A SURVEY ON DIFFERENT VISUAL PRIVACY PROTECTION TECHNIQUES FOR SURVEILLANCE

[1]Vishnu C K, [2]Dr. Arathy T
[1]MTech in VLSI and Signal Processing,LBS College of Engineering Kasaragod
[2]Assistant professor,Department of ECE, LBS, College of engineering Kasaragod
[1]thekkeparayil25@gmail.com , [2]arathiviswam09@gmail.com,

Abstract- Protection of visual privacy is one of the major component of video surveillance systems. Due to difficulties of storing and analyzing multimedia data in local severs deferring these tasks to cloud servers has gained popularity. This increases privacy concerns that such data can also acquired by unauthorized parties. This gives rise to various data hiding schemes. There are different methods of visual privacy protection such as false color based privacy protection, photo sharing based on secure jpeg,MPEG encryption and decryption, etc. A survey on different privacy protection techniques is explained.

Index Terms-False color, data hiding,JPEG, MPEG

I. INTRODUCTION

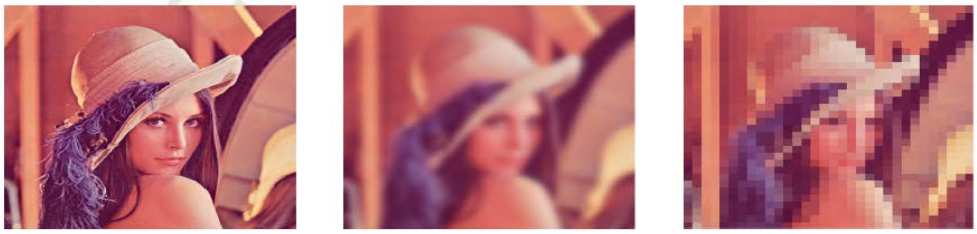
Sharing photos online is a common activity on social networks and photo hosting networks such as facebook , Instagram, flickr or pinterest. However after reports of citizens surveillance by governmental agencies and scandalous leakage of celebrities private photos online, people have become concerned about their online privacy and looking for ways to protect it. Popular social networks typically offer privacy protection solutions only in response to the public demand and therefore are often rudimental, complex to use and provide limited degree of control and protection. Most solutions either allow user who can access the shared photos or for how long they can accessed.

Due to difficulties of storing and analyzing this huge amount of multimedia data in local servers deferring these tasks to cloud servers has gained popularity. This increases privacy concerns that such data can also be acquired by unauthorized parties. This gives rise to various data hiding schemes in which data stored in servers are encrypted in a reversible manner,either as ciphertext[1] or as plaintext [2].

Visual Privacy is the relationship between collection and dissemination of visual information and the legal issues surrounding them and the expectation of privacy. Now a days cameras are everywhere. They are one of the most common sensors found in electronic devices, ranging from tablets to smartphones, and surveillance cams to lap tops. Privacy implications surrounding it limit its ability to seamlessly blend into our computing environment.The world population is increasing day by day. Therefore, this situation will not be sustainable in the near future, unless new solutions for the support.

A. Image filtering

To make various effects on images image filtering uses image filters to privacy sensitive regions.



(a) Lena (b) Lena with Gaussian Blur (c) Lena Pixelation

Fig. 1 Several examples of image filtering methods: (a) the original image without any modification, (b) image modified by applying a Gaussian Blur filter, and (c) image modified by a pixelating filter.

Image filtering methods using blurring and pixilation is illustrated in Fig.1. Blurring and pixilation [3] are two different visual privacy protection (VPP) methods that are based on ROI (region of interest).

In blurring a gaussian function is applied to an image. This Gaussian function modifies each pixel of an image using neighboring pixels. It update each pixel value with a Gaussian average of its neighborhood.Blurring is widely usedin Google Street View to modify human facesand number plates.

A pixelating filter divides an image into a gridof eight-pixel wide by eight-pixel high blocks. The average colorof the pixels of each block is computed and the resultant coloris assigned to all of the pixels belonging to that block. As a result,an image where the resolution of sensitive regions have beenreduced is obtained. Pixelating is commonly used in television to preserve the anonymity of suspects, witnesses or bystanders.

Hill, Bruce and Lander evaluated effectiveness of pixilation and blurring in conserving privacy. Results indicates that participants can identify some of the faces.

Disadvantages – 1) The complete information cannot be recovered completely.

2) Will also effect the intelligibility of non-sensitive content.

