Reversible Privacy Protection in Videos Using Haar-like Feature Selection and Chaotic Tent Map Based Encryption

Aparna Asokan
M. Tech Scholar,
Department of Information Technology,
Government Engineering College, Barton Hill
aparna.askhn1013@gmail.com

Simi Krishna K R
Assistant Professor,
Department of Information Technology,
Government Engineering College, Barton Hill
simikrishnakr@gmail.com

Abstract— Nowadays, security becomes a major concern, so it is very important to hide data from unauthorized person who tries to access data in an unauthorized way. Data is generally in the form of text, image, video and audio. For the protection of data, steganography and cryptography were introduced. We can hide data in videos and also protect it from attacks. This work is based on the reversible privacy protection in videos using the concepts of cryptography and steganography. This is mainly applicable in video surveillance systems, military systems etc. The proposed method will be fully reversible and may provide security more than the existing methods.

Keywords: Video steganography, reversible privacy protection, encryption.

I. INTRODUCTION

With the rapid development of internet and other security systems such as surveillance cameras, there will be chances of misusing these facilities and also data are prone to attacks that are transmitted through internet. So we need different methods to protect data transmitted through the internet as well as protect videos captured by the surveillance camera. Cryptography and steganography are the two main streams of techniques for protecting data. These types of video protection are required in the case of video surveillance systems, military systems, medical field etc.

Steganography and cryptography are the means of securing the confidentiality and secrecy of information [1]. These techniques can be used to prevent security attacks on the information. In Steganography the secret text will be embedded in another format of data. In cryptography secret text is converted into cipher text, by knowing the secret key, then only data can be decrypted. Data will be in the form of text, audio, image and video. This paper focuses on privacy protection in videos.

In the case of military systems, a lot of confidential information will be transmitted to different locations mainly through the Internet. So there will be many chances for different types of attacks on information by unauthorized persons. Text and image Steganographic methods are now replaced with audio and video Steganographic methods because video contains continuous frames. Therefore redundancy is high and this can be utilized for embedding secret data. So instead of hiding data in text or image, data can be hidden in videos and then send the encrypted video to the receiver. At the receiver side the original information can be extracted because it will be in fully reversible mode.

Video Surveillance is important as far as security is concerned these days, which will protect person or organizational assets and also helps in other security purposes. Commercial spaces, schools and hospitals, warehouses and other challenging indoor and outdoor environments require high end cameras for proper security. The majority of organization and administrations are making use of such security cameras with the intention to protect their business as well as property from terrorists and illegal entry. Cameras send their data to servers over the internet, where digital intruders and hackers just wait for an opportunity to attack like man-in-the-middle attacks, hijacking communications between camera and video management systems. Once hackers get access to the system, they can inject an alternate video feed to conceal illicit activity or manipulate live camera footage to selectively remove certain details or persons from the scene. Also video contains several images with face of persons. So with this video footage anyone can take faces from the video and use it for illegal activities like morphing etc. So we have to provide security to each and every person who is captured by the camera.

This paper introduces a new method to provide fully reversible privacy protection in videos for the two different applications explained above. The proposed system is a

combination of techniques of cryptography and steganography which will provide high security without having any loss of video quality.

II. LITERATURE SURVEY

Due to the advancement of Internet and multimedia technologies, digital videos have become a popular choice for data hiding [2]. In video steganography, the secret data is hidden in the video. The video contains continuous frames, so redundancy is high and this can be utilized for embedding secret data. Recently, there are many useful applications of video steganography techniques such as video error checking, military services, bandwidth saving, video surveillance and medical video security [2]. Pixel-domain approaches, Transform domain approaches and Bit-stream domain approaches are the existing privacy region protection approaches.

Pixel-domain approaches modify the pixel value of the privacy region and then compress the video sequences. For example, pixelization, Gaussian blur [7], pseudo random permutation [7], warping [8], replacement by background [9] and chaos cryptography based data hiding [10]. Privacy region is modified before going through lossy compression, so that this approach will reduce the video compression efficiency, and it is impossible to recover the original compressed video sequences.

