International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Motion Detection to Preserve Personal Privacy from Surveillance Data using Contrary Motion

Pavan Kumar Vadrevu, Sri Krishna Adusumalli, Vamsi Krishna Mangalapalli

Abstract*: Internet of Things network today naturally is one of the huge quantities of devices from sensors linked through the communication framework to give value added service to the society and mankind. That allows equipment to be connected at anytime with anything rather using network and service. By 2020 there will be 50 to 100 billion devices connected to Internet and will generate heavy data that is to be analyzed for knowledge mining is a forecast. The data collected from individual devices of IoT is not going to give sufficient information to perform any type of analysis like disaster management, sentiment analysis, and smart cities and on surveillance. Privacy and Security related research increasing from last few years. IoT generated data is very huge, and the existing mechanisms like k- anonymity, l-diversity and differential privacy were not able to address these personal privacy issues because the Internet of Things Era is more vulnerable than the Internet Era [10][20]. To solve the personal privacy related problems researchers and IT professionals have to pay more attention to derive policies and to address the key issues of personal privacy preservation, so the utility and trade off will be increased to the Internet of Things applications. Personal Privacy Preserving Data Publication (PPPDP) is the area where the problems are identified and fixed in this IoT Era to ensure better personal privacy.

Keywords: Personal Privacy, Surveillance Data, Motion Detection.

I. INTRODUCTION

Today the source of business is free online services like email, social networking sites and feeds of news and many mobile applications which can be analyzed and the data can be improved to get more customer satisfaction [1]. This can be done by the organizations that are going to get benefit out of the data or they can sell it to the third party to analyze. The data which is given to the third party for analysis should not contain any privacy breach. The privacy preserving data publication research is going from many years [2]. Addressing the internet related privacy preservation policies is not sufficient for the today's IoT era. The intensity of IoT technologies increasing every day very rapidly as compared with the internet era, the data generated from IoT technologies is also very huge and multi dimensional[10].

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
***** Correspondence Author
Pavan Kumar Vadrevu*, Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Paralakhemundi, Orissa.
Sri Krishna Adusumalli, Associate Professor, Department of Information Technology, Shri Vishnu Engineering College for Women, Bhimavaram , Andhra Pradesh
Vamsi Krishna Mangalapalli, Professor, Department of CSE, Chaitanya Institute of Science and Technology, Kakinada

Researchers and IT professionals focusing on providing novel algorithms and policies for privacy preservation for the data generated from these devices [1]. Even anonymization and differential privacy mechanisms need to be upgraded to address the personal privacy issues in this IoT Era[20]. Here the main focus is on preserving privacy for the personal identification through surveillance data. This paper is organized into few modules firstly the problem is formulated then the methodologies used to implement motion detection from the high resolution vide frames by means of different image processing techniques explained then the results and conclusions discussed.

II. PROBLEM FORMULATION

Protecting home and organization is a prior goal to every individual with the advancement of technology, surveillance cameras that record videos came into existence for providing security. 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 a societal challenge, protecting personal privacy from redundant recordings so, it needs surveillance system to know significant procedures and help human life understanding its recordings, but it also ensure that not interfering the user or other personal privacy [3]. It leads to contradict objectives they are avoiding surveillance system getting the entire visual information which contain personal information in hardware level to create the security system capture heavy comprehensive information from video from then it understand surrounding objects and events from surveillance. One solution towards the arrangement of privacy preservation system is the use the anonymization video recording. Motion Detection is designed by using image processing to protect personal privacy [3][20]. In this firstly, video is composed from the surveillance cameras that is in high resolution then convert video into high resolution frames and then those high resolution frames are then convert into low resolution frames from those low resolution frames, object and motion detection is done through which the personal privacy is preserved in a static way.

III. CONTRARY MOTION AND METHODOLOGY

Inverse Resolution is a method to convert low resolution frames of an image into high resolution frames and it is used to identify the objects and motion of the objects proposed by Michael S. Ryoo et all [3].Contrary Motion is a set of methods of scaling video or images from high resolution to low resolutions frames.Contrary Motion work effectively on several low resolution images holding different aspects of the same image frame. CM is a technique that involves inverting the resolution operator from high quality image frame to low quality image frame.

