www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

A Study of Copy Image Detection Using the Model of Raspberry Pi Machine Learning Process

Arunkumar Lourembam[1]; K.M.V. Madan Kumar[2]; Thounaojam Rupachandra Singh[3]
[1]Department of Computer Science, CMJ University, Shillong, India.
[1]aksingh31011@gmail.com
[2]Department of Computer Science, CMJ University, Shillong, India.
[2]madankukunuri@gmail.com
[3]Department of Computer Science, Manipur University, India.
[3]rupachandrath@manipuruniv.ac.in

Abstract
Many physical gadgets are associated to the internet shaping. They are known as the Internet of Things. These gadgets are developing a calculation of useless and useful data. The preparing and transmission of this data was an investigating task. Various internets of things are talked in the current research work. A sector of security was the unmistakable application in the internet of things system. It was efficient to reduce the crime and provides security to individuals form business, home, military and so on. This research paper consumes the Raspberry Pi Internet of things basic characteristics the representation for the machine learning process. It ends the request of customer employments for instance, to transmit information safely by the process of internet of things engineering. It analyzes for normal internet of things, very low manageable and finance process depend upon the structure of security learning process that aids detectable 97% proof, nearby identification and outsiders verification. These arrangements develops by using the USB web camera as an image capturing unit, door hit through electrical way that provides APIs, to accumulate preparations that was perfect along with the structure of internet of things for improving the video graph arrangement for Raspberry Pi app.

Key-words: Forgery, Raspberry Pi Model, Detection, Support Vector Machine, Finance Process, Deep Learning Features, Convolutional Neural Network.

1. Introduction

A digital images has exponentially developed with the arrival of latest tablets, cameras and smart phones.[1] Social Media like Twitter, WhatsApp, Fb and Instagram are contributed to its

deployment. These pictures are significantly evolved and its tools are manipulated digitally.[2] Software like smartphone, Photoshop and gimp applications like pile & snapseed develop it very important for every users to manipulate images easily. Many procedures are examined to monitor the manipulations of digital picture depend upon the artifacts from.jpeg compression, array of filter, resampling, camera forensics, lightening and so on.[3-5] A single picture may prompts a difficult notion in an easy way. i.e. a picture was worth a 1000 words.

An interfering image can change a fake impression that can guide to the divesting problems. An application programmable journalist Schreiber had taken the phone in the fig 1on thee G-20 summit in Germany, 2018. Then the photo was uploaded and changed to Fb by a Russian author.[6] The image was shared already for 1000 times in various social sectors by the time the author dated the post from Fb. A new website caused chaos and produced debate all over the world. A forged digital image may convey the wrong message to the political experts that can make them to take wrong decision in their political career or may be the initiate to war.[7]

Figure 1 - Image Splicing; (a) Original One and (b) False One.

(a) (b)

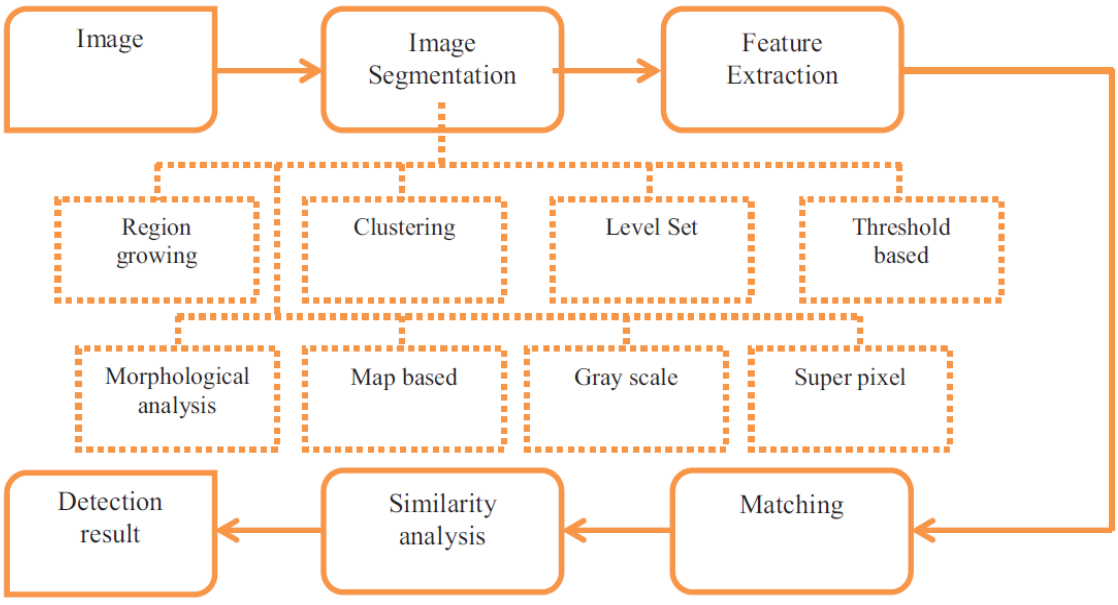
A protocol of unequal gathering was divided into 3 types. They are present, possibility and deterministic type. An algorithm of possibilities are very famous due to its fast growing, simplicity and energy efficient.[8] It is classified into 2 kinds, they are hybrid and random. A hybrid method use unsystematic procedure along with few parameters such as distance to bs value or residual power. These are iterative depend upon the competition that rises the difficulty in terms of time and message. [9, 10] An approach of random was simple and attained optimal but fail to enhance energy. CPCP sensors left ungrouping at the phase end to form the groups. These sensors joints do not involve into any group head and send its information to the neighbour joint which is very near to them. Because of this, the