Transform domain approaches are more efficient by modifying the compressed information of the privacy region. Examples are the sign of DCT coefficients and intra-frame prediction modes. However, video compression introduces strong dependency between different parts of the video; drift error to the non-privacy region may introduce due to the modification of the privacy region. Thus the non-privacy region should be adjusted to be visually intact so that the entire frame look like completed without any damage. In [11], the non-privacy blocks which refer to the privacy blocks are modified to be intra-coded to avoid inter-frame error drift in MPEG-4 videos. The candidate prediction modes of non-privacy blocks are restricted to make sure that the privacy blocks are not used for the encoding of the non-privacy blocks in the prediction mode-restricted privacy protection methods [12][13]. In existing methods, re-encode the non-privacy region and irreversibly replace the original compressed data with newly compressed one.

Bit-stream domain approaches modify the compressed information such as the DCT coefficients, intra-frame prediction modes and motion vector differences, in the bit-stream domain based on traditional encryption such as chaos stream cipher [14]. Also the drift-error issue of non-privacy region still exists in bit-stream do-main approaches. The method in [14] exploited FMO (Flexible Macro-block Ordering)-based scheme to address intra prediction error. FMO-based scheme proposed in [15] encodes the privacy region and non-privacy region separately to prevent the intra-frame error drift for H.264/AVC surveillance video. The author of [16] de-fined full reversibility as the ability to recover the unaltered video and cited the FMO-based scheme [15] discussed above as fully reversible. However, the recovered video of FMO-based scheme is the FMO recompressed video sequence, is not the original compressed video directly recorded in the camera. Besides, FMO-based scheme ignored the inter-prediction error and thus the reconstructed image will be warped [14].

In 2015 [17], Xiaojing Ma et al proposes a fully reversible privacy region protection for cloud video surveillance. This paper proposes a novel fully reversible privacy protection method for H.264/AVC compressed video. All the operations are performed in the compressed domain. This will avoid lossy re-encoding, so the original H.264/AVC compressed video can be fully recovered. This scheme is the first fully reversible method for privacy region protection. The original H.264 compressed video is first entropy decoded to get the intra-frame pre-diction modes and the quantized DCT coefficients. Based on the intra-prediction modes, the "Propagation Vectors" to describe Multi-steps Drift Impact of blocks in the privacy region are calculated to describe their drift influence on the non-privacy region [17]. To avoid introducing drift distortion to the non-privacy region, the quantized DCT coefficients of each block in the privacy region are scrambled according to its Propagation Vector. Finally, all the quantized DCT coefficients are entropy encoded to generate the protected H.264 compressed video. For authorized users equipped with the scrambling key, the original compressed video can be recovered. Low computational cost with full reversibility is the main advantage of this method.

Natacha Ruchaud and Jean Luc Dugelay [18] proposed a method Efficient Privacy Protection in Video Surveillance by StegoScrambling. This paper presents a near lossless reversible system which allows a user to protect privacy in video surveillance by replacing sensitive RofIs(Region of Interest) by its edges using steganography. This system can be used on videos from smart-phone, camera or sensors of drone by combining scrambling, steganography and cryptography. Here the system removes two LSBs of each pixel intensity from original RofI. As compared to those of the original RofI, the pixel intensity of the recovered RofI decreases of three. This has no effect for human vision and a minimal impact for machine. Disadvantage of this method is that, the reverse process is not enough robust against compression.

In a word, for original video recorded at the camera, existing methods addressed the error drift problem in a lossy way, thus it is impossible to recover the original video. The full reversibility with security remains an issue to be solved.

III. PROPOSED SYSTEM

The paper proposes a new fully reversible privacy protection in videos. The basic idea is: detecting faces from each and every frame in the video and apply pixelization and Steganographic techniques to the detected face then it will undergo an effective encryption purpose to get an extra security.

