

Motion Detection in Low Resolution Video Surveillance Data to Provide Personal Privacy

K.RangaNarayana¹, G.Venkateswara Rao²

Research Scholar Department of IT¹, Professor, Department of CSE²
GIT, GITAM University, Visakhapatnam, India.
Katakam916@gmail.com¹, dr.vrgurrala@gmail.com²

Abstract

Privacy protection from surreptitious video recordings is an important societal challenge. We desire a computer vision system (e.g., a robot) that can recognize human activities and assist our daily life, yet ensure that it is not recording video that may invade our privacy. This paper presents a fundamental approach to address such contradicting objectives: human activity recognition while only using extreme low-resolution anonymized videos. Although extensive research on action recognition has been carried out using standard video cameras, little work has explored recognition performance at extremely low temporal or spatial camera resolutions. Reliable action recognition in such a “degraded” environment would promote the development of privacy-preserving smart rooms that would facilitate intelligent interaction with its occupants while mitigating privacy concerns. Privacy protection from unwanted video recordings. We want a camera system to recognize important events and assist human daily life by understanding its videos, but we also want to ensure that it is not intruding the user’s or others’ privacy. This leads to two contradicting objectives. More specifically, we want to (1) prevent the camera system from obtaining detailed visual data that may contain private information, desirably at the hardware-level. Simultaneously, we want to (2) make the system capture as much detailed information as possible from its video, so that it understands surrounding objects and ongoing events for surveillance, life logging, and intelligent services. This paper presents an algorithm for motion detection in low resolution images.

Keywords: Personal Privacy, Surveillance Data, Motion Detection.

1. INTRODUCTION

Protecting home and organization is a prior goal to every individual with the advancement of technology, security cameras that record videos came into existence. These surveillance systems are able to provide us video footage whether live or recorded. These cameras increase security as they keep an eye on everything. These surveillance cameras are also cause a big societal challenge, personal privacy protection from redundant video recordings so, it needs a camera system to know significant procedures and help human daily life by understanding its videos, but it also ensure that it is not interfering the user or other personal privacy. This leads to contradicting objectives they are prevent the camera system from obtaining detailed visual data that contain private

information in hardware level and make the system capture as much detailed information as possible from its video, so that it understands surrounding objects and ongoing events for surveillance services. A fundamental solution towards the structure of a personal privacy preserving system is the use of anonymized videos. Motion Detection is designed by using image processing to protect personal privacy. In this firstly, video is collected from the surveillance cameras convert that high resolution video into high resolution multiple frames and then those high resolution frames are converted into low resolution frames from those low resolution frames, object detection and motion detection is done therefore, privacy is protected.

II. CONTRARY MOTION

Contrary Motion: Contrary Motion is a phrase for a set of methods of up scaling video or images. Contrary Motion (CM) works effectively when several low resolution images contain slightly different perspectives of the same object. Then total information about the object exceeds information from any single frame. It is based on the idea that a combination of low resolution (noisy) sequence of images of a scene can be used to generate a high resolution image or image sequence. Thus it attempts to reconstruct the original scene image with high resolution given a set of observed images at lower resolution.

CM is an inductive reasoning technique that involves inverting the resolution operator. CM is the concept of generating a set of low-resolution images from high-resolution images, by learning different image transforms optimized for the recognition task. Such transforms may include pixel translation, scale, revolution, and other affined transforms emulating possible camera motion.

Our CM targets the realistic scenario where the system is prohibited from obtaining high-resolution videos in the testing phase due to privacy protection but has access to a rich set of high-resolution videos publicly available. Instead of trying to enhance the resolution of the video, this approach is to make the system learn to benefit from high-resolution videos by imposing multiple different pixel transformations.

This enables to better estimate the decision boundary in the low-resolution space. From the contrary motion perspective, this is a different way of using the motion formulation, whose assumption is that multiple low resolution images may contain a comparable amount of information to a single high resolution image. It is called reverse contrary motion since it follows the

contrary motion formulation, while the input and the output is the reverse of the original.