B. Privacy preserving based on secure JPEG

Secure JPEG is an open, flexible, reversible and formatcompliant framework to secure JPEG images, which allows anefficient integration and use of different security and privacyprotection tools [4]. Information aboutthe original pixels and protected metadata, along with theprotection parameters are securely hidden in one or more JPEGapplication markers. Protection and reconstruction relies ona or more secret keys, which are transmitted separately in asecure way between a sender (a person who shares a photo)and trusted recipients (trusted people to share photo with).Multiple regions can be protected with different keys to enablehierarchical privacy protection.

Visual privacy in a JPEG photo can be protected usingdifferent visual distortions classified into two main types:

1) Pixel replacement:these techniques replace the pixels of an original image with other masks, distortions, or patterns. Simple blurring, pixilation, masking, or more complex methods such as inpainting can be used to replace the original pixel regions. The original pixels are then compressed, encrypted, and embedded, together with information about position and shape of the processed regions, via one or more APPn markers inside JPEG header. Reconstruction of original image is performed by extracting from JPEG header, decrypting, and placing back the original pixels.
2) Data manipulation: these techniques do not replacethe original pixels but change them in a specificway. Typical examples include image encryption andscrambling, which modify the original values of imagepixels, DCT coefficients, or bitstream in a

reversibleway with the help of a secret key. Only informationabout the shape of the protected regions needs to beembedded in APPn markers. Therefore, these methodsintroduce less overhead to the image bitrate comparedto pixel replacement methods. Only a correct secretkey is needed for the reconstruction of the originalimage.

Secure JPEG can be used for sharing photos on social network such as facebook, pinterest, twitter, etc.

Disadvantages – 1) This method cannot be used on full frames as it would destroy the intelligibility of the data.

2)It is targeted toward social photo sharing applications, rather than to be used for surveillance.

C. Face de-identification

Face-based identification is used in various applicationscenarios - from identification of a person based on stillimages in passport or identity card, to identification based onface images captured by a surveillance system without thecooperation of the person. In many application scenarios, especially in video surveillance,privacy can be compromised. De-identification is the process of concealing or removing personal identifiers, or replacing them with surrogate personal identifiers in personal information, in order to prevent the disclosure and use of data for purposes unrelated to the purpose for which the information was originally obtained. Personal information is any information relating to a person. Personal identifiable information (or personal identifier) is the personal information, which allow his or her identification.The k-Same family of algorithms implements the k-anonymity protection model for face images. It scientifically limits the ability of face recognition software to reliably recognize faces while maintaining facial details in the images. The algorithm determines similarity between faces based on a distance metric and creates new faces by averaging image components, which may be the original image pixels or eigenvectors. Faces de-identified using k-same algorithm is shown in Fig.2.

Disadvantages – They either require face regions to be manually marked or rely on face detection algorithm.

D. Visual privacy protection using false colors

Recently, false colors[7] are used for the purpose of visual privacy protection. To this end, an RGB input image is first transformed into grayscale. The 8-bit grayscale value is then used to index into an RGB color table (i.e. palette) and the corresponding RGB

Fig.2 Faces de-identified using the k-Same-Select algorithm

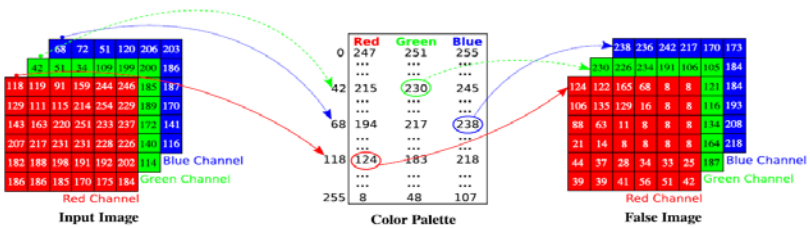


Fig.3 False color based visual privacy protection

triplet is used to replace the original pixel value (see Fig. 3). This approach has been applied for both images [5] and video [6].The input image is converted to false image using a color palette.The primary advantage of false color based VPP is that it can be applied on the entire image without compromising intelligibility. In other words, selection of a ROI is not required, which makes this method robust against the fragility of computer vision algorithms that aim to detect sensitive regions. However, this method is not fully reversible due to two reasons: 1) The original color to grayscale conversion dismisses the color information and 2) the color palettes are typically not one-to-one, which means that two different grayscale values may get mapped to the same color value rendering the recovery of the original grayscale value impossible. Two schemes are used here. The second scheme shows better performance compared to first.In scheme 1 input image is first converted to grey scale image then to false image.