Fig.1. shows the overall architecture of the proposed system. Firstly detect face from the video frames using Haar-like feature extraction method with a skin color map algorithm. This combination is done for the effective detection of the faces from the video frame. Thus these two algorithms were combined to get an effective face detection method which is the base of the proposed system. Detected face is then undergoing DWT pixelization; it is done up to three levels. After this MSB based steganographic method is implemented and apply chaotic tent map for encryption purpose. This will provide more security to the system. In this proposed system the user will have to access the system using the key first that means a better protection will be provided and no other person will be able to view the footage other than the authorized and registered people.

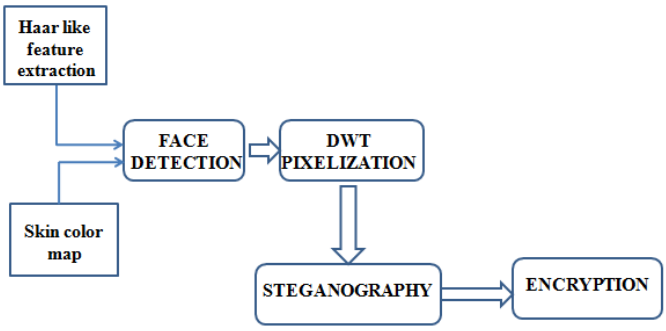

Fig.1.Architecture of proposed method

A. Face Detection

Face detection is the process of detecting faces from image or video. There will be several face detection algorithms which detects face using different features. In the proposed method, combination of two algorithms, Haar-like feature extraction algorithm [3] and Skin color detection algorithm [4] were used for effectively detecting each and every faces in the case of different movements of head positions.

Haar-like feature's principle is based on detection of features encoding of some information about the class to be detected [3]. In an image they are adjacent rectangles in particular positions.The Haar-like principle is simple; it lies on computing the difference between the sum of white pixels and the sum of black pixels. The main advantage of this method is the fast sum computation using the integral image. Rectangle features can be computed rapidly using an intermediate representation of the image called the integral image.Viola and Jones [3] used AdaBoost learning algorithm to select a specific Haar-like feature as a threshold. AdaBoost is used to create strong classifier from combining a collection of weak classification functions [3]. A chain of weak classifiers for efficient classification of image regions i.e. cascade classifiers are used to reject more false positives (non-face regions) of the sub-windows. Each node in the chain is a weak classifier and filter for one Haar feature. AdaBoost gives weights to the nodes, and the highest weighted node comes first.

Real-time Human Skin Color Detection Algorithm using Skin Color Map [4] is an algorithm for detecting face using skin color which gives promising results in complex background. Color space used here is YCbCr color space and skin color model used is explicitly defined regions. The technique used in the color space model is pixel based segmentation and color space is a set of colors are represented using mathematical expression.RGB color space, YCbCr color space and HIS color space are different types of color spaces. This algorithm focuses on detecting human skin color on real time basis using skin color map for the complex background YCbCr color space as this is more suitable for video processing applications and the skin color model used is explicitly defined region skin color model. Easy implementation and low storage space requirement with good processing speed are the major advantages of this method.

Combining these two methods will increase efficiency of detecting faces in video. This will be a major step in the proposed method.

B.DWT Pixelization

In DWT, digital image or frame is decomposed into four sub bands, with the lower sub band having relevant information and high sub band having finer details [2]. Sub bands are represented as LL, HL, LH and HH. Here the LL sub band is the low frequency portion and so it looks like the original image. The temporal resolution is the main advantage of this technique. It transforms a discrete time signal to discrete wavelet representation. In this paper, detected face is undergone three levels of DWT Pixelization. Then the face become not in an understandable format. This is what we want to do. Firstly divide the digital image (here it is a face) into four sub bands. Then again divide LL band to four sub bands and again the process repeats and place to the image portion. Then image will be in a blurred format.

