Neural Comput & Applic (2017) 28 (Suppl 1):S91–S95
DOI 10.1007/s00521-016-2323-7

ORIGINAL ARTICLE

High capacity information hiding for privacy protection in digital video files

Ahmed Elhadad[1] · Safwat Hamad[2] · Amal Khalifa[2,3] · A. Ghareeb[1]

Received: 1 February 2016 / Accepted: 6 April 2016 / Published online: 21 April 2016

Abstract In this paper, a framework to hide privacy in video is proposed based on data hiding principals. A novel data hiding technique is proposed and implemented to hide the original frame into the in-painted one. The proposed hiding technique is carried out in the discrete wavelet transform domain of the cover video. The proposed technique is embedding video into video. Furthermore, the proposed data hiding method can blindly reconstruct the original frame from the fake one. Experimental results showed that the proposed method can successfully hide the complete frames of the original video into their corresponding in-painted ones that are as large as themselves. Simple visual inspection of the results showed that the quality of the stego-frames maintain very high (above 45 dB) while providing an acceptable visual quality for the retrieved original frames.

Keywords Information hiding · Privacy information framework · Capacity

✉ Ahmed Elhadad
ahmed.elhadad@sci.svu.edu.eg

[1] Department of Mathematics and Computer Science, Faculty of Science, South Valley University, Qena, Egypt

[2] Department of Scientific Computing, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

[3] College of Computer and Information Sciences, Princess Nora Bint Abdulrahman University, Riyadh, Kingdom of Saudi Arabia

1 Introduction

Recently, private business such as jewelery stores and supermarkets or public service facilities are under risk of robbery, human scuffles or crimes. Therefore, surveillance systems play an important role in recording and monitoring of any normal/abnormal behavior to protect human property or themselves. Previous surveillance tools such as long distance glasses and radios were mainly used by spy groups. Currently, surveillance monitoring is a very wide field that has many associated modern technologies such as closed-circuit television [1], radio-frequency identification [2], night vision cameras [3] and global positioning system [4]. These are usually used for managing security personnel, track and monitor threats, and prevent/investigate criminal activities.

Sometimes surveillance systems violate "the right to privacy"; however, many countries have different constraints to protect privacy information. De-identification is one of the techniques that has recently introduced for ensuring or supporting privacy. In this work, de-identification refers to the process of scrambling or removing a pre-identifiable person from the recorded multimedia files. On the other hand, re-identification is the inverse process of the de-identification in which individuals are identified and their privacy information is revealed.

In fact, re-identification becomes crucial in many situations especially in the case of crimes. Hence, most privacy techniques focus on modifying the original scene by removing and replacing private parts using black boxes, blurring or in-paint hiding. However, it is almost impossible to correctly regenerate the original video through the re-identification process. Therefore, hiding techniques were introduced with the de-identification approaches. Data hiding—commonly known as steganography—is the art

and science of embedding secret data within a carrier. The carrier can be the form of any medium used to convey information, including wood tablets, tiny photographs or word arrangements. Modern steganographic techniques utilize different kinds of digital data such as sound tracks, images, videos and even 3D objects [5].

In this paper, we propose a novel high capacity hiding technique that allows embedding privacy information after the de-identification process takes place. Later, the embedded information can be retrieved to facilitate the re-identification process of the original scene. A secret key must be involved in order to ensure that the re-identification process is made by authorized users only.

2 Related work

In De-identification systems, hiding privacy methods start by removing authorized persons from the scene. In [6] Wickramasuriya et al. under title "Privacy Protecting Data Collection in Media Spaces," introduced an integrated framework that combines between sensors and video streams to select privacy details and scene view, respectively. Depending on authorization, the video stream is further viewed without the authorized persons. The privacy details are hidden using blurring filter, pixel coloring or bounding box. Although this approach is a good start in privacy, it is difficult to retrieve the original video when needed.