Protection pipeline: The main workflow of thescheme (scheme-2) is shown in Fig. 4. However, this scheme capitalize on the coherence between the original image and the inverted false color image to significantly reduce the size of the protect image.In this scheme, the false color image, *FI*, is computed somewhat differently to avoid color-to-gray conversion.

For each color value I_C(x,y) in the original image, the corresponding false color value FI_C(x,y) is computed as

$$FI_C(x,y) = P_C[I_C(x,y)] \quad (1)$$

Where P_C denotes the C^{th} channel of the color palette P.

Next, after $FI_C$is encoded and decoded, instead of directly subtracting it, we first apply an inverse table look-up to obtain

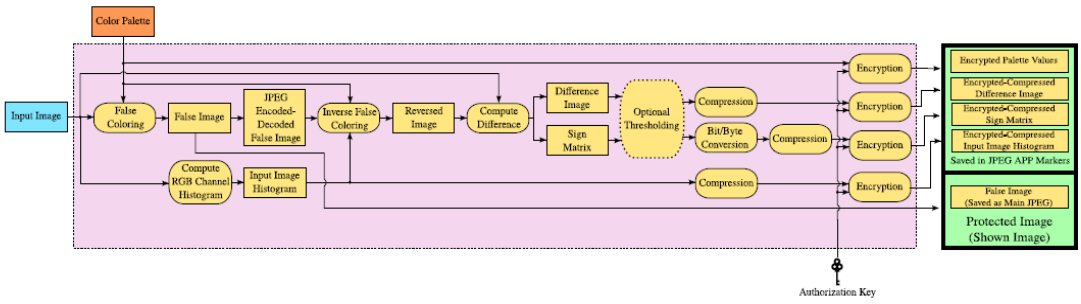


Fig.4 Protection pipeline

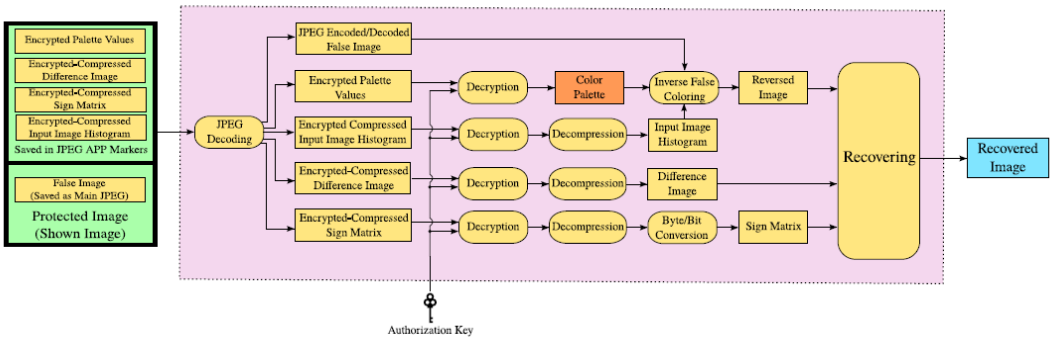


Fig.5 Recovery pipeline

$$I_C'(x,y)=P_C inv[FI_C'(x,y)] \quad (2)$$

Here, P_C^{inv} represents a pseudo-inverse of the C^{th} channel of the color palette. We call it pseudo-inverse as most color palettes are not one-to-one and therefore non-invertible. In practice, given, we search inside P_C to find the index of the most similar color value

$$I_C'(x,y) = \underset{i \in \{0,1,\ldots\ldots\ldots,255\}}{\arg\min} |P_C(I) - FIC'(x,y)| \quad (3)$$

If there are multiple such values that minimize this difference, we choose the index according to the histogram of the original image. For example, if i = 5 and i = 125 are two solutions of (3), and hist(I_C)[125]> hist(I_C)[5], we choose 125 as the inverse. This ensures that the inverted value will be similar to the original value for the maximum number of pixels. Once I_C' is computed in this fashion, it is subtracted from I to obtain the difference and sign images.

$$DI_C(x, y) = |I_C(x, y) - I_C'(x, y)| \quad (4)$$

where (x, y) indicates the pixel index and c Є{R, G, B}.

$$SI_C(x,y) = \begin{cases} 1 & if\ I_C(x,y) - I_C'(x,y) < 0 \\ 0 & otherwise \end{cases} \quad (5)$$

Furthermore, an opportunity for a different type of lossy compression presents itself in this particular case. Depending on a quality threshold, τ, all values in DI that are smaller than τ may be set to zero

$$DIC'(x,y) = \begin{cases} 0 & if\ DIC(x,y) < tau\ DIC(x,y) \\ DIC(x,y) & otherwise \end{cases} \quad (6)$$

Recovery Pipeline: In the recovery pipeline of the second scheme (Fig. 5), first all encrypted metadata is decrypted followed by decompression, if needed. Then using the decoded false color image FI, the input image histogram hist(I_C), and the color palette P, an approximate of the original image, I is computed using (2). This image is then combined with the difference and sign images using

$$R_C(x, y) = I_C'(x, y) + sDI_C(x, y)$$

II. RESULTS

The original image, generated false image is given in Fig.6.