inner group communication over group heads rises. The main goal of this script was to do the method for monitoring the forgery image by CNN method.

2. Literature Survey

The discovery of the copy region and image was mandatory to monitor the deployed image composite along with symmetrical consistency of copy and image. Many image techniques are appeared to the picture for the isolation of mesh information and image. [11] A processing image was an important technique for analysing the image by mathematical functions through any signal processing. An output processing was set of parameters &c features or image regarding the picture that holds the mesh information. [12] Segmentation was a main technique that used in the processing of image to found the image objects. An analysis of image can be finished upon the discovery of object. [13] An unstructured copy region or image from the picture may be separated effortlessly for the validation by holding the technique of segmentation. [14] A segmentation f image technique was recognized as a task in many image field. The segmentation was appeared to take away the inconsistent area from the picture depend on the characterisitcs are analysed, extracted and matched to authenticate the original magee. Fig.3shows the segmentation depend upon the image copy detection.

Fig. 2 - Segmentation of Copy Image Process

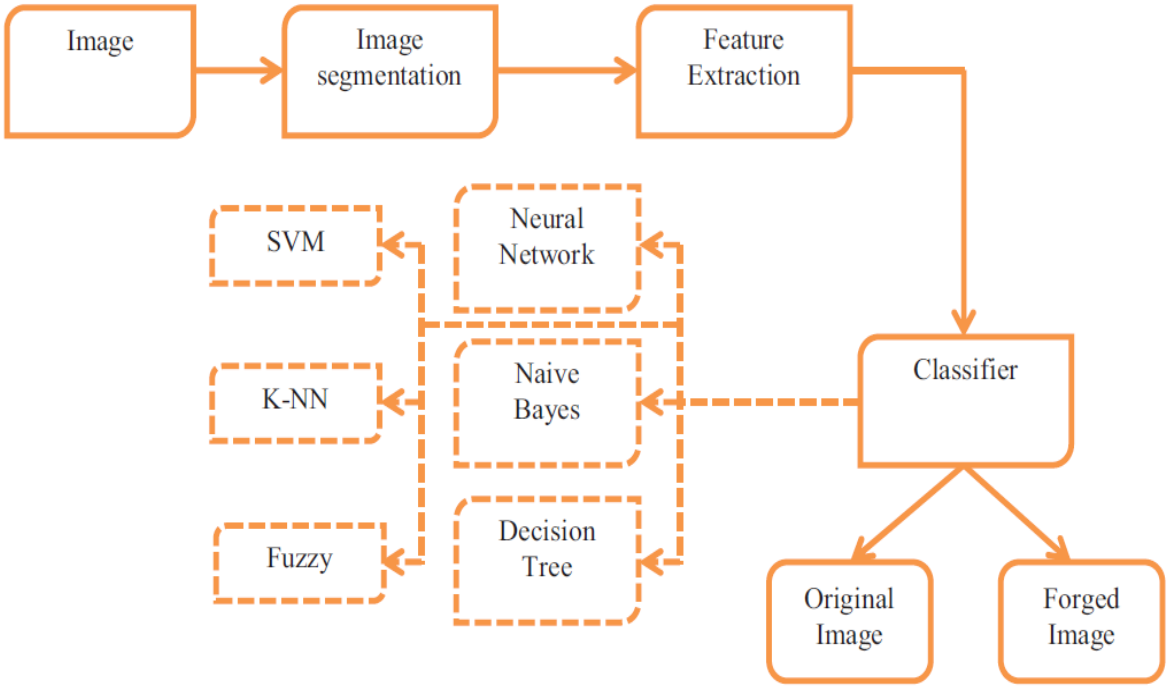


An artificial intelligence was a state of art issue was used in any sector linked with the vision of computer.[15] MLT was a kind of artificial intelligence along with the capability to study with no

explicit program and divide or judgement depend upon the studied information. A well-defined information analysis was given feasibly through the technique of machine learning. [16] A technique of machine learning was used for authenticating the image validation in the picture forgery. The image copy depends upon the forgery detection. The machine learning process was indispensible. [17]

Learning depends monitoring approaches increases the monitoring process of the adapted scheme. Some of the important benefit of the matching learning techniques are the ability to analyse the real image, segmentation characteristics matching study result developing grouping level depend upon the study of morphology, map depend upon the gray scale issue, capacity to divide the data base with unfinished data.[18] These benefits are mandatory in the picture forgery. This technique was appeared as one of the important stays in the picture forgery. Fig 3 clearly shows the machine learning technique to identify the forgery image. The characteristics concerned along with the light strength and image texture. The characteristics goals are fed to the technique of machine learning after the extraction process.

Fig 3 - Machine Learning Depend Copy Image Detection



An examined approach was executed to recognize and monitor the digital image under examination was forged by the convolutional neural network depend pre-defined Raspberry Pi design on the available MICC-F230 data set pictures. It was analysed the characteristics of deep learning

process depend upon the Raspberry Pi design. This design was satisfactory. Many input are corresponded to the images to process the pre-defined raspberry pi depend convolutional pooling and operations with the activation process to take away the characteristics of deep learning process. [19] A SVM division was trained along with the characteristics of deep leaning from the pre-defined raspberry design and correlated the output with 6 different approaches for the MICC F230 data set. This data set was used to identify the forgery image. The dataset pictures are resized and pre-analysed to 278x278 as per the raspberry design. To decreases the impact of samples for the deep characteristics, an average division was computed with 5 repetitions over the picture in the data set. This segment gives the execution of the examined approach by the hardware as Intel(R) Core™ i8-5890U Central Processing Unit with 3.20 Giga Hertz, 18Giga Byte Random Access Memory and software as Ubuntu 17.02 with Matlab release R2017a and correlated the examined approached with the approach of state of art.[20]

