumination. This is somewhat different from tattoo images obtained from web services such as Facebook or Picasa, where tattoo still images are taken under well controlled lighting conditions from short distances and tattoos can cover a large proportion of a skin area. These types of tattoo still images will be addressed in future work.

The experiments can be described as follows. A simple ad-hoc tattoo localization method was used in the first experiment. This ad-hoc method declares all holes in the skin colour area, obtained in the ROI detection module, as tattoos. Colour, texture, SIFT features and the tattoo database were used for tattoo localization in the second experiment. All tattoo regions detected in both experiments were swapped with skin patches as described in the *tattoo swapping* module.

The system was evaluated based on the results of the tattoo localization, the level of privacy protection and the naturalness of the de-identified still images.

Tattoo localization was evaluated based on the percentage of false positive R_{FP} and false negative R_{FN} tattoo detection ratios:

$$R_{FP} = \frac{N_{FP}}{N_{ALL}} \times 100\,\%\text{, and } R_{FN} = \frac{N_{FN}}{N_{TAT}} \times 100\,\%,$$

where N_{FP} is the number of original images that have at least one falsely detected tattoo region which after de-identification has a visual appearance in the corresponding de-identified image region that is noticeably different from in the original image, N_{ALL} is the total number of still images with and without tattoos, N_{FN} is the number of original images for which at least one tattoo region has not been located, and consequently the tattoo appearance was not removed, and N_{TAT} is the total number of still images used in the experiment with at least one tattoo. False positive and negative tattoo detections have an impact on the naturalness and level of privacy protection of the de-identified images respectively.

The privacy protection level is estimated based on the performance of hiding the tattoo locations R_{LOC} and tattoo appearances R_{APP} in the tattoo de-identification process:

$$R_{LOC} = \frac{N_{DL}}{N_{TAT}} \times 100\,\%\text{, and } R_{APP} = \frac{N_{DA}}{N_{TAT}} \times 100\,\%,$$

where N_{DL} is the number of de-identified images that have all tattoo locations successfully hidden and consequently all tattoo appearances are successfully removed, N_{TAT} is the total number of still images with at least one tattoo, and N_{DA} is the number of de-identified images that have all tattoo appearances successfully removed but some tattoo locations are not necessarily completely hidden. Note that if a tattoo location is hidden successfully, then the tattoo appearance is also removed successfully ($N_{DA} \geq N_{DL}$).

The naturalness of the de-identified tattoo images was subjectively evaluated on a scale from 1 (natural) to 5 (unnatural) in all still images used in the experiments. The statistical properties of the SIFT features obtained from the tattoo database and the still images used in the experiments are shown in Table I.

TABLE I. STATISTICAL PROPERTIES OF SIFT FEATURES OBTAINED FROM THE TATTOO DATABASE, THE STILL IMAGES USED IN THE EXPERIMENTS AND THEIR CORRESPONDING ROIS.

Description	Tattoo database	Test images	ROIs
Total number of still images	24	204	-
Total number of SIFT features in all images	1338	165461	25942
Minimal number of SIFT features per image	10	250	0
Maximal number of SIFT features per image	172	2023	497
Average number of SIFT features per image	55.75	811.08	127.17

Examples of de-identified tattoo still frames are shown in Fig. 12. The results of the tattoo de-identification experiments are shown in Table II. Based on the results shown in Table II, it can be concluded that the performances of hiding tattoo locations and tattoo appearances were similar for each method. False positive tattoo localisation is much higher in the first ad-hoc method than in the second one, which results in the lower naturalness of the de-identified images in the first method. False negative tattoo localisation is much lower in the first method than in the second one, which results in a higher level of privacy protection in the first method. Notice that there is a trade-off between the level of privacy protection and the naturalness of the de-identified still images in both methods. Methods that have a higher level of privacy protection typically result in lower naturalness. In future, it will be necessary to develop methods that increase the level of privacy but not at the expense of naturalness.