It is the idea of creating a set of low resolution images from high resolution images, by using dissimilar image transformation techniques for better recognition task of the object.

Total information about the object exceeds from a single frame it is based on combination

of high resolution sequence of image frames of scene that can be used to generate low resolution image frames. It attempts to construct the original scene image with low resolution given a set of images at high resolution [4]. Transformation includes size, pixel conversion, insurrection, and affined emulation possible by the surveillance camera motion.CM targets the sensible situation where the arrangement is illicit from getting the high resolution video in the testing stage appropriate to the guard of personal privacy, except it has admission to a set of high resolution videos. In its place to improve the resolution of the video to make the system learn to advantage of high resolution videos by magnificent dissimilar pixel transformation [20][5], Which enable good approximation of result boundary in low resolution frame. From the contrary motion viewpoint, this way of using motion formulation, the hypothesis is multiple low resolution images may have a similar quantity of information to high resolution image frame.

IV. TRANSFORMATION LEARNING

A new framework that uses low resolution training video generated from high resolution video pretentious a given transformation. Here the best set of motion transformation F = {Sk} n k=1 based on video. This F cultured video is predictable to execute greater to transformation arbitrarily or consistently chosen [4]. 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 Technique
2) Entropy

1) Boundary Matching Technique:

Markov chain Monte Carlo (MCMC) base approach is used to get the best set of transformation given that the perfect action classification result boundaries [6]. The core idea is that, if an n number of transformation Sk generate low resolution training sample, then it capable to learn the greatest low resolution classifier for the setback [6]. Denote perfect result boundary as $q\theta*$ reducing remoteness between $q\theta*$ and result boundary that can be cultured with this transformation, and need to found a set of transformations $F*$.

$$F* = \arg\_minF\ |q\theta - q\theta\ (F)|$$
$$\approx \arg\_minF\ \Sigma\ (x \in A)\ |q\theta*(x) - q\theta(F)(x)\ |$$
$$s.t.\ |F*| = n$$

Where $q\theta(F)(x)$ is classification function (decision boundary) learned from the training set T(F) (low resolution video generated using transformation S) [6]. It is a rationale with motion video, being use to quantify the experiential comparison among two classification functions. This execution is an rough to the given equation, so learning $q\theta*(x)$ theoretically require a very large number of transformation filter Sk. Assume $q\theta*(x) \approx q\theta(FL)(x)$, FL is a set with a large set of transform. And also use FL as the 'pool' of transforms is considered: $F \subset FL$. It take improvement of sampling method of Metropolis Hastings algorithm, wherever each exploit is adding or remove a particular motion transform filter Sk to or from the present set Ft [6]. The transition chance A is define as

$$A = \pi\ (F0)\ f\ (F0, Ft)\ /\ \pi\ (Ft)\ f(\ Ft\ ,\ F0\ )$$

End distribution π (F) is compute by

$$\pi\ (F) \propto\ power\ (e, -\Sigma\ (x \in A)|q\ \theta*\ (x) - q\theta\ (F)\ (x)|\ )$$

This is base on argmin phrase in above equation. And the pitch density f (F0,F(t)) is used with Gaussian distribution $|F0| \sim N(n, \sigma 2)$ where n is the number of resolution sample. The tender F0 is accepted with the transition likelihood A, and it becomes Ft+1 once established [6].

From the exceeding formulation, this draw through many iterations from F0 = {} to Sm where m is the number of maximum iterations [6]. Based on the sampled F0...Fm, the one with the highest $\pi(F)$ value is preferred as our transformation. $F* = \arg\_max\ Ft\ \pi\ (Ft)$ with the condition $|F| \leq n$.