3. Proposed Model

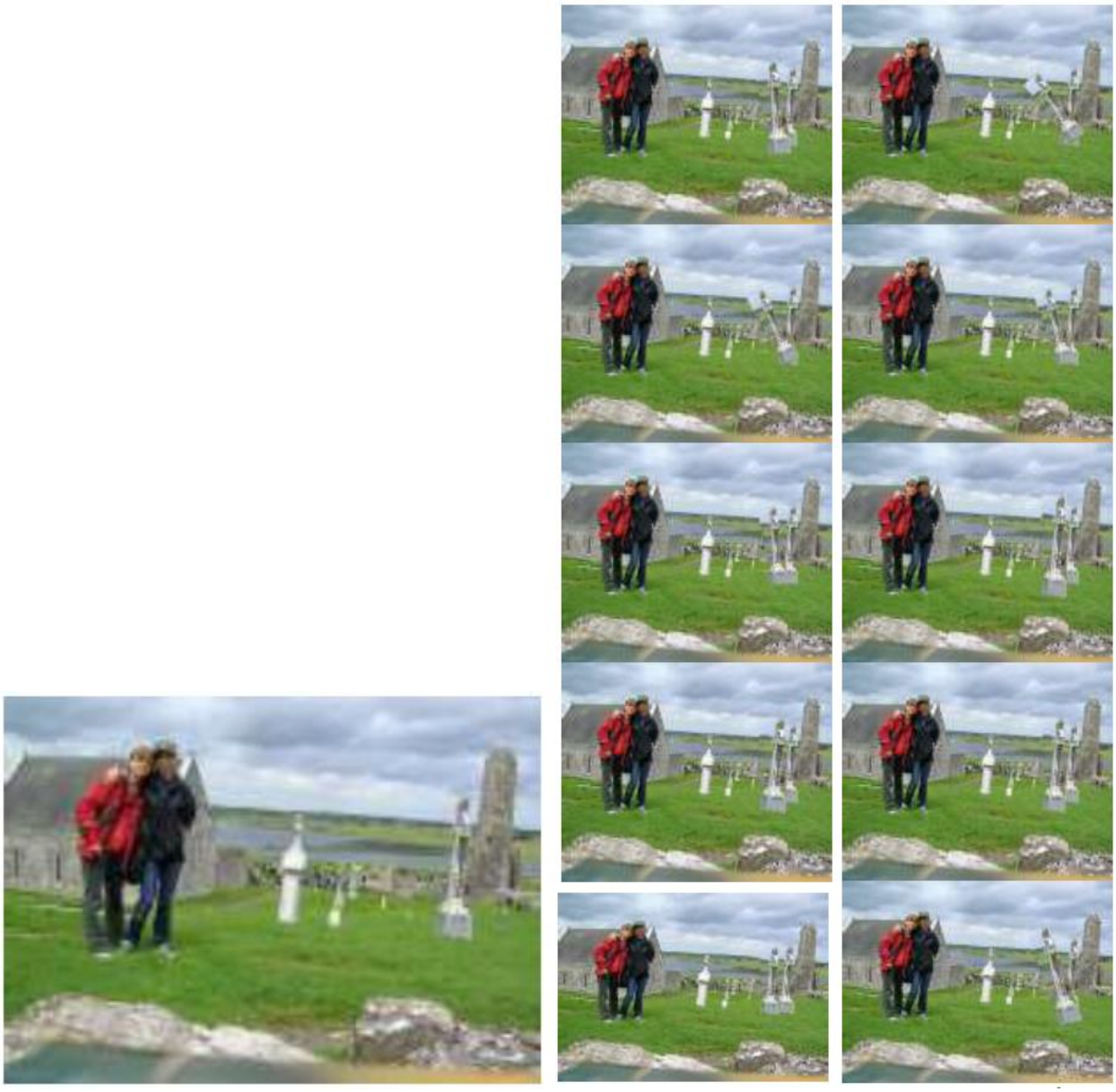
3.1. Dataset

MIcCC F230 dataset was used for the investigational output. This data set contains 120 forged and 120 non-forged along with three channels that is the size of colour image was 734x490 to 850x650 pixels along with ten various combinations of transformation and geometrical attacks to the correct picture. This was clearly shown in the figure 4.

3.2. Classifier

