Remote Sensing Image Forgery Detection Using Modified U-net

Himali Patil[1], Sangita Chaudhari[2], Vaibhav Narawade[3]

Department of Computer Engineering, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University,
[1]patilhimaliprakash@gmail.com
[2] sangita.chaudhari@rait.ac.in
[3] vaibhav.narawade@rait.ac.in

KEYWORDS: Remote sensing, Forgery, U-net, splicing.

ABSTRACT
Remote sensing is a technique for obtaining information about Earth's resources and environment typically through satellites. There is a plethora of applications like agriculture, military, security purposes, disaster management and recovery, Oceanography, Google Maps, Google Earth, Bing map wherein remote sensing plays an important role. It has become very easy to share these images nowadays over the Internet. However, it opens up the way to use them in an unauthorized way and alter it using many sophisticated technical approaches. There are many ways to alter image content (image forgery) to hide important information like copy-move, re-sampling, object replacement, and other attacks. Remote sensing data provides important information that helps in monitoring various applications such as image fusion, change detection and land cover classification. In Remote sensing image forgery, it is necessary to identify forged regions of the images because it maintains authenticity of image, as well as it is impossible for human vision to find the forgery. Lots of research has been done in the field of image forgery but very less research has been done in the field of remote sensing image forgery. Classification is one of the significant processes applied on remote sensing images and has a wider spectrum of use in multiple analysis approaches. However, if remote sensing images are forged then it has a severe impact on classification results and in turn on analysis and decision-making process.
In this paper, we have proposed a model to find out the forged region of remote sensing image. We have used RSICD (Remote Sensing Image Capturing Dataset) which contains the images collected from Google Maps, Google Earth, Bing map. We have created a synthetic dataset by altering the remote sensing images with the help of forgery techniques like copy-move, splicing. With this dataset we have implemented 2 variants of U-net and compared them to get the accurate result. First, we have implemented basic U-net to find out the forged region. Then we have implemented a modified U-net where the number of layers, size of images, epoch numbers are modified to detect the forgery. The variant of U-net is compared with the basic U-net model on the basis of different parameters like F1 score, Jaccard Index, Accuracy, RMSE, Peak SNR. From the results, it is observed that both the variants are giving significantly improved results compared to existing approaches.

1. INTRODUCTION

Image forgery is a big issue in publishing and printing today. With the help of social networking such as Facebook, Instagram, WhatsApp and may other services large amount of image data is generated and with that image processing software are also increased to tamper images. These images are the main source of fake news and are often used in malicious ways. Image forgery means manipulating or tampering a digital image to hide some meaningful or useful information about the image. There are different types of image forgery like copy move, splicing and re-sampling. Copy moves means coping particular object in another image. Splicing means combining two images and re-sampling means changing resolution of image, flipping, Rotating. First Image Forensics Challenge for image detection and localization was announced by

the IEEE Information Forensics and Security Technical Committee (IFS-TC) in 2013. They provided an open dataset of digital images composed of images captured under different lighting conditions and fake images created using algorithms. Various software's are available to change the parameters of an image such as pixels, size and resolution.

Nowadays, remote sensing images must be protected effectively. There are a lot of ways of manipulating image content to hide important information: combining multiple images, inserting some object in image, splicing, flipping, rotating, changing resolution, changing size of image, object replacement and other attacks. Remote sensing imagery overhead can be easily obtained and shared. The integrity of this type of images can no longer be assumed as sophisticated image manipulation tools based on classical and machine learning are available. Satellites images gives a good idea about what is happening at every point in the world, especially over oceans where large gaps in data occur. Data can only be taken at certain points around the world, without this data, forecasting would be as difficult as not having satellites. Images are used in various applications like agriculture, oceanography, geology, landscape, military and in many other fields. One of the popular examples of remote sensing image forgery is that colourful image of India during Diwali. People are claiming is that it is a picture of India taken from space on Diwali night. But it is not true, that image was created by the National Oceanic and Atmospheric Administration (NOAA) to show the population growth in India and also may other images are stitched together.

A question is that whether these images are authentic. It is necessary to find such type of manipulation as many of people consider whatever shared with them is true and forward to other people which is misleading everyone. For this high-resolution dataset Remote Sensing Image Capturing Dataset (RSICD) is used which consists of un-forged images. From this data set another dataset is formed for forged images.