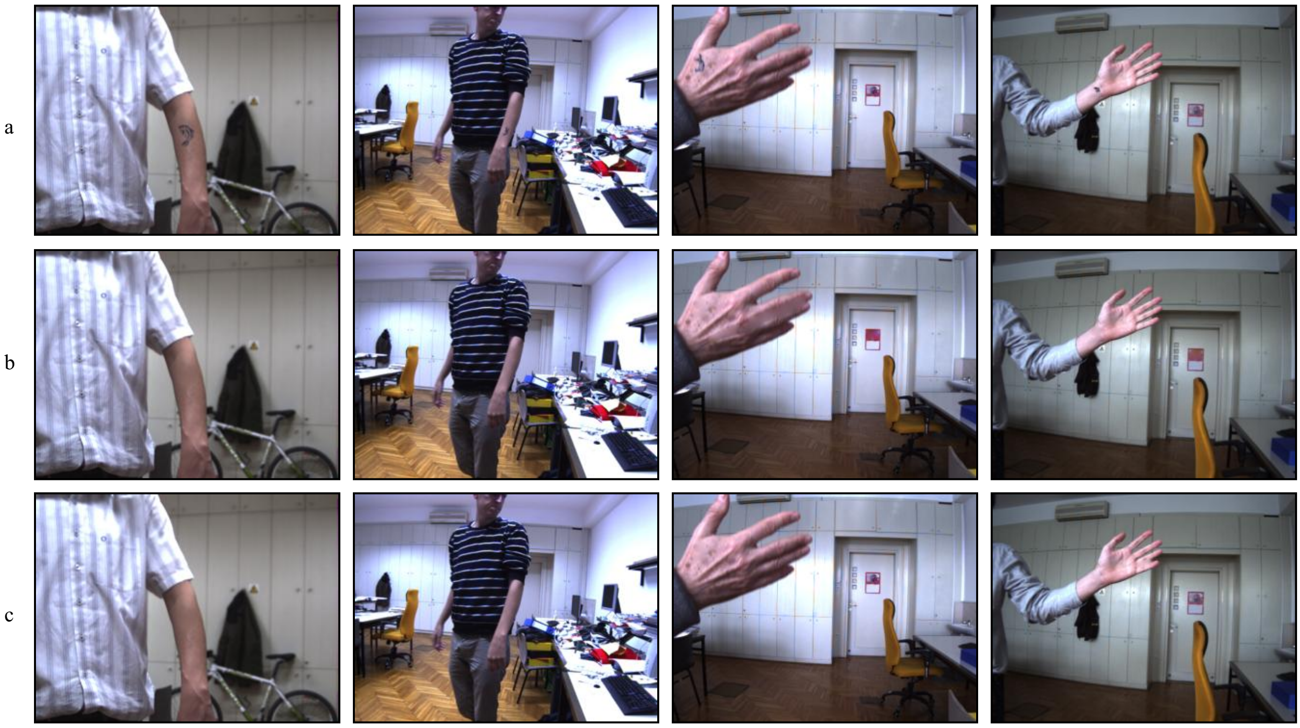

Fig. 12. Examples of de-identified tattoo still images: a) original still image; b) ad-hoc method; c) SIFT-based method.

TABLE II. RESULTS OF THE TATTOO DE-IDENTIFICATION EXPERIMENTS.

Category	Results	Experiment 1 (Ad-hoc)	Experiment 2 (SIFT)
Still images	N_{ALL}	204	204
	N_{TAT}	148	148
Tattoo localization	N_{FP}	39	10
	N_{FN}	12	43
	R_{FP}	19.12 %	4.90 %
	R_{FN}	8.11 %	29.05 %
Privacy protection	N_{DL}	134	104
	N_{DA}	136	105
	R_{LOC}	90.54 %	70.27 %
	R_{APP}	91.89 %	70.95 %
Naturalness	1 (natural)	161 (78.92 %)	193 (94.61 %)
	2	32 (15.67 %)	6 (2.94 %)
	3	9 (4.41 %)	3 (1.47 %)
	4	2 (0.98 %)	2 (0.98 %)
	5 (unnatural)	0 (0.00 %)	0 (0.00 %)
	Average	1.27	1.09

SIFT-based tattoo de-identification is computationally more expensive than the simple ad-hoc method. Average times needed by different computational steps of tattoo de-identification are shown in Table III. The methods were implemented in Matlab. The experiments were performed on an Intel i7 CPU @ 2.4 GHz laptop.

TABLE III. AVERAGE TIMES NEEDED BY DIFFERENT COMPUTATIONAL STEPS OF TWO TATTOO DE-IDENTIFICATION METHODS.