After that, Zhang et al. [7] proposed a method of storing privacy information in surveillance video as a watermark. This approach hides the privacy information and it becomes entirely invisible. On the other hand, authorized person can use a secret key to view the original video, including the privacy information. Unauthorized access cannot reconstruct the privacy details without the secret key, even in the exact algorithm of the surveillance system which is known to the attacker. Firstly, the authors used an identity sensor (e.g., RFID) to detect the authorized person. Secondly, they extracted the corresponding foreground object in each frame. Next, resultant frames are both compressed and encrypted. After that, the blobs left behind the foreground objects are filled in by the background model. Finally, the compressed foreground frames are embedded into the background frames.

Cheung et al. [8] described privacy protection in video surveillance system. In this system, the captured video is fed into the object identification and tracking unit to extract the foreground frames. Furthermore, the OIT unit visually tracks all moving objects in the scene and correlates them using RFID system and cameras. Next, image objects are extracted from the video and replaced by black background. After that, the compressed bit-streams are encrypted along with other auxiliary information used by the privacy data management system. The empty regions left behind by the removal of objects are perceptually filled in the video in-painting unit. The resulting protected video forms the cover work for hiding the encrypted compressed bit-streams using a perceptual-based rate-distortion optimized data hiding scheme. The data hiding scheme is combined with a H.263 encoder which produces a standard compliant bit-stream of the protected video to be stored in the database. The protected video can be accessed without any restriction as all the privacy information is encrypted and hidden in the bit-stream.

3 Proposed hiding method

Almost privacy techniques focused on modifying the original video by adding noises or removing and replacing the private parts so it is hard to retrieve the original video correctly. Hence, hiding techniques such as watermarking and in-painting are proposed [7, 8]. Therefore, a new hiding technique with improved privacy is proposed and implemented. In this technique, the original video will recovered by a secret key. In this paper, it is assumed that the video surveillance data are a video frames. Each movie frame is a single picture or still shot that is shown as part of a larger video or movie [9]. Hence, each frame can be selected on its own to print out a single image. In addition, each frame has an input mask that represents the privacy information related to it. For that reason, a privacy management system is needed to deliver the privacy information details for each frame in the original video. The privacy management system described in [10] is used to accomplish this task.

Wavelets and wavelet transforms are important to both researchers and practitioners in computer graphics and image processing because they are a natural step from the classic Fourier techniques. The general idea behind using wavelets in the proposed hiding method is simply to look at the wavelet coefficients as an alternative representation of each frame. So instead of performing operations on the spatial domain (pixels) of the frames, we can work with the wavelet coefficients. This gives us the opportunity to take advantage of their multi-resolution structure.

Here, the discrete wavelet transform (DWT) properties are used to develop the proposed hiding technique. In this technique, the original frame "*secret frame*" is embedded into its corresponding frame with removed private information "*cover frame*." Both secret and cover frames are normalized and their pixels will be on the interval [0, 1]. Thus, after applying discreet wavelet transform on the video frame, the coefficients values of the approximation region will be within the interval [0, 2] while horizontal,

vertical and diagonal coefficients values are going to be on the interval [−1, 1]. As a result, we construct the following equation system for embedding the secret frame pixels in the transformed regions of the cover frame coefficients:

$$\text{Stego}^{s}_{x,y} = \frac{2}{\beta}(\text{Msg} + i), \quad \frac{2i}{\beta} \leq \text{Cover}^{s}_{x,y} < \frac{2(i+1)}{\beta}$$

$$i = \begin{cases} 0, 1, 2, 3, \ldots(\beta - 1), & S = A \\ -2, -1, 0, 1, \ldots(\beta - 3), & S = H, V, D \end{cases} \quad (1)$$

where in these equation system, $\text{Stego}_{x,y}$ refer to the current coefficient in the *final frame*, *Cover* is the corresponding coefficient in the *cover frames*, Msg is the embedded pixel in the *secret frame* and β is the number of intervals which satisfy that the cover frame on the interval of [0, 2] or [−1, 1] corresponding approximation coefficient A and horizontal, vertical and diagonal coefficients H, V and D, respectively. Finally, the inverse wavelet transform is used to reconstruct the faked frame with secret embedded original frame.