Support Vector Machine was considered as a classifier. It was efficient and popular for the classification of binary system. The function of the examined approach was investigated at the level of image using the metrics process such as TPR, FPR, accuracy, F-measure and precision with the implementation time.

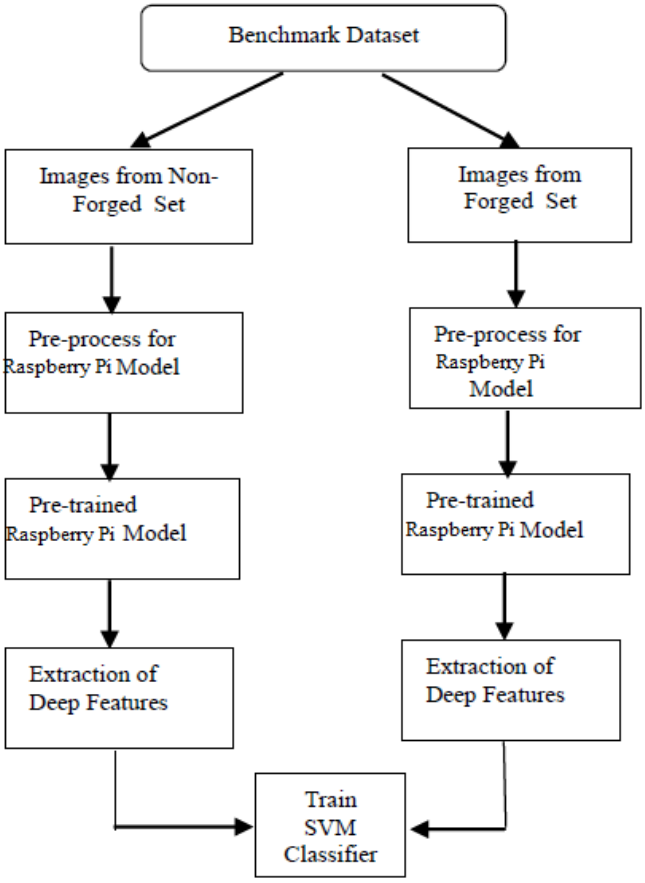
Fig. 4 a) Original Image b) Ten Various \ Transformations Attacks and Geometrical