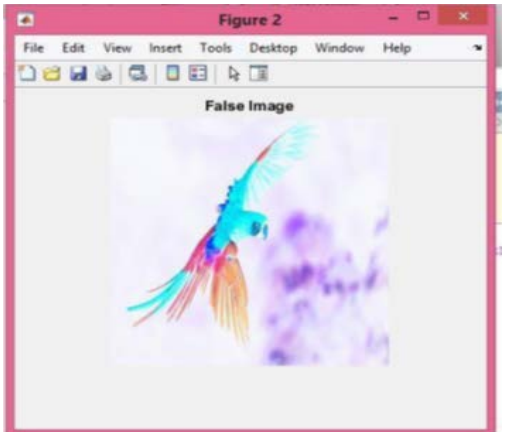


Fig.6 Input image and False image

The sign matrix image and difference image is shown in Fig.7

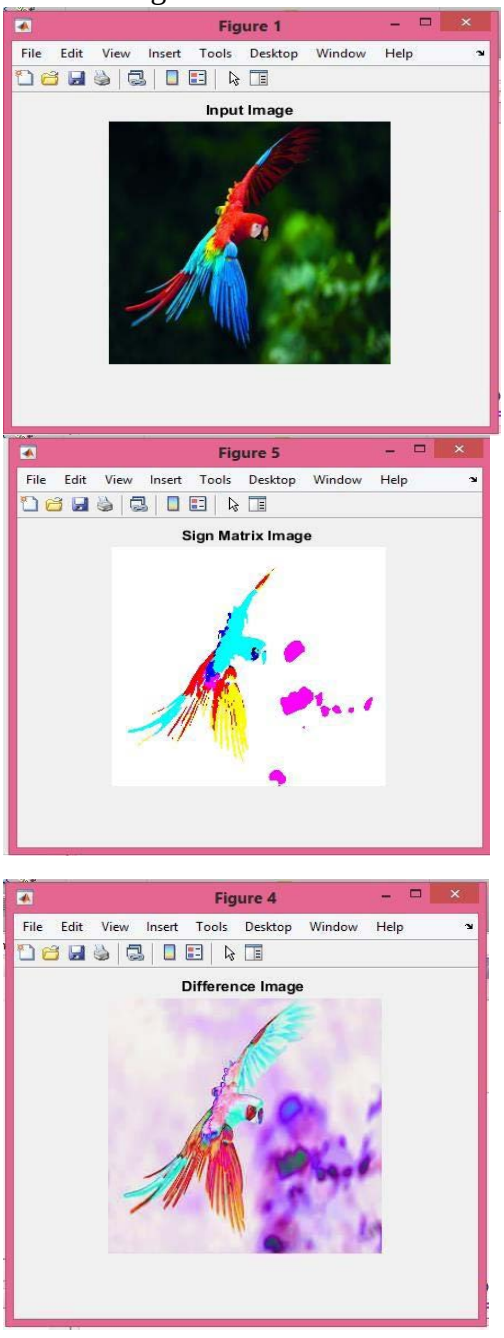


Fig.7 sign and difference image

In our experiments, we first analyzed a large number of color palettes available in National Library of Medicine Insight Segmentationand Registration Toolkit (ITK) [8]. We decided touse 3 color palettes based on their apparent effectiveness inpreserving privacy. Among these, the *Blues* palette has a moremonotonic variation of colors, *Hardcandy* is extremely erratic,and the *Green-Pink* is in-between. These palettes are shown in Fig. 8 together with 3D scatter plots that show the path traversedby each palette within the RGB color space.