Before the embedding process takes place, a preprocessing step is applied on the secret frames. This process is used for adjusting the pixels values of the secret frame using α, in order to avoid the truncation errors. This ensures that the embedded message will be recovered correctly. In addition, a secret key is used to improve security against attacks.

4 Application to hiding in-paint privacy information details framework

Figure 1 shows a detailed diagram of hiding in-paint privacy information framework in a basic layer view. The framework includes three main parts: presets layer, hide in-paint layer and recapture original video layer. First layer is the presets; in this layer, background modeling and privacy management system receive the original video from the surveillance scene cameras where the background modeling reconstructs suitable background from the scene. Here, we assume that the cameras are fixed, so the background can be generated using the Gaussian background model. In the same time, the privacy management system described in [10] receives the original video to reconstruct the private information video where the frames will be in black only and the privacy details (mask) will be left as it is. In this research, the main focus is on the second layer (hide in-paint) where the private information is removed depending on the generated background model. Then, the proposed hiding technique uses a secret key to hide the original frame into the modified one. Finally in the case of crimes or urgent cases, only authorized person with the secret key can extract the original frames from the faked ones. Keeping in mind the blindness of the proposed hiding technique, authorized access can watch the original scene frames only by using the secret key.

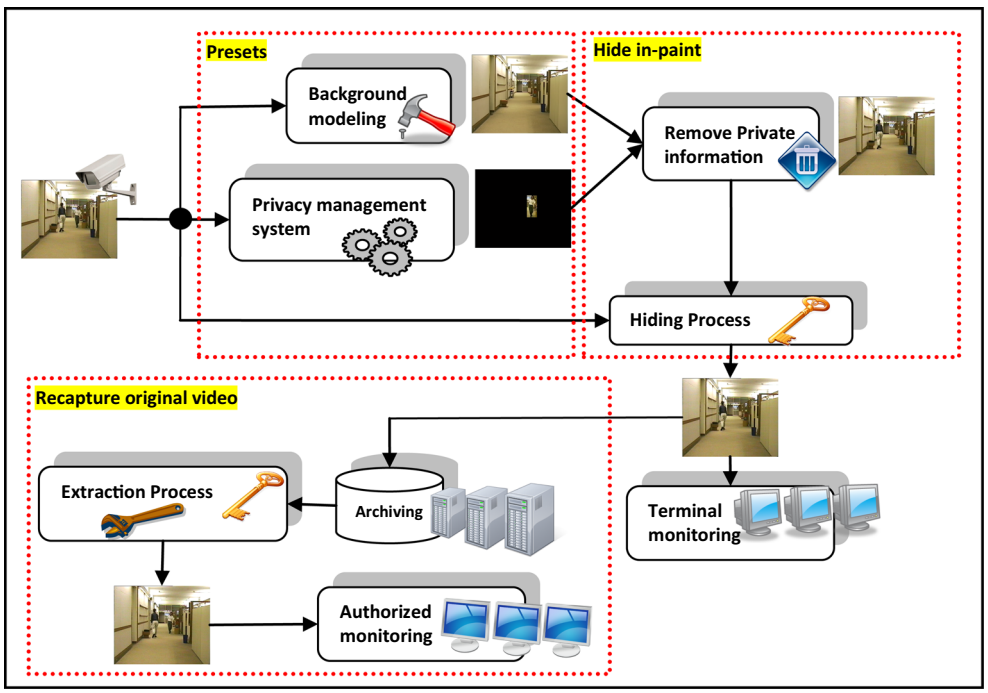


Fig. 1 Hiding in-paint privacy information details framework

5 Experimental results and discussion

5.1 Implementation

This research focuses on hiding private information details in the modified scene of surveillance system frames. Therefore, we developed MATLAB code using common Image Processing Tool Box and data file management. In addition, "*Hall monitor*" avi video files in [11] are tested as input. Hence, "*hall-org.avi*" and "*hall-private.avi*" video files are used for original video scene and private information details, respectively. Original and private information details video files include 299 frames, RGB color format, uint8 data type and 288 × 352 frame size. However, the modified original video without privacy information and final faked video are mj2 files including 299 frames, RGB color format, uint16 data type and 288 × 352 frame size. Figure 2 shows sample of frame 150 in all files inputs and result files. Figure 2a–d illustrates the original video, background model, private information (mask) and the original video without private information, respectively. On the other hand, Fig. 2e, f shows the correspondence resultant frame when $\beta = 100$ and 600, respectively.

