ORIGINAL RESEARCH PAPER

Volume-8 | Issue-3 | March-2019 | PRINT ISSN No 2277 - 8179

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

VISUAL PRIVACY PROTECTION SCHEMES

Computer Science

Ms. Shabna M Asst. Professor, Dept of CSE, Cochin College of Engineering

Sonia Rehin R C* PG Scholar, Dept of CSE, Cochin College of Engineering *Corresponding Author

ABSTRACT

Recent widespread preparation and increased so-phistication of video surveillance systems have raised appre-hension of their threat to individuals right of privacy. Privacy protection technologies developed to this point have focused primarily on different visual obfuscation techniques .In this paper we tend to reviewed completely different VPP technics like blurring ,pixilation, image coding, face de-identification, inpainting etc. despite the fact that these technics give privacy to some extent, they wont give complete protection to user data. These techniques additionally need specification of Region of interest either manually or employing a computer vision module. This project proposes a way that provides complete VPP using false colors. This technique doesn't need to specify ROI.

KEYWORDS

Video Surveillance,Visual Privacy Protec-tion, Region of Interest, False Colors

I. INTRODUCTION

Video surveillance may be a quickly growing trade driven by low-hardware prices.Cameras[1] are unit employed in public areas for police work services in streets, parking heaps, banks, airports, train stations, searching centres, mu-seums, sports installations and plenty of others. In ancient video police work systems cameras are managed by human operators that perpetually monitor the screens sorting out specific activities or incidents thanks to difficulties of storing and analyzing this large quantity of multimedia system infor-mation in native servers, deferring these tasks to the cloud servers has gained quality. Privacy protection is associate increasing concern in trendy life, as additional and additional information on people is keep electronically, and because it becomes easier to access and distribute that information.

A major disadvantage in most of the prevailing privacy protection systems is that after the modifications are done on the video for the aim of privacy protection, the original video will not be retrieved. It's clear that the protection of the individuals privacy is of interest group in telecare applications moreover as in video police work, regardless whether or not they operate in camera or public areas. The most threats and risks of police work technologies like televi-sion system cameras, range plates recognition, geolocation[2] and drones. Another necessary issue associated with visual privacy is that is that the sensitive info or region of interest to be protected. In several works solely the face is obscured however that's not enough to guard visual privacy. Even once the persons face is obscured, different parts might exist within the image through that person identification could also be performed, as an example, exploitation logical thinking

channels and previous information like garments, height, gait, and therefore the like are often accustomed establish the person.This project aims to strike a balance between various criteria that are vital in visual privacy protection, namely privacy, intelligibility, reversibility, security, and robustness.

II. RELATED WORKS

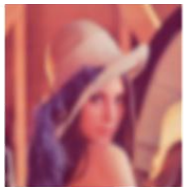
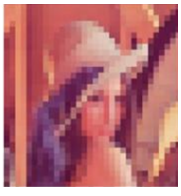
Image and video modification or redaction ways are the most common visual privacy protection ways. They modify the sensitive regions of a picture to hide personal info regarding the topics appearing on it. so as to work out the privacy sensitive regions in which a redaction methodology operates, computer vision algorithms are used.

A. Image Blurring and Pixelation

The filtering method involves eliminating the maximum amount noise as attainable whereas losing a minimum of knowledge. A blurring filter applies a Gaussian function[3] over a picture. This function modifies every element of a picture using neighbouring pix els. As a result, a blurred image is obtained during which the main pointsof sensitive regions are removed. The "Gaussian Blur" involves the convolution of a kernel, represented by a Gaussian perform, with the pixels of the image. The convolution in the discrete case is given by G(x; y) = 1=(2 ^{2})e$^{(}$ x^{2}=(2 ^{2}))

In image process, the Gaussian distribution has to be approximated by a convolution kernel. Therefore, values from this distribution are used to build a convolution matrix then applied to the initial image. every pixel's new value could be a weighted average of that pixel's neighborhood. Thus, the initial pixel's value receives the heaviest weight (having the best Gaussian value) and neighboring pixels receive smaller weights as their distance to the initial pixel will increase.If the image includes a high SNR, the utilization of the technique investigated here might worsen the image. The Gaussian blur is better used once the initial image includes a low SNR. Besides, though filtering pictures with a large variance within the Gaussian function blurs and worsens the image