2. PROPOSED SYSTEM

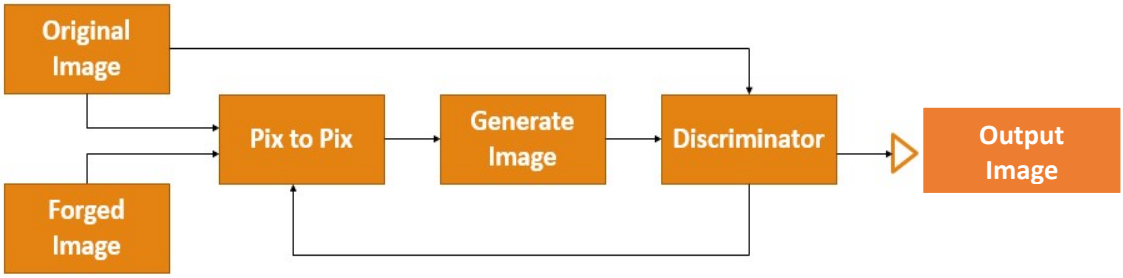

Figure 1. Proposed System

In proposed system, Figure 1 shows the complete implementation and give the basic idea about the system. For input dataset with different forgery techniques is created. In dataset for 100 images copy move, splicing techniques are applied and total dataset of 200 images is formed and this are given as input to dimensionality reduction and band selection. Where Principal components analysis (PCA) technique is used for reducing the dimensionality. This technique is applied to multispectral and hyperspectral remotely sensed data. PCA is a dimensionality reduction commonly used to reduce the dimension of the variables of a larger dataset being compressed to the smaller one that contains the most information to create an efficient model.

Pix2pix model is used for training. The pix2pix model is the type of conditional GAN used for general image to image translation where the generation of the output image is conditional on an input, in this case, a original image. The discriminator receives both an original image and a forged image and must determine whether the image is a probable transformation of the forged image. After training subtract the original input image from forged image and as a output forged region is displayed which is a final output image.

In proposed system, Remote Sensing Image Capturing Dataset (RSICD) is used which contains high resolution of images. From this Dataset 100 images are taken of size 256 x 256. On this 100 images copy move, splicing techniques are applied and total dataset of 200 images is formed and trained.

3. IMPLEMENTATION

For training the system Pix2pix model is used where learning rate is optimized as well as size of pixel to pixel is optimized along with type is also optimized. Type means weather the image is input image or forged image or difference image (Original - forged image). Total 500 images are given to model for training. These images are taken from Remote Sensing Image Capturing Dataset (RSICD) of size 256 x 256. Pix2pix network is better as we are giving input as forged image. The Pix2Pix is a generative adversarial network (GAN) for image-to-image translation. It is based on the conditional generative adversarial network CGAN, where a target image is generated, conditional on a given input image.
After checking pixels of both the images prediction image is generated. The prediction of network is averaged obtaining a final robust and accurate likelihood estimate for each pixel of the image. Possible forged image is given as input to the trained network and in output getting possible un-forged image. And then by subtracting it is giving output forged image where only forged region is highlighted.

3.1 Basic U-Net

Pix2pix is also called as CGAN (Conditional Generative Adversarial Network). Adversarial means reproducing the image which is not existing. The conditional generation of images by a generator model is CGAN. CGAN consists of a generator and a discriminator model. The generator model is responsible for generating new feasible images that are distinct from actual dataset images and the discriminator model is responsible for classifying a given image are either real or fake. U-net is the network used in CGAN.As name suggest U-net is a encoder-decoder network architecture consisting of four encoder blocks and four decoder blocks connected by a bridge in U shape. Where encoder acts as a feature extractor, learning an abstract representation of the input image through a sequence of the encoder blocks. The decoder network doubles the spatial dimensions and half the number of feature channels.