2) Entropy:

An unusual style to learn the optimal set of transformation filter $F*$. The methodology of comparing the classification function gives an elevated quality solution for the setback, good number of iterations is required for a reliable outcome [7]. It also require a part justification set a, which resources system split the provided exercise set to the real exercise set and the validation set. It builds the transformation set learning itself to less practice of exercise data put into practice. Here, is one more advance of using the entropy calculate called information theoretic quantify represents amount of information preferred, and often used to quantify ambiguity in machine learning (Settles2010). This proposal is to study the set $F*$ by repeatedly identifying transformation filter $S1 \cdots n$ that will give the maximum quantity of information when applied to the training video [7]. Each iteration, it select Sk that will make new low resolution sample with the most ambiguity (utmost entropy) designed based on the classifier trained with the set of transformations: $q\theta(Ft)$, such samples to the preparation set make the new classifier to have the majority information. That is, it updates the set

$$Ft+1 = Ft \cup \{St*\}\ where$$
$$St* = \arg\_max\ k$$
$$X\ i\ H\ (dkFkXi) = \arg\_max\ k - X\ i\ X\ j\ P\theta\ (Ft)\ (yj|dkSkXi)$$
$$logP\theta\ (Ft)\ (yj|dkSkXi)$$

Here, Xi is video in the set, $P\theta$ (Ft) is the likelihood computed from classifier $q\theta$ (Ft). It essentially searches for filter that provide biggest amount of data gain if added to the present transformation Ft [7]. Clearly, sum entropy H of all low resolution preparation video that can generate the filter Sk = H (dkSkXi). This come close to add one transform $St*$ for every iteration t, that is the greedy stratagem based entropy gauge, in anticipation it reaches the nth in circles $F* = Fn$ such entropy is intended with every video with or without argument reality label. It build the projected move toward appropriate for the scenario of unsupervised learning [7].

3) Fuzzy C-Means:

FCM (Fuzzy C means clustering) was developed by J.C. Dunn in 1973, and improved by J.C. Bezdek in 1981[8]. Cluster of arithmetical data from the base of any classification system model. The basic point of cluster to discover normal consortium of data from huge data set for creating brief illustration of a system performance.

FCM is cluster procedure for which a dataset is group into n clusters

with each data tip in the dataset belong to every cluster to a definite extent [8]. For example, an optimistic data tip that deceit close to the middle of cluster it will contain far higher than the ground quantity of membership to that cluster and other data tip that deceit far from the middle of the cluster and will have a small degree membership to the cluster [8]. Fuzzy logic function perform clustering, it starts from initial guess for the cluster middle, which future mark to mean the location of the cluster. This guess for first cluster middle is the most likely to be wrong. The next assign every data tip membership grade for each cluster. As a result of iteratively updating these cluster center and membership grade for each data tip, it iteratively move from the cluster middle to right location inside data set [8]. It is based on minimizing the objective function that it represents remoteness from the given data tip to a cluster middle weighted by that data tip membership grade. Fuzzy logic is multi valued logic where the reality value deceit among 0 & 1. Any system there are 2 phases first the training and the other is testing [8]. In training or learning phase the data model is as input to the system for training the given system, to order the input according to uniqueness of the setback. In testing the data instance is as input to check whether system classifies properly or not [8]. The first phases called training consume huge quantity of time. Then the system enhanced from end to end from the adaptive miss out technique.

4) Mean Shift tracking algorithm:

This algorithm is used to identify and construct the candidate object models to estimate the gain and to iterate for required quantity of efficiency. The steps as follows.

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

Step 2: Identify candidate object area in the frame, by constructing a candidate object representation with object middle of the earlier frame as the middle of the object area.

Step 3: Estimate comparison function, and calculate the weight coefficient.

Step 4: Initialize the number of iterations then calculate the new area of middle.

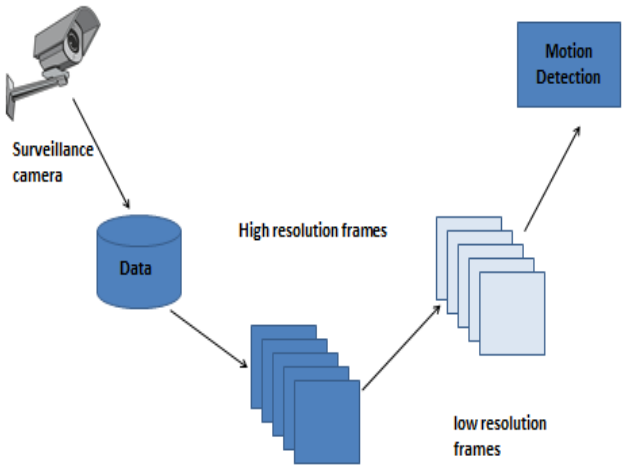
Step 5: Estimate the similarity function by constructing candidate object representation with new candidate regional middle.