The pixelize filter produces a mosaic impact across a pic-ture lower pictures in every row . It works by re sampling[4] an image a single video frame employing a coarser grid. The image is split into rectangles of equal space, wherever all of the pixels in square measureas a neighborhood are reset to the mean of their original colours. . As a result, a picture wherever the resolution of sensitive regions are

reduced is obtained. The pixelize filter is computationally cheap and might be applied in real time to video stream. The pixelize filter is wide utilized in existing prototypic privacy-preserving video media house applications, it should indeed be a poor selection of filter.Viewing a moving image de-creases the effectiveness of pixelation as an identity masking technique.

B. Image Encryption

Image and video encryption ways code imagery informa-tion in such some way that the initial information becomes unintelligible as will be determined in . The main goal of those ways is reliable security in storage and secure transmission of content over the network. usually used encryption algorithms like data encryption standard (DES), Rivests Cipher (RC5), Advanced encryption standard (AES), Rivest, Shamir and Adleman (RSA) and then on, are used. These algorithms guarantee the best security level however, unfortunately, they're not suitable for real-time video encryp-tion as a result of they're terribly time consuming.

These algorithms keep using text-based encryption how-ever encrypt solely a particular a part of the video bit-stream so on get real-time encryption. Different encryption algorithms have also been projected for real-time encryp-tion, specifically light-weight encryption algorithms These algorithms are suitable for real-time applications as a result of, once encrypting, they use an easy XOR cipher or only encrypt some bits of the video bit stream. Thereby, they're a lot of quicker than the primary ones. Finally, there are strate-gies supported scrambling .

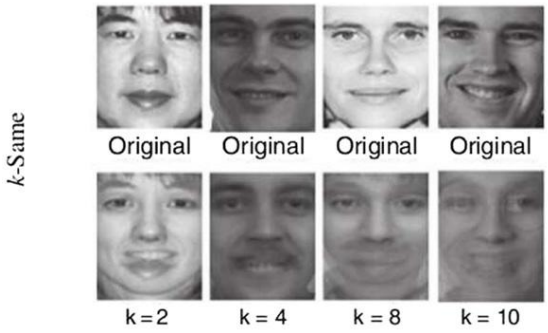
Ancient scrambling modify an analogue video signal like those found on television system cameras to form it unintelligi ble. However scrambling tech-niques are applied to digital videos within the field of video encryption. Scrambling algorithms are supported permutation only strategies during which transformed coefficients are then permuted so as to distort the resulting image.

Regarding selective encryption, AEGIS[5] is an algorith-mic program that uses DES to encrypt only the I-frames of the MPEG video bitstream. By ciphering I-frames, the needed B-frames and P-frames can't be reconstructed either. However, the algorithmic program isn't utterly secure due to partial information leakage from the I-blocks in P and B frames[6].Similarly, the video encryption algorithmic pro-gram proposed by Qiao et al(1997)[7] works with I-frames. It divides them in 2 halves that ar XORed and keep in one half. One of the half is encrypted using DES algorithmic program. though this algorithm is secure, it's not appropriate for time period applications. Raju, Umadevi, Srinathan, and Jawahar (2008)[?] analyse the distribution of the DCT coefficients (DC and AC) of compressed MPEG videos so as to develop a computa- tionally economical and secure encryption scheme for real-time applications.

DC and AC coefficients are managed otherwise relating to their visual influence, and electronic code block and cipher block chaining modes are interleaved to adapt the encryption method to the video information. The represented scheme uses RC5 for encrypting DCT coefficients. Boult (2005)[8] used DES and AES to cypher faces in JPEG pictures throughout compression in their privacy approach through invertible cryptographic obfuscation. the knowledge required for the decrypting method is keep within the JPEG file header. As for light-weight video encryption, Zeng and Lei (2003)[9] presented an efficient algorithm for H263 that operates within the frequency domain. Bit scrambling is em-ployed to rework coefficients and motion vectors throughout video coding while not touching the compression potency. By using this technique every frame of the resulting video is totally distorted. A cryptographic key is used to control the scrambling method, thereby authorized users are going to be able to undo the scrambling using the key.