Time (ms)	SIFT	Ad-hoc
Skin area	293	
ROI	17	
SIFT extraction	696	-
SIFT matching	100	-
Tattoo detection	250	9
Skin swapping	23	
Total	1379	342

IV. CONCLUSION

An experimental system for tattoo localization and de-identification for privacy protection in still images has been described in this paper. Tattoo localization is based on colour, SIFT features and texture. The experiments show that tattoo localization is a tough problem for still images where tattoo location, distance, size, illumination, and motion blur vary greatly. Tattoo localization based on SIFT features shows satisfactory results in well-controlled conditions such as lighting, high tattoo resolution, and no motion blur. For tattoos with a low quality visual appearance, SIFT features have to be combined with some region segmentation based on a combination of colour, gradient and/or texture methods. In order to improve the naturalness of de-identified images, it is necessary to develop a better method for skin swapping in the tattoo de-identification process, using ideas from the area of image inpainting.

In future research work, we plan to develop a tattoo de-identification system for surveillance applications which will utilize skin and tattoo area tracking. By using spatial and temporal correspondence between frames, tattoo detection, localization and de-identification will be improved.

Privacy protection for multimedia contents is a tough problem due to the large number of biometrical traits that can be used for identification. In the field of privacy protection, further improvement in tattoo de-identification is necessary to supplement currently used face de-identification technologies.

ACKNOWLEDGMENT

The work presented in this paper was supported by the COST Action IC1206 and the University of Zagreb grant VIF2013-26.

REFERENCES

[1] F. Porikli, F. Brémond, at al., "Video Surveillance: Past, Present, and Now the Future", IEEE Signal Processing Magazine, vol. 30, Issue 3, 2013, pp. 190-198.

[2] J. Pegueroles, L. J. de la Cruz, at al., "The TAMESIS Project: Enabling Technologies for the Health Status Monitoring and Secure Exchange of Clinical Records", International Conference on Complex, Intelligent, and Software Intensive Systems, 2013, pp. 312-319.

[3] J. Bonneau, J. Anderson and G. Danezis, "Prying Data out of a Social Network", Advances in Social Network Analysis and Mining, 2009, pp. 249-254.

[4] Z. Stone, T. Zickler and T. Darrell, "Autotagging Facebook: Social Network Context Improves Photo Annotation", Computer Vision and Pattern Recognition Workshops (CVPRW), 2008, pp. 1-8.

[5] A. Frome, G. Cheung, "Large-scale privacy protection in Google Street View", IEEE International Conference on Computer Vision (ICCV), 2009, pp. 2373-2380.

[6] A. K. Jain, J.-E. Lee, and R. Jin, "Tattoo-ID: Automatic tattoo image retrieval for suspect & victim identification", In Proc. Pacific-Rim Conf. on Multimedia, 2007, pp. 256-265.

[7] D. Manger, "Large-Scale Tattoo Image Retrieval", Conference on Computer and Robot Vision, 2012, pp. 454-459.

[8] A. E. Laumann and A. J. Derick, "Tattoos and body piercings in the United States:A national data set", Journal of the American Academy of Dermatology, vol. 55, Issue 3, 2006, pp. 413-421.

[9] ANSI/NIST-ITL 1-2000 standard: American National Standard for Information Systems - data format for the interchange of fingerprint, facial, & scar mark & tattoo (SMT) information, ftp://sequoyah.nist.gov /pub/nist_internal_reports/sp500-245-a16.pdf, 2000, pp. 34-64.

[10] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints" IJCV, vol. 60, no. 2, 2004, pp. 91-110.

[11] J-E. Lee, A. K. Jain and R. Jin, "Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification", Biometrics Symposium, 2008, pp. 1-8.

[12] B. Heflin, W. Scheirer, and T. E. Boult, "Detecting and Classifying Scars, Marks, and Tattoos Found in the Wild", IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2012, pp. 31-38.

[13] S. Acton and A. Rossi, "Matching and Retrieval of Tattoo Images: Active Contour CBIR and Glocal Image Features", IEEE Southwest Symposium on Image Analysis and Interpretation, 2008, pp. 21-24.

[14] R. Gross and L. Sweeney, "Towards Real-World Face De-Identification", IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2007, pp. 1-8.

[15] J. Kovac, P. Peer and F. Solina, "Human Skin Colour Clustering for Face Detection", EUROCON, 2003, pp. 144-148.

[16] Y. Lin, S. Wang, Q. Lin and F. Tang, "Face Swapping under Large Pose Variations: a 3D Model Based Approach", IEEE International Conference on Multimedia and Expo, 2012, pp. 333-338.

[17] E. Reinhard, M. Adhikhmin, B. Gooch, et al., "Color transfer between images", IEEE Computer Graphics and Applications, vol. 21, no. 5, 2001, pp. 34-41.