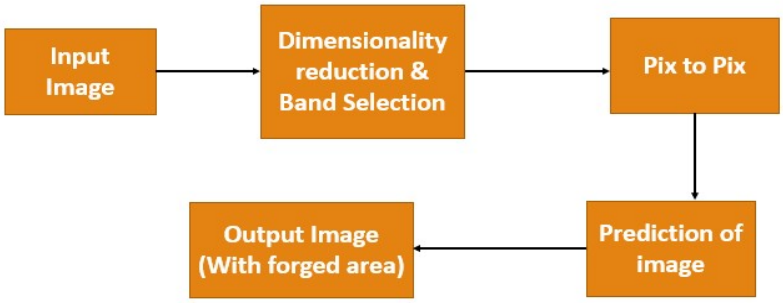

Figure 2. Basic U-net

In training Figure 2, it has one original image and one forged image. It gives forged image to pix2pix for training and demands for image that is same like original image. So, it generates one generated image, which is given as input to discriminator. Discriminator checks the difference between original image and generated image. If difference is true, it stops the optimization of pix2pix and if difference is false or it needs improvement then the operation continues. As soon as operation stops that means network is generated.
U-net is used with generator as well as discriminator. The generator synthesizes predictions for the forged region from the input images. The left part of generator is called as encoder which is contracting part which reduces the size of image and right part is called as decoder which is expansive path which will bring the image into its original size which will generate prediction image. Then the prediction image along with ground truth is given to discriminator. Here the size of network is reduced and it will give output as image is fake or not.

3.2 Modified U-Net

In modified U-net the image is input at the starting of the network. The data is then spread through all possible paths and, in the end, the segmentation map comes out. we modified the parameters such as convolution layer. In basic u-net there are 23 layers here we increased that to 32 to get more accurate result. Main disadvantage of increasing layers is that performance can be decreased but accuracy is not only depended upon number of layers there for we have trained the model properly to 500 epochs to get accurate result and to not to decreased performance of u-net. Maximum epochs in basic u-net are 100. In modified u-net u-net consists of encoder and decoder of 3 X 3 convolutions. Procedure of finding forgery in image is same only difference is that parameters are modified. Here for training original and forged image is given to network and then u-net model is trained with modified parameters and then by subtracting original image from forged image we get output as forged region.

4. EXPERIMENTAL RESULTS

RSICD data of remote sensing imaged is used where 1st we have applied copy move forgery to images, where small part of image is forged and other method is splicing where half part of image is spliced with other image. We applied basic u-net and modified u-net to find out forged region. Forged region is highlighted from image. The variant of U-net is compared with the basic U-net model on the basis of different parameters like F1 score, Jaccard Index, Accuracy, RMSE, Peak SNR.

A. Original Image | B. Copy move Forgery | C. Splicing | D. Output of Copy move | E. Output od splicing

Figure 3. Basic U-net

A. Original Image | B. Copy move Forgery | C. Splicing | D. Output of Copy move | E. Output od splicing

Figure 4. Modified U-net

In Basic U-net Figure 3 and Modified U-net Figure 4 A. is original image from dataset. B. is a copy move forged image where we have inserted small region and C. is a spliced forged image where we merged two images half part is original image and other half part is from other image which is actually a forged region and D. and E. are an output image where we are getting actual forged region highlighted of copy move and spliced forgery.

4.1. Parameters Comparison

	Basic U-net		**Modified U-net**	
Parameters	**Copy Move**	**Splicing**	**Copy Move**	**Splicing**
MI	0.1369061707	0.2383280777	0.04772816365	**0.330932104**
PEAK SNR	6.22989467	6.917144317	5.816523357	**7.134349818**
RMSE	0.2813286576	0.259938926	**0.2950297923**	0.2535056067
F1 Score	0.9996694736	0.9859888855	**0.999777388**	0.9798653699
Accuracy	**0.9996693786**	0.9857970159	0.9977692936	0.9794642903
Jaccard index	**0.9993391656**	0.9723649686	0.9955576493	0.9605255434

From above table we can conclude that, Mutual Information (MI) is always greater than or equal to zero. MI of modified U-net is larger than Basic U-net that means in Modified U-net there is greater relationship between two variables. For PSNR we will see higher the PSNR value better quality of compressed image. RMSE values are better that means images are accurate. F1 score is almost equal to zero for all types of images that means classification is accurate. While calculating accuracy higher the value better the output results. Jaccard index ranges from 0 to 1 if it is closer to 1 that means two images are similar. So for copy move technique in both variants of U-net we can see thar index is 0.99 almost near to 1 that means two images are same as we have only altered small part of image.