3.3. Proposed Approach

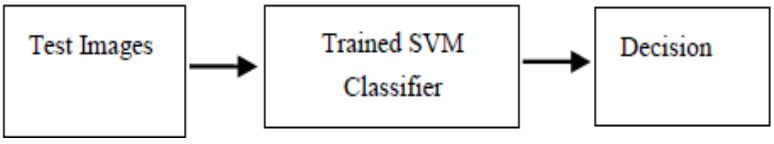
An examined approach was carried out in two levels, one appears the support vector machine classifier by a pre-defined Raspberry Pi design depend upon the characteristics of deep learning. Figure 5 shows the examined approach.

Figure 5 - Diagram to Analyse the Support Vector Machine Classifier by the Design of Raspberry Pi



The second one was the investigating process. Figure 6 shows the test images which are provided as input to pick the forged image.

Figure 6 - To Prove the Image was Forged or Non-forged



The method may be analysed as

1. Images are chosen from the non-forged and forged image in the training level.
2. A pre-processed image are analyzed the input segment of the 1st layer of raspberry pi design.
3. Pre-defined Convolutional neural network depend the design of raspberry pi to extract the characteristics of deep learning method.
4. A vector feature including of 4083 deep characteristics to train the support vector machine classifier.

Received: 11.06.2021 – Accepted: 14.07.2021

5. Examined images are selected from the data set and nourish into the well-defined support vector machine classifier to judge the forge or non-forged image. An output was measured for the provided data set.

4. Result and Discussion

There is different method to identify the correct investigational outputs. The metric process of the convolutional neural network depend pre-defined raspberry pi design using support vector machine classifier was examined by the matrix which was shown in the tab 1 and 2.

FP - Non-Forged Image detected as forged.

Table 1- Confusion Matrix

Actual	Predicted Forged	Predicted Non-Forged
Forged	(True Positive) TP	(False Negative) FN
Non-Forged	(False Positive) FP	(True Negative) TN

FN - Forged Image detected as non-forged

TN - Non-Forged Image detected as non-forged

TP - Forged Image detected as forged

$$\text{False Positive Rate (FPR)} = FP/(FP+TN) \quad (1)$$

$$\text{True Positive Rate (TPR) or Recall} = TP/(TP+FN) \quad (2)$$

$$\text{Precision} = TP/(TP+FP) \quad (3)$$

$$\text{F-Measure} = 2 * ((\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})) \quad (4)$$

$$\text{Accuracy} = (TP+TN)/(TP+TN+FP+FN) \quad (5)$$

Table 2 - Confusion Matrix for the Test Data Set

Test Dataset	Forged Predicted	Non-Forged Predicted	Accuracy
Forged	50%	0%	93.94%
Non-Forged	6.06%	43.94%	

It was analyzed that MICC f230 data set the perfection was 94.89% with TPR or recall rate was 100%, F-measure was 95.87%, precision was 90.01% and the minimum implementation time for the method was 5.87 seconds. Table 3 shows the TPR, FPR and time on MICC-F230 data set.

Table 3 - FPR, TPR and Time (Seconds) for Different Methods on MICC-F220 Dataset

Approach	FPR, %	TPR, %	Time, s
(Amerini et al., 2011)	8	100	4.94
(Mishra et al., 2013)	3.64	73.64	2.85
(Fridrich et al., 2003)	84	89	294.69
(Popescu and Farid, 2004)	86	87	70.97
(Diaa M. Uliyan et al., 2016)	8	92	NA
(D.M. Uliyan et al., 2016)	2.86	96.5	NA
Proposed Approach	12.12	100	4.86

The process of forgery monitoring was investigated at the image stage. The mistake was calculated by FPR. The corresponding graphs reveal the forgery image detection by support vector machine classifier. It was very clear that the support vector machine classifier generated with a perfection of 99.6% which was shown in the figure 7. The low performance of the support vector machine was shown in the figure 8.