Step 6: Then the similarity function can compare the estimated gain.

Step 7: Set iteration entry and the highest number of iterations, if the condition is good, then the iteration is finished else return to Step 2.

V. GENERAL DESCRIPTION:

Mean Shift tracking algorithm is similar to k-means algorithm which takes many number of clusters and assign coefficients arbitrarily to each data tip being in the cluster [9]. Iterate pending algorithm has sheltered the coefficients changes among two iterations is not more than ε the specified sensitivity threshold and calculate the middle for each cluster. For each data tip in the cluster, calculate its coefficient of being in the cluster [9]. The give frame work depicts the over view of motion detection process from capturing video to identifying the objects in low resolution video frames by which the privacy can be protected through static process. If this process is incorporated at hardware level the recording will happen only in low resolution whenever there is any abnormal situation that time only the admin authorities can take the high resolution videos to identify and analyze the problem.



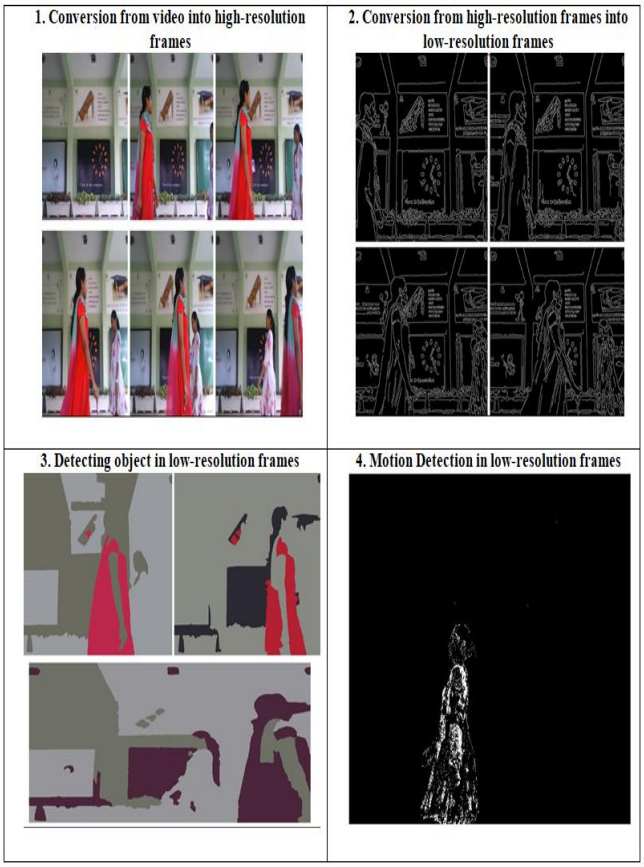
Frame Work

VI. CONCLUSIONS

In this work a hybrid image processing algorithms are used to read the video, to convert that video into high resolution frames, to convert high resolution frame to low resolution frame, detecting the object in low resolution frame and detecting the motion in the low resolution frame [8]. The collected inputs from the surveillance camera and then videos are converted into high resolution frames by using Noof Frames algorithm and those high resolution

frames are converted into low resolution frames using Edge algorithm [9]. 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 Mean Shift and Particle Filter [9]. By this implementation invading personal 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 [20]. This should identify an abnormal situation under recording and that incident should be intimated to the admin authorities for further processing of the data.

VII. SAMPLE RESULTS



ACKNOWLEDGEMENT:

I am very thankful to the IT Department and Management of Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhrapradesh, India for providing all the necessary resources to carry out this work.

REFERENCES.