III. TRANSFORMATION LEARNING

Here a new framework is used that takes advantage of LR training videos generated from HR videos assuming a ‘given’ set of transforms. Here, methods to ‘learn’ the optimal set of such motion transforms $F = \{S_k\}_{k=1}^n$ based on video data. Such F learned from video data is expected to perform superior to transforms randomly selected or uniformly selected. There are several methods available to select best frames in low-resolution frames. In those two methods were identified to select best low-resolution frames. They are:

- 1) Boundary Matching
- 2) Entropy

Boundary Matching:

Markov chain Monte Carlo (MCMC) based search approach is used to find the optimal set of transforms providing the ideal activity classification decision boundaries. The main idea is that, if this have an infinite number of transforms S_k generating LR training samples, then it would be able to learn the best low-resolution classifiers for the problem. Let us denote such ideal decision boundary as $q\theta^*$. By trying to minimize the distance between $q\theta^*$ and the decision boundary that can be learned with this transforms, and need to find a set of transformations F^* :

$$F^* = \operatorname{argmin}_F |q\theta - q\theta(F)|$$

$$\approx \operatorname{argmin}_F \sum_{(x \in A)} |q\theta^*(x) - q\theta(F)(x)| \quad (1)$$

s.t. $|F^*| = n$

Where $q\theta(F)(x)$ is a classification function (i.e., a decision boundary) learned from the training set $T(F)$ (i.e., LR videos generated using transforms in S). A is a validation set with activity videos, being used to measure the empirical similarity between two classification functions. In this implementation, furtherly approximate the above equation, since learning $q\theta^*(x)$ conceptually requires an infinite (or very large) number of transform filters S_k . That is, assume

$q\theta^*(x) \approx q\theta(FL)(x)$ where FL is a set with a large number of transforms. And also use FL as the ‘pool’ of transforms are considered: $F \subset FL$. This take advantage of a MCMC sampling method with Metropolis-Hastings algorithm, where each MCMC action is adding or removing a particular motion transform filter S_k to/from the current set F_t . The transition probability a is defined as

$$a = \pi(F_0) \cdot f(F_0, F_t) / \pi(F_t) \cdot f(F_t, F_0)$$

where the target distribution $\pi(F)$ is computed by

$$\pi(F) \propto \text{power}(e, -\sum_{(x \in A)} |q\theta^*(x) - q\theta(F)(x)|) \quad (2)$$

This is based on the argmin term in above equation. And the proposal density $f(F_0, F(t))$ is used with a Gaussian distribution $|F_0| \sim N(n, \sigma^2)$ where n is the number of inverse super-

resolution samples. The proposal F_0 is accepted with the transition probability a , and it becomes F_{t+1} once accepted.

Using the above MCMC formulation, this approach goes through multiple iterations from $F_0 = \{\}$ to S_m where m is the number of maximum iterations. Based on the sampled F_0, \dots, F_m , the one with the maximum $\pi(F)$ value is finally chosen as our transforms: $F^* = \operatorname{argmax}_{F_t} \pi(F_t)$ with the condition $|F| \leq n$.

Entropy:

Here, an alternative methodology to learn the optimal set of transforms filters F^* . Although the above methodology of directly comparing the classification functions provides us a good solution for the problem, a fair number of MCMC sampling iterations is needed for a reliable solution. It also requires a separate validation set A , which often means that the system is required to split the provided training set into the real training set and the validation set. This makes the transformation set learning itself to use less training data in practice. Here, there is another approach of using the entropy measure.