Figure 7 - Entire Accuracy of Support Vector Machine Classifier

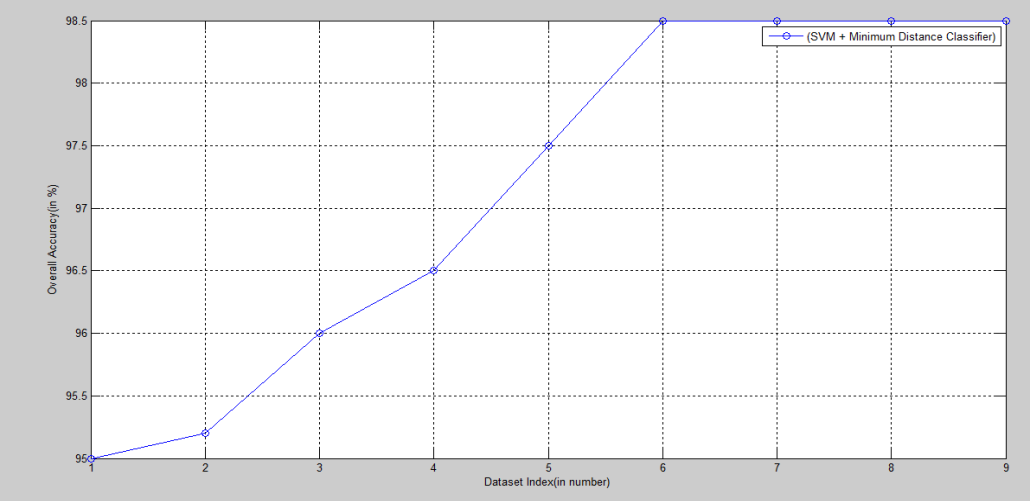


Figure 8 - Support Vector Machine Classifier Low Performance

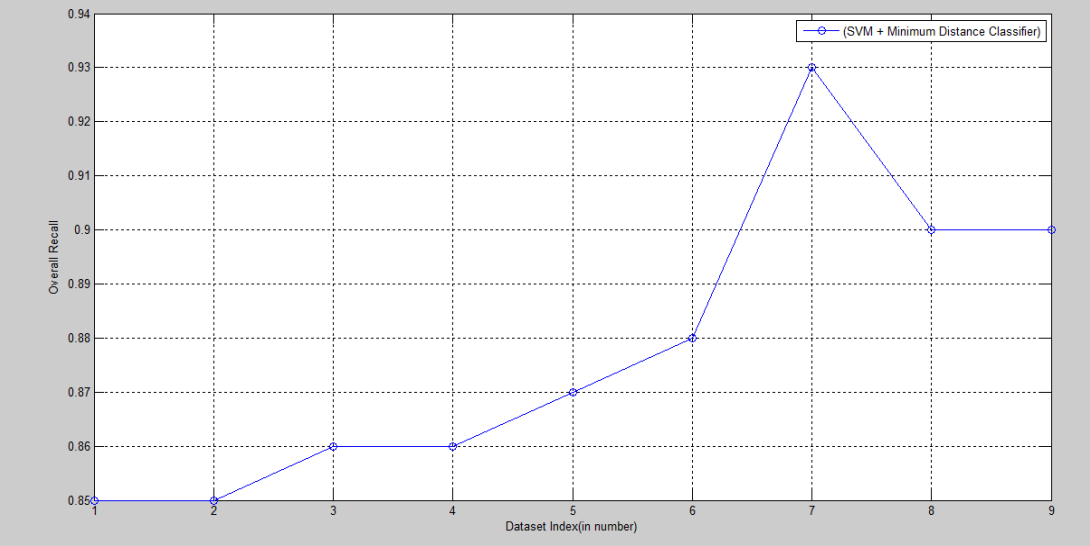


Figure 9 - Support Vector Machine Increased the Performance

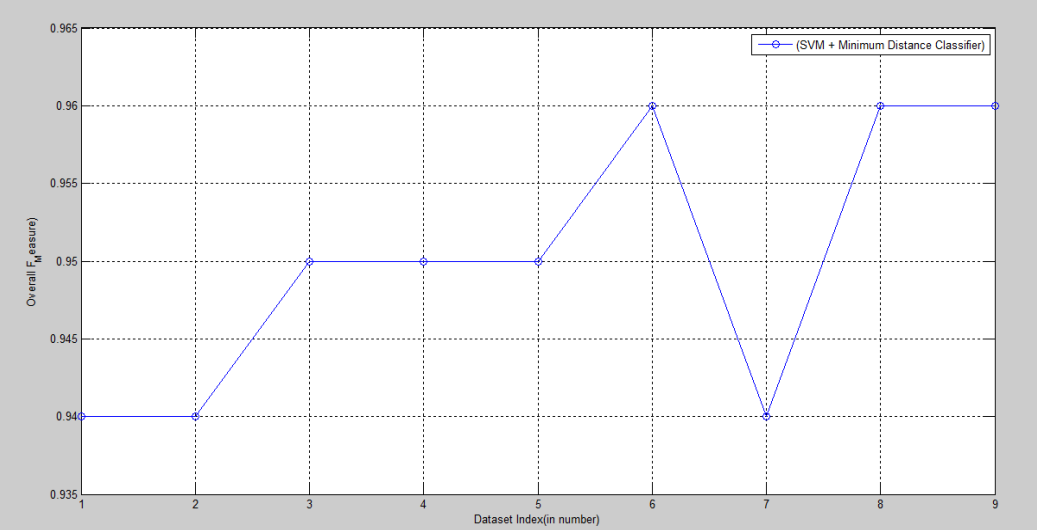