C. Face de-identification

Face de-identification[10] consists within the alteration of faces to hide person identities. The goal is to change a face region in such away that it can't be recognised using face recognition software system.This formal model will preserve privacy, there aren't any guarantees of the utility of the infor-mation. The k-Same family of algorithms is oneof the recent and ordinarily used algorithms for face de-identification. K-Same was 1st introduced by Newton et al. (2005)[11]. Intu-itively, k-Same[12] performs de-identification by computing the typical of k face images in a very face set. Then, all of the pictures of the given cluster are replaced by the obtained average face. Using this rule, a de-identified face is representative of k members of the first used face set. This way, if the chance of a de-identified face of being properly recognised by a face recognition software system is not any more than 1/k



It's same that this rule provides k-anonymity privacy protection (Sweeney, 2002)[12]. However, despite the actual fact that this formal model will preserve privacy, there aren'tany guarantees of the utility of the information. The k-Same-based algorithms have some constraints. For instance, if a theme is represented quite once within the dataset then k-Same doesn't offer k-anonymity privacy protection. In order to handle this defect, Gross, Sweeney, Cohn, Torre, and Baker (2009) planned a multi-factor model that unifies linear, bilinear and quadratic models. By employing a generative multi-factor model, a face image is factorised into identity and non-identity factors. Afterwards, the de-identification rule is applied and also the de-identified face is reconstructed using the multi-factor model.

D. Image Inpainting

The Object and other people removal deals with con-cealing persons or objects showing in a picture or a video in such the way that there are not trails of them within the resulting changed version. concerning image inpainting, there are many approaches:texture synthesispartial differen-tial equations (PDE) impressed algorithms and ideal primarily based. In texture synthesis, an artificial texture derived from one portion of the image is employed to mend another portion.This artificial texture could be a plausible patch that doesn't have visible seams nor repetitive options. Algorithms supported texture synthe sis are able to fill in giant regions however at the cost of not conserving linear structures. PDE inspired algorithms reconstruct the gap using pure

(a) Real image (b) Modified image

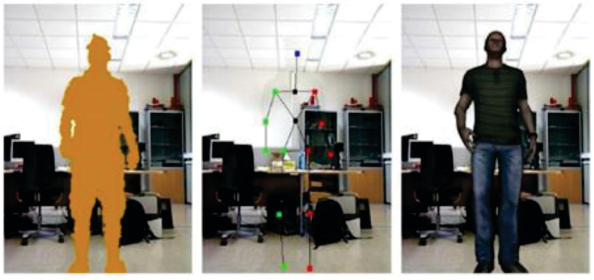
mathematics data to interpolate the missing components. A diffusion process propagates linear structures of equal grey price (isophotes) of the encircling space into the gap re-gion.Though these algorithms preserve well linear structures, the diffusion method introduces some blurring once filling in large regions. Finally, exemplar-based strategies are of spe-cific interest. rather than generating artificial textures, these strategies operate under the assumption that the knowledge that's necessary to complete the gap needs to be fetched from close regions of identical image. They generate newtextures by checking out similar patches within the image with that the gap is filled. Moreover, some exemplar-based algorithms additionally search the required information in databases of millions of pictures so as to finish the remaining information (Whyteet al., 2009)[13].

These algorithms mix the advances of texture synthesis and isophote-driven inpainting by a priority-based mecha-nism that determines the region filling order, thereby reduc-ing blurring caused by previous techniques. of the encircling space into the gap region. though these algo- rithms preserve well linear structures, the diffusion method introduces some blurring once filling in massive regions. Finally, exemplar-based ways are of specific interest. rather than gen- erating artificial textures, these ways operate below the assumption that the knowledge that's necessary to complete the gap needs to be fetched from near regions of a similar image. They generate newtextures by looking for similar patches within the image with that the gap is stuffed. Moreover, some exemplar-based algo- rithms additionally search the required info in databases of millions of pictures so as to complete the remaining info (Whyte et al., 2009)[13]. moreover, these algorithms usually mix the advances of texture synthesis and isophote-driven inpainting by a priority-based mechanism that determines the region filling order, thereby reducing blurring caused by previous techniques.