Entropy is an information-theoretic measure that represents the amount of information needed, and it is often used to measure uncertainty in machine learning (Settles 2010). This idea is to learn the set F^* by iteratively finding transform filters $S_1 \dots S_n$ that will provide us the maximum amount of information gain when applied to the training videos. At each iteration, it selects S_k that will generate new LR samples with the most uncertainty (i.e., maximum entropy) measured based on the current classifier trained with the current set of transforms: $q\theta(F_t)$. Adding such samples to the training set makes the new classifier to have the most information gain. That is, it iteratively update the set as

$$F_{t+1} = F_t \cup \{S_{t^*}\} \text{ where}$$

$$S_{t^*} = \operatorname{argmax}_k$$

$$\sum_{X_i} H(D_k F_k X_i) = \operatorname{argmax}_k - \sum_{X_i} \sum_j P_{\theta}(F_t)(y_j | D_k S_k X_i) \log P_{\theta}(F_t)(y_j | D_k S_k X_i).$$

(3)

Here, X_i is each video in the training set, and $P_{\theta}(F_t)$ is the probability computed from the classifier $q\theta(F_t)$. It essentially searches for the filter that will provide the largest amount of information gain when added to the current transformation set F_t .

More specifically, it sums the entropy H (i.e., uncertainty) of all low resolution training videos that can be generated with the filter S_k : $H(D_k S_k X_i)$. The approach iteratively adds one transform S_{t^*} at every iteration t , which is the greedy strategy based on the entropy measure, until it reaches the n th round: $F^* = F_n$. Notice that such entropy can be measured with any videos with/without ground truth labels. This makes the proposed approach suitable for the unsupervised learning scenarios as well.

IV. FUZZY C-MEANS (FCM)

The Fuzzy Logic Toolbox function *fcm* performs FCM clustering. It starts with an initial guess for the cluster centers, which are intended to mark the mean location of each cluster. The initial guess for these cluster centers is most likely incorrect. Next, *fcm* assigns every data point a membership grade for each cluster. By iteratively updating the cluster centers and the membership grades for each data point, *fcm* iteratively moves the cluster centers to the right location within a data set. This iteration is based on minimizing an objective function that represents the distance from any given data point to a cluster center weighted by that data point's membership grade. Fuzzy logic is a multi-valued logic where the truth values lies between zero and one. In any system there are two phases namely the training (learning) and testing phases. In the training or learning phase the data samples are given as input to the system for training the Fuzzy system, to classify the inputs according to the characteristics of the problem. In the testing phase the data instances are given as input to check whether the system classifies correctly. The training phase consumes a large amount of time. The fuzzy system is improved through the adaptive skipping method.

The FCM algorithm for segmentation of hyperspectral image is described below:

1. Take randomly K initial clusters from the $m \times n$ image pixels.
2. Initialize membership matrix u_{ij} with value in range 0 to 1 and value of $m=2$.

Assign each pixel to the cluster $C_j \{j=1,2,\dots,K\}$ if it satisfies the following condition [$D(\cdot, \cdot)$ is the Euclidean distance measure between two values].

$$u_{ij}^m D(I_i, C_j) < u_{iq}^m D(I_i, C_q), q = 1, 2, \dots, K$$

$$j \neq q \quad (4)$$

The new membership and cluster centroid values as calculated as

$$u_{ik} = \frac{1}{\sum_{j=1}^K \left(\frac{D(C_i, I_k)}{D(C_j, I_k)} \right)^{\frac{1}{m-1}}}, \text{ for } 1 \leq i \leq K$$

$$C_j^{\wedge} = \frac{\sum_{j=1}^n u_{ij}^m I_j}{\sum_{j=1}^n u_{ij}^m} \quad (5)$$

3. Continue 2-3 until each pixel is assigned to the maximum membership cluster.

V. MEAN SHIFT TRACKING ALGORITHM

Step 1: In the initial frame, the object area is first selected by the user and the object model is constructed, and the center position of the object is initialized.