Table I Comparison between SSIM values of scheme-1 and scheme-2

	Q=10		Q=50		Q=85	
	Scheme-1	Scheme-2	Scheme-1	Scheme-2	Scheme-1	Scheme-2
Blues	0.7346	0.9516	0.8118	0.9692	0.8534	0.9706
Dark2	0.7959	0.9507	0.8126	0.9594	0.8234	0.9722
Greens	0.6988	0.9327	0.8287	0.9609	0.8360	0.9800

Table II Face recognition accuracy rates

	Video 1	Video 2	Video 3	Video 4	Video 5	Video 6	Average
Blurring	0.73	0.47	0.56	0.60	0.65	0.53	0.59
Pixelation	0.78	0.61	0.55	0.58	0.69	0.54	0.62
False Coloring	0.64	0.43	0.54	0.55	0.69	0.60	**0.57**

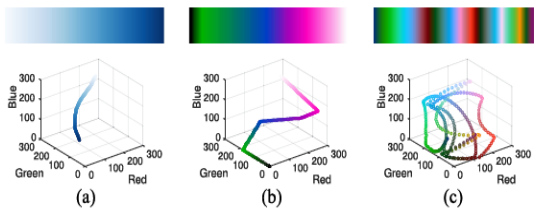


Fig.8 Characteristics of the color palettes used in this study. a) *Blues*. b) *Green-Pink* c)*Hardcandy*.

The comparison between SSIM values of scheme-1 and scheme-2 for different quality factor is given in the table I.Compared to scheme-1, scheme-2 shows better performance in terms of SSIM (structural similarity index). SSIM is a perceptual metric that qualifies image quality degradation caused by processing such as data compression or by lossy data transmission. The range of SSIM values extends between -1 and +1.

Comparison between Face recognition rates are shown in Table II.In Table II, it can be seen that the mean face recognition rate forfalse coloring, 0.57, is the lowest among the compared methods(0.59 for blurring and 0.62 for pixelation).

III. CONCLUSION

Comparison between different methods of visual privacy protection for surveillance is done. Five important terms n visual privacy protection are *privacy*, *intelligibility*, *reversibility*, *security*, and *robustness*. More specifically our goals are: 1) An individual recorded in a security video should not be easily identifiable by human observers and face recognition algorithms (privacy); 2) the privacy protected video should still allow identification of suspicious behaviors and gathering of non-sensitive information such as the number of

people in a given area (intelligibility); 3) in case of a crime, the privacy protected footage could be reversed to obtain the original unprotected footage by authorized users (reversibility); 4) this reversal could only be performed by legally authorized parties and not by any third parties who may have acquired the protected content by some means (security); and 5) privacy protection should be robust in that it should not depend on fragile computer vision algorithms or manual annotations that may fail to detect sensitive regions in some frames (robustness).
The disadvantages of privacy protection methods such as image filtering, secure JPEG and face de-identification methods are: 1) the complete information cannot be recovered completely.2) Will also effect the intelligibility of non- sensitive content.

False color based image privacy protection provide all five goals mentioned above and provide better results.

REFERENCES

[1] Z. Qian, X. Zhang, and S. Wang,"Reversible data hiding in encrypted JPEG bitstream," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1486–1491,Aug. 2014.

[2] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Trans. Multimedia, vol. 18, no. 8, pp. 1469–1479, Aug. 2016.*

[3] K. Lander, V. Bruce, and H. Hill, "Evaluating the effectiveness of pixilation and blurring on masking the identity of familiar faces," *Appl.Cognitive Psychol.*, vol. 15, no. 1, pp. 101–116, 2001.

[4] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharingbased on a secure JPEG," in *Proc. IEEE Conf.Comput.Commun.Workshops*,Apr./May 2015, pp. 185–190.

[5] S. C¸ iftc¸i, P. Korshunov, A. O. Aky¨uz, and T. Ebrahimi, "Using falsecolors to protect visual privacy of sensitive content," in *Proc. IS&T/SPIEElectron. Imaging*, 2015, pp. 93 941L–93 941L.

[6] S. C¸ iftc¸i, P. Korshunov, A. O. Aky¨uz, and T. Ebrahimi, "Mediaeval 2015drone protect task: Privacy protection in surveillance systems using falsecoloring," in *MediaEval Benchmarking Initiative Multimedia Eval.*, 2015.[Online]. Available: http://ceur-ws.org/Vol-1436/

[7]Serdar C¸ iftc¸i , Ahmet O˘guz Aky¨uz, and Touradj Ebrahimi, *Member, IEEE,"A Reliable and Reversible Image Privacy Protection Based on False Colors"*.IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 20, NO. 1, JANUARY 2018.

[8]J. Tesic, *"Metadata practices for consumer photos,"* IEEE MultimediaMag., vol. 12, no. 3, pp. 86–92, Jul./Sep. 2005.