6 Discussion

In this subsection, the proposed hiding technique performance is discussed according the faked and extracted video files. The most popular hiding quality test is *peak signal-to-noise ratio* "PSNR." PSNR is defined as the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. PSNR is an approach to human observation of invisibility quality. Generally, PSNR is measured in decibels (dB) and higher values refer to higher quality invisibility.

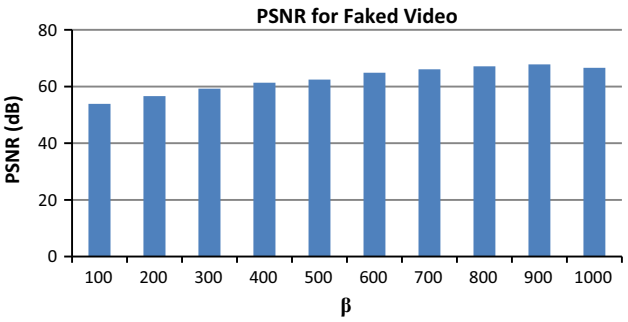
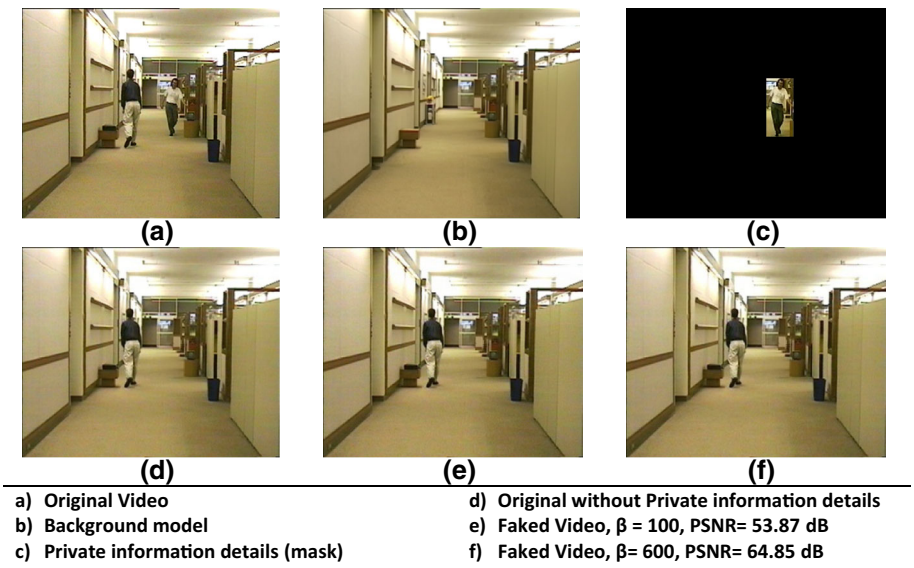


Fig. 3 Peak signal-to-noise ratio "PSNR" of the proposed method at different values of β

In the proposed hiding technique, the original frame is hidden instead of the private information details (mask). In this case, the required capacity will be 100 % to embed the original frame into the modified frame without privacy information using the in-paint technique. In addition, the proposed hiding technique performs increasing PSNR values. The proposed hiding equation system (1) depends on a new parameter called "β." β refers to the number of intervals used to divide the values in the wavelet transformed domain. Figure 3 shows the average results of PSNR for faked video frames with the values of intervals β from 10 to 1000 where the minimum value of PSNR is 53.88 dB. On the other hand, Fig. 4 represents the similarity between the extracted video and the original video. The similarity is measured in percent and the result is up to 99.81 % for the various values of β.