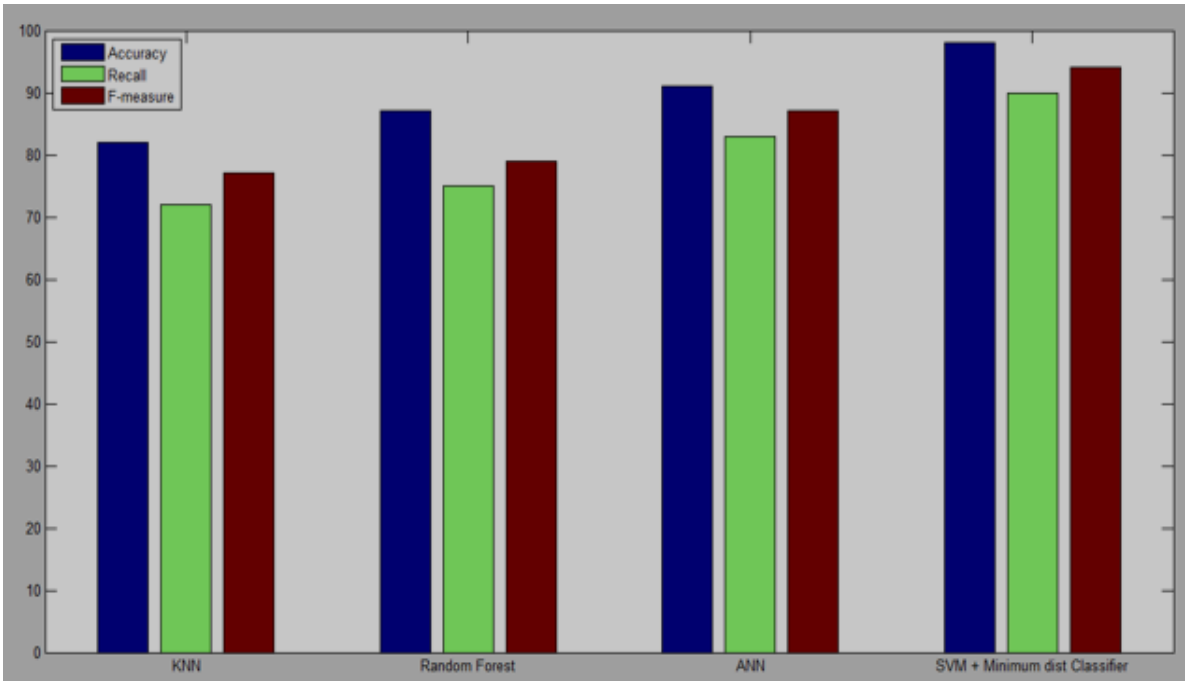


Fig. 10 - Relative Study of Copy Image Detection



The increased process of support vector machine was shown in the figure 9. After the improvisation the process increased up to 0.99%. The comparative study of raspberry PI, support vector machine, ken and an are shown in the figure 10.