C. Steganography

Steganography is the process of hiding data inside another medium. In Steganography the secret message is embedded in the cover message and transmitted in such a way that the existence of information is undetectable [1]. This method use MSB based bit differencing algorithm for hiding image. Fig.2 shows how to hide bits in pixel. Bit no 8 is used to store the secret bits based on the difference in 8^{th} and 1^{st} bits of the cover image. If the difference between 8^{th} and 1^{st} bits is not equal to the data bit, then replace the 8^{th} bit with the data bit. Likewise Bit no 7 is used to store the secret bits based on the difference in 7^{th} and 2^{nd} bits of the cover image. If the difference between 7^{th} and 2^{nd} bits is not equal to the data bit, then replace the 7^{th} bit with the data bit and so own. Generally attacker focus on the LSB bits for finding secret data, but the proposed method uses MSB bits so this makes more security for hidden data. This technique has greater PSNR and higher payload capacity, so that can hide more than one data in a single cover image.

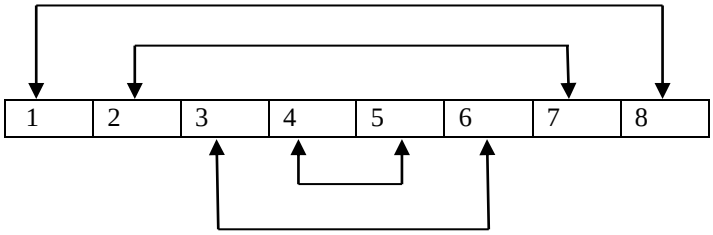

Fig.2.Arrangement of pixels for data hiding

D. Encryption

Encryption is the process of converting image or text into a cipher format using a key which is known by the sender. It will provide security for the message. Here the work uses an RT-enhanced CTM algorithm for encryption and decryption [5]. Algorithm proposes a novel image encryption algorithm by using the combination of the rectangular transform and the CTM principle. It encrypts the three channels of the plain image at the same time, and these channel encryptions associate with each other. RT-enhanced algorithm introduce the two dimensional rectangular transform (2D-RT) which is an extension of the Arnold map and it can directly be used to permutate non-square images [5]. Mathematically CTM equation can be represented as,

$$X_{i+1} = \begin{cases} \mu x_i, & \text{if } xi < 0.5 \\ \mu\,(1 - x_i), & \text{otherwise} \end{cases} \quad (1)$$

In encryption process, split image into three RGB planes and apply permutation [6]. In this permutation step RGB based transposition and shuffling takes place. After this shuffling convert each matrix into vectors and find chaotic sequences and key streams. Then find cipher format for each color plane and finally combine them to form a final cipher image. In the decryption process just reverses the overall process.

IV. IMPLEMENTATION AND RESULTS

The work is done in MATLAB R2016a in windows 8.1 with 64 bit processor. In the proposed method these steps are done step by step in each and every frame extracted from the video. So the system will protect video from unauthorized access with a reversible mechanism and also provide a fully reversible data hiding in a video. This method promises that the quality of the video is not reduced.

V. CONCLUSIONS

This paper proposes a privacy region protection scheme for video surveillance which allows full recovery of the original video and also fully reversible data hiding in videos. For efficiently detecting each and every faces from video frame, combination of haar-like combined cascade classifiers and skin color detection is used. For better security three levels DWT pixelization, MSB bit changing Steganographic algorithm and enhanced chaotic tent maps based encryption scheme is combined. Results of the proposed method shows that, the system is highly secure from attacks and having lower distortion with high quality of video. The main advantage of the proposed work is that the system is fully reversible and only authorized person can view the original data.

REFERENCES

[1] Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali and Muhammad Naeem “An Improved Image Steganography Technique based on MSB using Bit Differencing”. The sixth International Conference on Innovative Computing Technology(INTECH 2016).978-1-5090-2000-3/16/$31.00 ©2016 IEEE.

[2] Aparna Asokan, SimiKrishna K R “A survey paper on video steganography”. RACIS,January 10,2018.

[3] Souhail Guennouni, Ali Ahaitouf, Anass Mansouri“Face Detection: Comparing Haar-like combined with Cascade Classifiers and Edge Orientation Matching” 978-1-5090-6681-0/17/$31.00 ©2017 IEEE.