Step 2: Selecting a candidate object area in the current frame, constructing a candidate object model with the object center of the previous frame as the center of the candidate object area;

Step 3: Estimate the similarity function, and calculate the weight coefficient, initialize the number of iterations, and then calculate the new candidate area center;

Step 4: And then re-estimate the similarity function by constructing a new candidate object model with a new candidate regional center;

Step 5: The similarity function is compared and then estimated again;

Step 6: Set the iteration threshold and the maximum number of iterations, and if the condition is satisfied, the iteration is terminated. Otherwise, return to Step 2 to continue iterating.

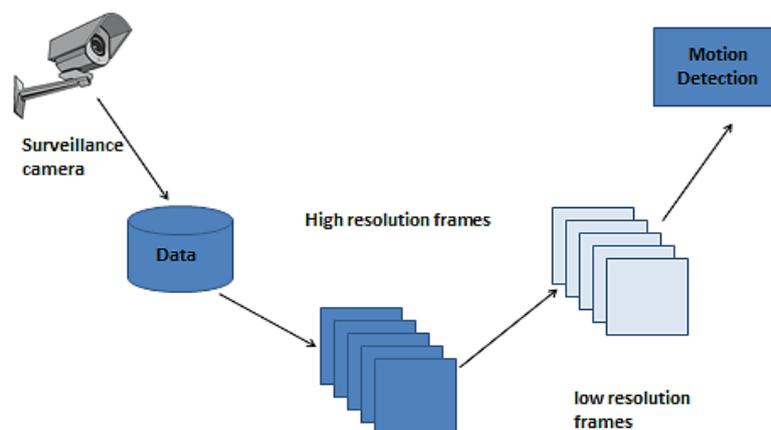


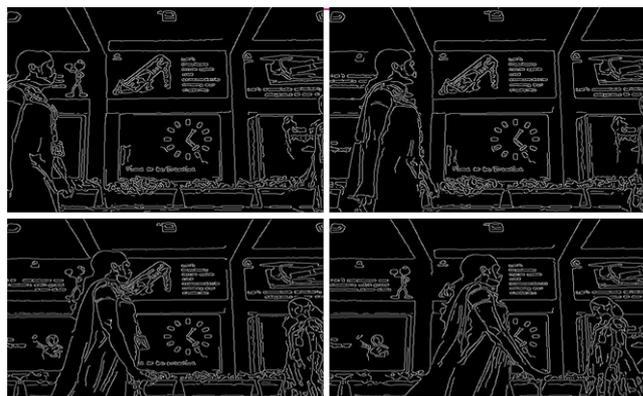
Figure 2. Frame Work

VI. EXPERIMENTAL RESULTS

1. Conversion from video into high-resolution frames



2. Conversion from high-resolution frames into low-resolution frames



3. Detecting object in low-resolution frames



4. Motion Detection in low-resolution frames



VII. CONCLUSIONS

In this work a hybrid of knowledge based image processing algorithms are used to read the video, to convert that video into high-resolution frames, to convert high-resolution frames to low-resolution frames, detecting the object in low-resolution video and detecting the motion in the low-resolution video. Here firstly videos are collected as input from the surveillance camera and then videos are converted into high-resolution frames by using No of Frames algorithm and those high-resolution frames are converted into low-resolution frames using Edge algorithm. From those low-resolution frames object detection by using Fuzzy c-Means algorithm and motion detection is done by using Motion detection algorithms such as MeanShift and Particle Filter. By this implementation invading privacy from surveillance camera is protected. In this work video is collected from surveillance camera and converted into low-resolution frames and then motion of an object is detected to protect personal privacy. This should identify an abnormal situation under recording and that incident should be intimated to the admin authorities.