E. Visual abstraction/object replacement

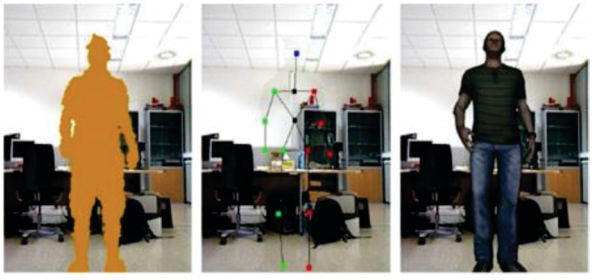
Object replacement involves the substitution of objects (or per sons) by a visual abstraction (or visual model) that pro-tects the privacy of an individual whereas enabling activity awareness. Common visual models might be some extent, a bounding box, a stick figure, a silhouette, a polygonal model etc. totally different works use visual abstraction and object replace ment. as an example, a silhouette illustration will be used as a visual abstraction of an individual (Tansuriyavong Hanaki, 2001)[14]. This removes data regarding textures whereas maintaining the form of the person, thereby com-

plicating the identification. A silhouette representation is employed, as an example, to preserve individuals pri- vacy during a fall detector and object finder system (Williams et al., 2006)[15]. Another illustration will be obtained by using an edge motion history image (Chen, Chang, Yan, Yang, 2007, 2009)[16]. By using this pseudo-geometric model, the complete body is obscured and therefore the person appears like a ghost within the final image. This method detects



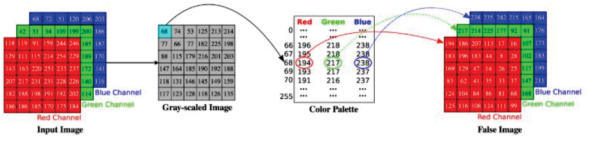
Solid silhouette Skeleton 3D avatar

edges of the body look and motion, accu- mulating them through the time, so as to smooth the noise, and partly preserve body contours. Chinomi et al. (2008)[17] pro- posed twelve operators for visual abstractions: as-is, transparent, monotone, blur, mosaic, edge, border, silhouette, box, bar, dot and transparency. so as to decide on among one in every of them, the relation- ship between the topic beingmonitored and therefore the viewer is taken into account. additionally to the illustration that are seen so far, 3D avatars will be used too. Avatar creation (Sadimon, Sunar, Mohamad, Haron, 2010) may be a terribly fascinating field with straight-forward application in visual abstraction in addition. Lyons, Plante, Jehan, Inoue, and Akamatsu (1998)[18] conferred a technique that uses automatic face recognition and physicist moving ridge rework for making avatars. It mechanically extracts a face from a picture, and build a individualised avatar by rendering the face into a generic avatar body. However, on condition that the avatar maintains recognisable aspects of the face, privacy wouldn't be protected.



Solid silhouette Skeleton 3D avatar

F. False Color Based VPP



In image process, false colours are sometimes used as a visualization aid to represent otherwise invisible informa-tion.Recently, false colours are used for the aim of visual privacy protection. to this end, an RGB input image is initial transformed into grayscale. The 8-bit grayscale value is then used to index into an RGB color table (i.e. palette) and therefore the corresponding RGB triplet is employed to exchange the initial picture element value the first advantage of false color based mostly VPP is that it can be applied on the whole image while not compromising intelligibility. In alternative words, choice of a ROI isn't required, that makes this technique strong against the fragility of computer vision algorithms that aim to find sensitive regions.

III. CONCLUSIONS

Privacy protection methods mainly focus on preserving visual privacy in images correct detection is fundamental in order to make protection methods work as desired. Blurring and, to a lesser extent, pixelation may provide a balance, but it would be a precarious balance at best. it seems that image filters can hardly provide a balance between privacy and information utility, and generally privacy loses in this balance. Nevertheless, when such a balance is not needed, image filters may be used. Like inpainting techniques, en-cryption ones have high computational requirements. The
election of which protection method to use depends on the application requirements.

