Visual Cryptography for preserving privacy in Surveillance System

Praveen Gujjar J

Associate Professor
CMS Business School, Jain (Deemed-to-be University)
Bengaluru, Karnataka, India. Email: dr.praveengujjar@cms.ac.in

Prasanna Kumar H R

Professor
PES Institute of Technology and Management
Shivamogga, Karnataka, India. Email: hrpbhat@gmail.com

Abstract: Advances in technologies has made intelligent monitoring system for video surveillance in preserving the privacy. This paper proposes the method which automatically interprets visual data. Using the visual cryptography technique visual data is encrypted and this will not reveal any information about the visual data. Only the authenticated person may able to decrypt the encrypted visual data. This intelligent surveillance system can also be called as next generation surveillance system. The proposed method makes use of face identification technique to capture the face from the surveillance system and the same region is encrypted with the help of visual cryptography technique. This paper also describes the importance of privacy preservation in the public surveillance system.

Keywords: Visual Cryptography, encryption, decryption, surveillance system, face identification

I. INTRODUCTION

Data is the need of the hour. Deep learning and machine learning help in analysing the data and automating many applications in the real world scenario. To implement any deep learning and machine learning concept researcher may required higher end infrastructure to carry out their work. Some of the examples of deep learning and machine learning applications are natural language recognition, sentiment analysis, e-commerce suggestions/recommendations and social network recommendations etc., [1]. Many deep learning and machine learning application it rely on heavy computations on massive datasets. GPU is an acronym for Graphical processing units which may helps in parallel task processing [2]. Most of the applications in deep learning and machine learning use NVIDIA GPUs [3] [4]. Google Colab will help in providing the necessary infrastructure to carry out the task for a free of cost by default Google colab provide 12 GB RAM and 32 GB of Disk space. If any researcher wants to use more Google cloud provide necessary infrastructure in a pay-by-hour manner to use the hardware with a fully configured GPU for deep learning applications [5] [6]. In this paper Deep learning and machine learning applications such as MobileNetV2 and XLM-Roberta models has been discussed. MobileNetV2 and xlm both are trained models which are also called as transfer learning. MobileNetV2 and xlm model has been implemented in Google Colab. MobileNetV2 is used for the image classification and image prediction. Xlm is used for natural language processing. Xlm is mainly used to classifying the text based on the certain categories. Amazon and Microsoft both will provide high performance computing hardware and the necessary infrastructure to carry out the deep learning and machine learning applications. Relatively Google colab is cost effective [7] [8]. Expósito et al. [9] shown that Amazon EC2 is having the performance bottlenecks in application scalability especially with high performance computing infrastructure. A convolution neural network is used for image classification and prediction [10]. Transfer learning is nothing but a reuse of the trained model for classification and prediction [11]. Sentiment analysis and opinion mining can be done using the textblob library using the tool Google colab [12] [13]. Visual cryptography [14] is a mathematical method developed to hide visible information where decryption is straightforward.

II. RELATED WORKS

Shares can be obtained as mentioned by the Naor and Shamir [13] Visual Cryptography is the method used for secret-sharing that encrypts a secret image into several shares; the hidden secret image can be retrieved visually by overlaying the encrypted shares and then the secret image becomes clearly visible. In the basic settings of visual cryptography the information is shared among many fragments, as in threshold cryptography [14], and each of those fragments do not sound when they do not merged again with proper technique. Whenever the fragments are transferred on separate channels or stored on different media, the original visible information could be kept secure if at least one of the channels are secure or alternatively one of the media is kept secure. Note that, this assumption holds when the channels, media and shares are independent from each other.

III. PROPOSED METHOD

The proposed methodology includes the following steps: Image acquisition, image pre-processing, information hiding, share creation, transferring & storing created shares for independent entities. The steps of the proposed method can be visualized as in Fig 1. In this model Image/video is acquired from the surveillance system. By applying the face detection algorithm find the face. Further generate and apply the share to the identified portion of the image which is obtained from the surveillance system. In the case of suspect obtained the original image/video by stacking the shares in the proper order.