REFERENCES

- [1] Zakaria Gheid et.al. "Efficient and Privacy-Aware Multi-party Classification Protocol for Human Activity Recognition", *Journal of Network and Computer Applications* 2017.
- [2] Wang, Z.; Chang, S.; Yang, Y.; Liu, D.; and Huang, T. S. 2016. Studying very low resolution recognition using deep networks. In CVPR.
- [3] Kim, J.; Lee, J. K.; and Lee, K. M. 2016. Deeply-recursive convolutional network for image super-resolution. In CVPR.
- [4] Tran, L.; Kong, D.; Jin, H.; and Liu, J. 2016. Privacy-cn: A framework to detect photo privacy with convolutional neural network using hierarchical

- features. In AAAI.
- [5] Butler, D. J.; Huang, J.; Roesner, F.; and Cakmak, M. 2015. The privacy-utility tradeoff for remotely teleoperated robots. In ACM/IEEE International Conference on Human-Robot Interaction, 27–34.
- [6] Dai, J.; Saghafi, B.; Wu, J.; Konrad, J.; and Ishwar, P. 2015. Towards privacy-preserving recognition of human activities. In ICIP.
- [7] Ryoo, M. S.; Rothrock, B.; and Matthies, L. 2015. Pooled motion features for first-person videos. In CVPR.
- [8] Shokri, R., and Shmatikov, V. 2015. Privacy-preserving deep learning. In ACM Conference on Computer and Communications Security (CCS).
- [9] Wu, C., and Guo, Y. Enhanced User Data Privacy with Pay-By-Data Model. *Proc. of Big Data Conference*, 2013.
- [10] Jensen, M. Challenges of Privacy Protection in Big Data Analytics. *Proc. Of Big Data Congress*, 2013.
- [11] Li, M., Zang, W., Bai, K., Yu, M. and Liu, P. MyCloud: Supporting User-Configured Privacy Protection in Cloud Computing. *Proc. of ACSAC*, 2013.
- [12] Agrawal, D., El Abbadi, A., and Wang, S. Secure and Privacy- Preserving Database Services in the Cloud. *Proc. of ICDE*, 2013.
- [13] Jang, M., Yoon, M., Chang, J.-W. A Privacy-Aware Query Authentication Index for Database Outsourcing. *Proc. of BigComp*, 2014
- [14] Ishibuchi, H., Yamane, M., and Nojima, Y. Learning from Multiple Data Sets with Different Missing Attributes and Privacy Policies: Parallel Distributed Fuzzy Genetics-based Machine Learning Approach. *Proc. of Big Data Conference*, 2013.
- [15] Rizvi, S., Ryoo, J., Liu, Y., Zazworsky, D., and Cappeta, A. A Centralized Trust Model Approach for Cloud Computing. *Proc. of WOCC*, 2014.
- [16] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal on Uncertainty, Fuzziness and Knowledge based Systems*, 10(5):571–588, October 2002.
- [17] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramanian. Diversity: privacy beyond k-anonymity. *ACM transactions on Knowledge Discovery from Data*, 1(3):146–, 2007
- [18] T.M. Truta and B. Vinay. Privacy Protection: p - Sensitive k - anonymity Property. In *Proceedings of the International Conference on Data Engineering Workshops*, pages 94–, 2006.
- [19] N. Li and T. Li. t-closeness: privacy beyond k - anonymity and l -diversity. In *Proceedings of 23rd International Conference on Data Engineering (ICDE07)*, pages 106–115, Istanbul, Turkey, 2007.
- [20] R.M. Tanley, O. Oliveira, and R. Zaane. Privacy Preserving Clustering By Data Transformation. *Journal of Information and Data Management*, 1(1):53–56, 2010.
- [21] T. Dalenius and P.R. Steven. Data swapping: A technique for disclosure control. In *proceedings of section on survey research methods*, pages 191–194, 1978.
- [22] M. Krishnamurthy and S. Rathindra. Data shuffling: A new masking approach for numerical Data. *Journal of Management Science*, 52(5):658–670, 2006
- [23] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, “Context Aware Computing for The Internet of Things: A Survey,” *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 414- 454, 2013.
- [24] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelffle, “Vision and Challenges for Realising the Internet of Things,” *Cluster of European Research Projects on the Internet of Things*, 2010.