Common definitions about what visual privacy should be, when privacy is protected, which are the sensitive areas, and so on are needed. correct detection is fundamental in order to make protection methods work as desired. pri vacy and intelligibility trade-off is the main issue in the case of blurring and pixilation. More effective and reliable visual privacy protection methods and systems are required increase the users acceptance of using video cameras in private spaces.

REFERENCES

[1] A. Senior and A. W. Senior, Protecting privacy in video surveillance. Springer, 2009, vol. 1.
[2] J. R. Padilla-Lopez,´ A. A. Chaaraoui, and F. Florez´-Revuelta, “Visual privacy protection methods: A survey,” Expert Systems with Applica-tions, vol. 42, no. 9, pp. 4177–4195, 2015.
[3] E. S. Gedraite and M. Hadad, “Investigation on the effect of a gaussian blur in image filtering and segmentation,” ELMAR Proceedings, pp. 393–396, 2011.
[4] M. Boyle, C. Edwards, and S. Greenberg, “The effects of filtered video on awareness and privacy,” in Proceedings of the 2000 ACM conference on Computer supported cooperative work. ACM, 2000, pp.1–10.
[5] G. A. Spanos and T. B. Maples, “Performance study of a selective encryption scheme for the security of networked, real-time video,” in Computer Communications and Networks, 1995. Proceedings., Fourth International Conference on. IEEE, 1995, pp. 2–10.
[6] I. Agi and L. Gong, “An empirical study of secure mpeg video transmissions,” in Network and Distributed System Security, 1996., Proceedings of the Symposium on. IEEE, 1996, pp. 137–144.
[7] L. Qiao, K. Nahrstedt et al., “A new algorithm for mpeg video encryption,” in Proc. of First International Conference on Imaging Science System and Technology, 1997, pp. 21–29.
[8] T. E. Boult, “Pico: Privacy through invertible cryptographic obscura-tion,” in Computer Vision for Interactive and Intelligent Environment, 2005. IEEE, 2005, pp. 27–38.
[9] W. Zeng and S. Lei, “Efficient frequency domain selective scrambling of digital video,” IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 118–129, 2003.
[10] S. L. Garfinkel, “De-identification of personal information,” NISTIR, vol. 8053, pp. 1–46, 2015.
[11] E. M. Newton, L. Sweeney, and B. Malin, “Preserving privacy by de-identifying face images,” IEEE transactions on Knowledge and Data Engineering, vol. 17, no. 2, pp. 232–243, 2005.
[12] L. Sweeney, “k-anonymity: A model for protecting privacy,” Inter-national Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557–570, 2002.
[13] O. Whyte, J. Sivic, and A. Zisserman, “Get out of my picture! internet-based inpainting.” in BMVC, vol. 2, no. 4, 2009, p. 5.
[14] S. Tansuriyavong and S.-I. Hanaki, “Privacy protection by concealing persons in circumstantial video image,” in Proceedings of the 2001 workshop on Perceptive user interfaces. ACM, 2001, pp. 1–4.
[15] A. Williams, D. Xie, S. Ou, R. Grupen, A. Hanson, and E. Riseman, “Distributed smart cameras for aging in place,” MASSACHUSETTS UNIV AMHERST DEPT OF COMPUTER SCIENCE, Tech. Rep., 2006.
[16] D. Chen, Y. Chang, R. Yan, and J. Yang, “Tools for protecting the privacy of specific individuals in video,” EURASIP Journal on Advances in Signal Processing, vol. 2007, no. 1, p. 075427, 2007.
[17] K. Chinomi, N. Nitta, Y. Ito, and N. Babaguchi, “Prisurv: privacy protected video surveillance system using adaptive visual abstraction,” in International Conference on Multimedia Modeling. Springer, 2008, pp.144–154.
[18] M. Lyons, A. Plante, S. Jehan, S. Inoue, and S. Akamatsu, “Avatar creation using automatic face processing,” in Proceedings of the sixth ACM international conference on Multimedia. ACM, 1998, pp. 427– 434.