5. CONCLUSION

Remote sensing is an important technique for obtaining information about Earth's resources and environment. The remote sensing images are popular due to the fact that it is easily available online through various mapping applications such as Google Earth and Bing Maps. These applications have helped the GIS community with project planning, disaster and natural disaster monitoring, and civil defence support. Remote sensing data provides essential information that helps in monitoring various applications such as image fusion, change detection and land cover classification. The focus is on remote sensing image forgery because remote sensing images are only used for classification purpose for classifying its component and based on that some decisions are taken so if forgery happens in that then classification will be wrong and results will not be accurate. From the above approach we can say that modified U-net is better than basic U-net as it is giving better results in most of the parameters.

REFERENCES

[1] S. Kalyan Yarlagadda, D. Guera, P. Bestagini, F. Zhu, ¨ S. Tubaro, and E. Delp, "Satellite image forgery detection and localization using gan and oneclass classifier," Proceedings of the IST International Symposium on Electronic Imaging, vol. 2018, pp. 214–1–214–9, Feb. 2018. Burlingame, CA.

[2] J. Horvath, D. Guera, S. Kalyan Yarlagadda, P. Bestagini, F. Maggie Zhu, S. Tubaro, and E. J. Delp, “Anomaly-based manipulation detection in satellite images,” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 62–71, June 2019, Long Beach, CA.

[3] L. Ali, T. Kasetkasem, F. G. Khan, T. Chanwimaluang, and H. Nakahara, “Identification of inpainted satellite images using evalutionary artificial neural network (EANN) and knearest neighbor(KNN) algorithm,” Proceedings of the IEEE International Conference of Information and Communication Technology for Embedded Systems, pp. 1–6, May 2017. Chonburi, Thailand.

[4] E. R. Bartusiak, S. Kalyan Yarlagadda, D. Guera, F. M. Zhu, ¨ P. Bestagini, S. Tubaro, and E. J. Delp, “Splicing detection and localization in satellite imagery using conditional gans,” Proceedings of the IEEE International Conference on Multimedia Information Processing and Retrieval, pp. 91– 96, March 2019, San Jose, CA.

[5] J´anos Horv´ath, Sriram Baireddy, Hanxiang Hao, Daniel Mas Montserrat, Edward J. Delp: ”Manipulation Detection in Satellite Images Using Vision Transformer.” CVPR Workshops 2021: 1032-1041

[6] J. Horvath, D. Guera, S. Kalyan Yarlagadda, P. Bestagini, F. Maggie Zhu, S. Tubaro, and E. J. Delp, “Anomaly-based manipulation detection in satellite images,” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 62–71, June 2019, Long Beach, CA.

[7] R. Chalapathy, A. K. Menon, and S. Chawla, “Anomaly detection using one-class neural networks,” arXiv:1802.06360, February 2018.

[8] D. Mas Montserrat, J. Horvath, S. K. Yarlagadda, F. M. Zhu, and E. J. Delp, “Generative autoregressive ensembles for satellite imagery manipulation detection,” in IEEE International Workshop on Information Forensics and 6 Security (WIFS), 2020

[9] A. Piva, “An overview on image forensics,” ISRN Signal Processing, vol. 2013, pp. 22, 2013. [10] June 2019, Long Beach, CA. [4] J. Brandt, “Spatio-temporal crop classification of low-resolution satellite imagery with capsule layers and distributed attention,” arXiv:1904.10130, April 2019.

[10] Andrey Kuznetsov” Remote Sensing Data Copy-Move Forgery Protection Algorithm”, Part of the Lecture Notes in Computer Science book series (LNCS, volume 9972), pp. 10 September 2016.

[11] Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopolou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. 7(6), 1841–1854 (2012)

[12] https://towardsdatascience.com/image-forgery-detection2ee6f1a65442

[13] https://www.tensorflow.org/tutorials/generative/pix2pix

[14] https://paperswithcode.com/dataset/rsicd

[15] https://github.com/201528014227051/RSICD_optimal