Fig. 2 Sample frame# 150



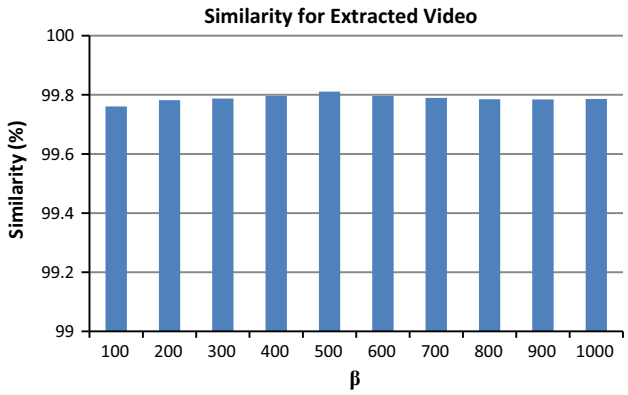


Fig. 4 Similarity of the extracted video at different values of β

7 Conclusion

In this paper, a novel high capacity hiding technique that allows embedding privacy information after the de-identification process takes place. The proposed hiding technique actually embeds the video captured by the surveillance camera into another processed video where the private information is removed.

The hiding process is carried out in the DWT domain of the cover. The hiding function is based on a parameter β, which divides the range of coefficients values into non-overlapping regions. The extraction process can be done in a blind fashion where the cover video is not needed to retrieve the hidden video.

Experimental results showed that the proposed method successfully hides an original video into its correspondence one with removed private information details that are as large as itself. Simple visual inspection of the results shows that the quality of the stego-frame maintains extremely high (over 45 dB) while maintaining an acceptable visual quality retrieval of the original frame with similarity up to 99.81 %.

References

1. Birch I, Raymond L, Christou A, Fernando MA, Harrison N, Paul F (2013) The identification of individuals by observational gait analysis using closed circuit television footage. Sci Justice: J Forensic Sci Soc 53(3):339–342
2. Howerton CL, Garner JP, Mench JA (2012) A system utilizing radio frequency identification (RFID) technology to monitor individual rodent behavior in complex social settings. J Neurosci Methods 209(1):74–78. doi:10.1016/j.jneumeth.2012.06.001
3. Nieto M, Johnston-Dodds K, Simmons CW (2002) Public and private applications of video surveillance and biometric technologies. California State Library, California Research Bureau, California
4. Payne BK, DeMichele M (2011) Sex offender policies: considering unanticipated consequences of GPS sex offender monitoring. Aggress Violent Behav 16(3):177–187. doi:10.1016/j.avb.2011.02.002
5. Rama K, Thilagam K, Priya SM, Jeevarathinam A, Lakshmi K (2011) Survey and analysis of 3D steganography. Int J Eng Sci Technol (IJEST) 3(1):638–643
6. Wickramasuriya J, Datt M, Mehrotra S, Venkatasubramanian N (2004) Privacy protecting data collection in media spaces. In: Proceedings of the 12th annual ACM international conference on Multimedia, New York, NY, USA
7. Zhang W, Cheung SS, Chen M (2005) Hiding privacy information in video surveillance system. In: IEEE International Conference on Image Processing (ICIP), 11–14 Sept (2005) vol 3, pp 868–871. doi:10.1109/ICIP.2005.1530530
8. Cheung SCS, Venkatesh MV, Paruchuri JK, Zhao J, Nguyen T (2009) Protecting and managing privacy information in video surveillance systems. In: Senior A (ed) Protecting privacy in video surveillance. Springer, London, pp 11–33. doi:10.1007/978-1-84882-301-3_2
9. Russell W (2013) Video frame definition—What is a video frame. About.com Guide. http://presentationsoft.about.com/od/uvw/g/95video-frame-definition.htm
10. Cheung SS, Paruchuri JK, Nguyen TP Managing privacy data in pervasive camera networks. In: Image processing, 2008. ICIP 2008. 15th IEEE international conference on, 12–15 Oct 2008, pp 1676–1679. doi:10.1109/ICIP.2008.4712095
11. Video Inpainting (2013) http://www.vis.uky.edu/∼jameszhao/video_inpainting.html