[4] Amit Kumar, Shivani Malhotra ,” Real-time Human Skin Color Detection Algorithm using Skin Color Map” 2015 2^{nd} International Conference on Computing for Sustainable Global

Development(INDIACom)978-9-3805-44168/15/$31.00©2015 IEEE.

[5] Xiaolin Wu, Bin Zhu, Yutong Hu, And Yamei Ran "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps" IEEE conference,March 13, 2017.

[6] Pratyaksha Ranawat, Sarika Khandelwal "Chaos Image Encryption Using Transposition and Pixel Shuffling" International Journal of Innovations in Engineering and Technology (IJIET), Volume 4 Issue 4 December 2014, ISSN: 2319 – 1058

[7] P. Carrillo, H. Kalva, and S. Magliveras, "Compression Independent Reversible Encryption for Privacy in Video Surveillance," EURASIP J. Inf. Secur., vol. 2009, pp. 5:1–5:13, Jan. 2009, doi: 10.1155/2009/429581.

[8] P. Korshunov and T. Ebrahimi, "Using warping for privacy protection in video surveillance," 18th International Conference on Digital Signal Pro-cessing (DSP'13), pp. 1–6, Jul. 2013, doi: 10.1109/ICDSP.2013.6622791.

[9] W. Zhang, S. S. Cheung, and M. Chen, "Hiding privacy information in video surveillance system," IEEE International Conference on Image Pro-cessing (ICIP'05), vol. 3, pp. II–868–71, Sep. 2005, doi: 10.1109/ICIP.2005.1530530.

[10] M. A. H. Sk. Md. Mizanur Rahman, "A real-time privacy-sensitive data hiding approach based on chaos cryptography," IEEE International Con-ference on Multimedia and Expo (ICME'10), pp. 72–77, Jul. 2010, doi: 10.1109/ICME.2010.5583558.

[11] F. Dufaux and T. Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems," IEEE Trans. Circuits and Systems for Video Tech-nology, vol. 18, no. 8, pp. 1168–1174, Aug. 2008, doi: 10.1109/TCSVT.2008.928225.

[12] Y. Wang, M. O'Neill, and F. Kurugollu, "Privacy region protection for H.264/AVC by encrypting the intra prediction modes without drift er-ror in I frames," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'13), pp. 2964–2968, May 2013, doi:10.1109/ICASSP.2013.6638201.

[13] L. Tong, F. Dai, Y. Zhang, and J. Li, "Restricted H.264/AVC video cod-ing for privacy region scrambling," 17th IEEE International Conference on Image Processing (ICIP'10), pp. 2089–2092, Sep. 2010, doi: 10.1109/ICIP.2010.5653444.

[14] F. Peng, X. Zhu, and M. Long, "An ROI Privacy Protection Scheme for H.264 Video Based on FMO and Chaos," IEEE Transactions on Infor-mation Forensics and Security, vol. 8, no. 10, pp. 1688–1699, Apr. 2013, doi: 10.1109/TIFS.2013.2259819.

[15] F. Dufaux and T. Ebrahimi, "H.264/AVC video scrambling for privacy protection," IEEE International Conference on Image Processing (ICIP'08), pp. 1688–1691, Oct. 2008, doi: 10.1109/ICIP.2008.4712098.

[16] F. Dufaux, "Video scrambling for privacy protection in video surveillance: recent results and validation framework," Proceedings of SPIE, vol. 8063, pp. 2–14, May 2011, doi: 10.1117/12.883948.

[17] Xiaojing Ma, Laurence T. Yang, Yang Xiang and Deqing Zou and and Hai Jin "A fully reversible privacy region protection for cloud video surveillance" IEEE Transactions on Cloud Computing, TCCSI-2015-03-0122 2168-7161 (c) 2015.

[18] Natacha Ruchaud and Jean Luc Dugelay "Efficient Privacy Protection in Video Surveillance by StegoScrambling"