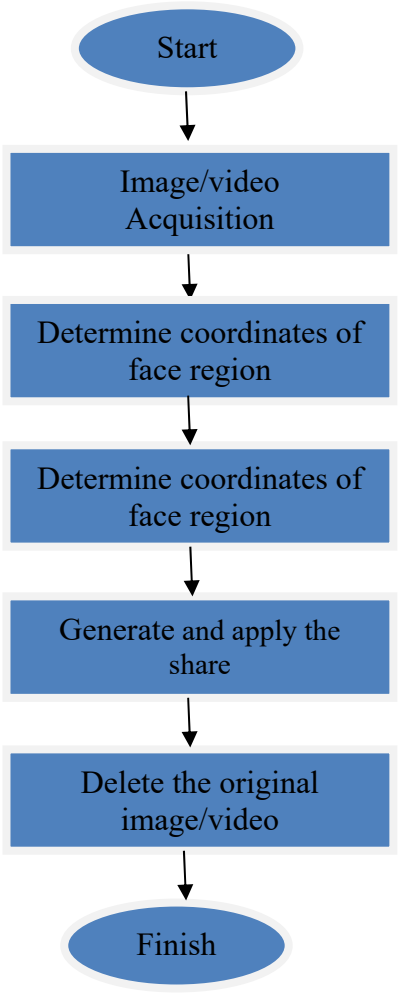

Fig 1: Steps of proposed method

V CONCLUSION

In this paper, privacy enhancing mechanism was introduced. The proposed mechanism is cost effective and it can be used in the surveillance system and safety cameras. The proposed technique is make use of visual cryptography technique, which takes image and convert it into shares which is in unidentified manner and this shares stores in independent entities. Visual cryptographic technique based infrastructure is very helpful in providing the privacy in critical locations. In case of security and safety is vital, in those location this technique is more beneficial.

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, p. 436, 2015.
[2] A. Brodtkorb, C. Dyken, T. Hagen, J. Hjelmervik, and O. Storaasli, “State-of-the-art in heterogeneous computing,” Scientific Programming, vol. 18, no. 1, pp. 1–33, 2010.
[3] NVIDIA Corporation, “Tesla V100 performance guide: deep learning and HPC applications,” NVIDIA Corporation Whitepaper, 2016.
[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, et al., “Above the clouds: A Berkeley view of cloud computing,” Technical Report UCB/EECS-2009- 28, EECS Department, University of California, Berkeley, Tech. Rep., 2009.
[5] NVIDIA Corporation, “Introduction to NVIDIA GPU cloud,” NVIDIA Corporation Application Note, 2018.

[6] Google, "Colaboratory: frequently asked questions ," 2018, [Access: 6-21-2018]. [Online]. Available: https://research.google.com/colaboratory/faq.html
[7] G. Juve, E. Deelman, K. Vahi, G. Mehta, B. Berriman, B. P. Berman, and P. Maechling, "Scientific workflow applications on amazon ec2," in 2009 5th IEEE International Conference on E-Science Workshops. IEEE, 2009, pp. 59–66.
[8] K. R. Jackson, L. Ramakrishnan, K. Muriki, S. Canon, S. Cholia, J. Shalf, H. J. Wasserman, and N. J. Wright, "Performance analysis of high-performance computing applications on the amazon web services cloud," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2010, pp. 159–168.
[9] R. R. Expósito, G. L. Taboada, S. Ramos, J. Touriño, and R. Doallo, "Performance analysis of hpc applications in the cloud," Future Generation Computer Systems, vol. 29, no. 1, pp. 218–229, 2013.
[10] Sharma, N., Jain, V., & Mishra, A. (2018). "An Analysis of Convolutional Neural Networks for Image Classification", Procedia Computer Science, Vol.132, pp.377-384.
[11] Shaha, M., &Pawar, M. (2018). "Transfer Learning for Image Classification". In 2018 Second International Conference on Electronics, Communication, and Aerospace Technology (ICECA), IEEE, pp. 656-660.
[12] Praveen Gujjar and Prasanna Kumar H R (2020), "Sentimental analysis for running text in Email Conversation", International Journal of Computer Science and Engineering (IJCSE), Volume 9, Issue 4 pp 67-68,
[13] T Manjunatha and Praveen Gujjar (2018), "Performance Analysis of Indian Information Technology Companies using DuPont Model", IUP Journal of Management Research, Volume 17, Issue 4, pp 7-14.
[14] M. Naor and A. Shamir, Visual cryptography, pp. 1–12. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994.