5. Conclusion

Many physical gadgets are associated to the internet shaping. They are known as the Internet of Things. These gadgets are developing a calculation of useless and useful data. The preparing and transmission of this data was an investigating task. Various internet of things are talked in the current research work. A sector of security was the unmistakable application in the internet of things system. It was efficient to reduce the crime and provides security to individuals form business, home, military and so on. This research paper consumes the Raspberry Pi Internet of things basic characteristics the representation for the machine learning process. It ends the request of customer employments for instance, to transmit information safely by the process of internet of things engineering. It analyses for normal internet of things, very low manageable and finance process depend upon the structure of security learning process that aids detectable 97% proof, nearby identification and outsiders verification.

References

2nd International Conference on (pp. 1074-1077). IEEE https://ai.intel.com. n.d.

Amerini I, Ballan L, Member S, Caldelli R, Bimbo A Del, Serra G. A SIFT Based Forensic Method for Copy – *Move Attack Detection and Transformation Recovery* 2011; 6: 1099–110.

Ansari MD, Ghrera SP, Tyagi V. Pixel-Based Image Forgery Detection: A Review. *IETE J Educ.*, 2014; 55: 40–6. doi:10.1080/09747338.2014.921415.

Asghar, K., Habib, Z., & Hussain, M. (2017). Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, *49*(3), 281-307

Chen, C., McCloskey, S., & Yu, J. (2017, July). Image Splicing Detection via Camera Response Function Analysis. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 5087-5096).

Chen, J., Kang, X., Liu, Y., & Wang, Z. J. (2015). Median filtering forensics based on convolutional neural networks. *IEEE Signal Processing Letters*, 22(11), 1849-1853.

Dureja A., Pahwa P. (2018), Image Retrieval Techniques: A survey, *International Journal of Engineering & Technology.* Vol 7, No 1.2, 215- 219

Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. *In Proceedings of Digital Forensic Research Workshop*.

Hakimi, F., Hariri, M., & GharehBaghi, F. (2015, November). Image splicing forgery detection using local binary pattern and discrete wavelet transform. In *Knowledge-Based Engineering and Innovation (KBEI), 2015*

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems* (pp. 1097-1105).

Mishra, P., Mishra, N., Sharma, S., & Patel, R. (2013). Region duplication forgery detection technique based on SURF and HAC. *The Scientific World Journal*, *2013*

Mushtaq, S., & Mir, A. H. (2014, November). Forgery detection using statistical features. In *Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH), 2014 Innovative Applications of* (pp. 92-97). IEEE.

Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, *53*(10), 3948-3959.

Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on* (pp. 1-6). IEEE.

Uliyan DM, Jalab HA, Abdul Wahab AW. *Copy move image forgery detection using Hessian and center symmetric local binary pattern.* ICOS 2015 - 2015 IEEE Conf Open Syst 2016:7–11

Uliyan, D. M., Jalab, H. A., Wahab, A. W. A., Shivakumara, P., & Sadeghi, S. (2016). A novel forged blurred region detection system for image forensic applications. *Expert Systems with Applications*, 64, 1-10.

Walia, S., & Kumar, K. (2018). Digital image forgery detection: a systematic scrutiny. *Australian Journal of Forensic Sciences*, 1-39.

Zhang, J., Zhu, W., Li, B., Hu, W., & Yang, J. (2016, November). Image copy detection based on convolutional neural networks. *In Chinese Conference on Pattern Recognition* (pp. 111-121). Springer, Singapore.

Zhang, Y., Goh, J., Win, L. L., & Thing, V. L. (2016, January). Image Region Forgery Detection: A Deep Learning Approach. *In SG-CRC* (pp. 1-11)

Zhou, J., Ni, J., & Rao, Y. (2017, August). Block-Based Convolutional Neural Network for Image Forgery Detection. In *International Workshop on Digital Watermarking* (pp. 65-76). Springer, Cham.