1. Wang, Z.; Chang, S.; Yang, Y.; Liu, D.; and Huang, T. S. 2016.Studying very low resolution recognition using deep networks. In CVPR.
2. Sri Krishna, V. Valli Kumari, "An Efficient and Dynamic Concept Hierarchy Generation for Data Anonymization", Proceedings of the ninth International conference on Distributed Computing and Internet Technology, Springer-Lecture Notes in Computer Science, Volume 7753/2013, pp. 488-499, 2013.
3. Michael S. Ryoo, Brandon Rothrock, Charles Fleming,Hyun Jong Yang. Privacy- Preserving Human Activity Recognition from Extreme Low Resolution, Proceedings of the Thirty- First AAAI Conference on Artificial Intelligence (AAAI-17)
4. Tran, L.; Kong, D.; Jin, H.; and Liu, J. 2016. Privacy-cnh: A framework to detect photo
5. Privacy with convolutional neural network using hierarchical features. In *AAAI*.
6. Sanath Narayan, Mohan S. Kankanhalli, Kalpathi R. Ramakrishnan: Action and Interaction Recognition in First-person videos, 2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops
7. Zhang, D. and Liao, Q. Inverse Modeling Using Markov Chain Monte Carlo Aided by Adaptive Stochastic Collocation Method with Transformation
8. https://ui.adsabs.harvard.edu/abs/2016AGUFM.H24D..01Z
9. Chengming Qi, Maximum Entropy for Image Segmentation based on an Adaptive Particle Swarm Optimization, Appl. Math. Inf. Sci. 8, No. 6, 3129-3135 (2014).
10. R.Suganya, R.Shanthi, Fuzzy C- Means Algorithm- A Review, International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012 1 ISSN 2250- 3153.
11. Soumi Ghosh, Sanjay Kumar, Comparative Analysis of K-Means and Fuzzy C-Means Algorithms, May 2013, International Journal of Advanced Computer Science and Applications 4(4).
12. Sri Krishna, V. Valli Kumari, " An Efficient and Dynamic Concept Hierarchy Generation for Data Anonymization" Proceedings of the ninth International conference on Distributed Computing and Internet Technology, Springer-Lecture Notes in Computer Science, Volume 7753/2013, pp. 488-499,2013.
13. Privacy- Preserving Data Publishing By Bee- Chung Chen, Daniel Kifer, Kristen LeFevre and Ashwin Machanavajjhala Vol.2, Nos 1-2(2009) 1-67 DOI: 10.1561/1900000008.
14. InternetSecurity Threat Report, Synantec Corporation Annual Report, 2013, www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat- report-volume-20-2015-social_v2.pdf.
15. C.Dwork,"Differential privacy,"in ICALP,2006.Machanavajjhala A, Gehrke J, Kifer D, Venkitasubramaniam M (2006) L-diversity: Privacy beyond k-anonymity. In: Proceedings of the 22nd IEEE International Conference on Data Engineering (ICDE'06),IEEE Computer Society, Washington,Dc,USA.
16. R.C.W. Wong, J. Li, A.W.C. Fu, and K. Wang, "(α,k)-anonymity: an enhanced k- anonymity model for privacy preserving data publishing", Proceeding of the 12th ACM SIGKDD Conference on KDD, PA: ACM Press,Philadelphia, Aug. 2006, pp. 754-759.
17. Zude Li, Guoqiang Zhan, Xiaojun Ye, "Towards an Anti-inference (K, l)-anonymity Model with Value Association Rules", DEXA, Springer-Verlag Berlin Heidelberg, Krakow, Sep. 2006, pp. 883-893.
18. Personalized privacy preservation Xiaokui Xiao ,Yufei Tao Proceedings of the 2006 ACM SIGMOD international conference on Management of data Pages 229-240
19. Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions, Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V.Vasilakos IEEE Communication Magazine,January 2017.
20. The Quest for Privacy in the Internet of Things, Pawani Porambage and Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Athanasios V. Vasilakos, IEEE CLOUD COMPUTING PUBLISHED BY THE IEEE COMPUTERSOCIETY 2016.
21. A Survey on Personal Privacy Preserving Data Publication in IoT Pavan Kumar Vadrevu, Sri Krishna Adusumalli, Vamsi Krishna Mangalapalli, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-6C2, April 2019

AUTHORS PROFILE

Pavan Kumar Vadrevu, Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Paralakhemundi, Orissa (e-mail: vadrevu.pavan@gmail.com)

Sri Krishna Adusumalli, Associate Professor, Department of Information Technology, Shri Vishnu Engineering College for Women, Bhimavaram , Andhra Pradesh (email : srikrishna@svecw.edu.in)

Vamsi Krishna Mangalapalli, Professor, Department of CSE, Chaitanya Institute of Science and Technology, Kakinada. (email: vamsimangalam@gmail.com)