Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

Deep Learning-Based Image Tamper Detection Techniques: A Study

Shilpa Ravindra Muley
Research Scholar, Dept. of CSE
Shri JJTU University,
Rajasthan

Shailesh Kumar
Professor, Dept. of CSE
Gopalan College of Engineering and Management
Bengaluru

***Abstract*— The most potent and reliable form of expression is photography. Digital photos today serve as hidden communication agents in addition to providing false information. Users and experts in picture editing work with digital photographs to achieve different goals. Scientists and researchers manipulate images for their work to be published; journalists create dramatic effects for their stories by tampering with medical images to misrepresent patients' diagnoses; politicians, lawyers, and forensic investigators use tampered images to sway public opinion, the court, or the law, and so on. As a result, separating real photos from copies and verifying the legitimacy of digital photos have become increasingly important recently. This work aims to comprehend various methods for detecting image manipulation through the application of Deep Learning.**

***Keywords*— Image Tampering, CNN, Deep learning, Copy-Move**

I. INTRODUCTION

An image is a unique information carrier that conveys a meaningful message. They play a crucial role in transporting sensitive data. However, secrecy is not granted arbitrarily or without a system. The goal of many security services is to improve information security. One such method of information security is encryption. Images serve as authentication systems for copyright protection, hence they must be kept strictly confidential. To protect the data, images serving as authenticators are encrypted.

Information can be transformed into an incomprehensible format by the process of encryption, which necessitates understanding the recovery procedure. While it does not permit content interception, it does not stop interference. Using encryption, which is especially useful for medical image retrieval, one can achieve the security of an image [Hyma et al., 2016]. Encryption solves security issues like authentication and copyright protection, and research is being done in this area, but there is still more work to be done because digital technology is easily manipulated.

Technology has made it easier for even a non-expert to alter digital images with the development of picture editing software, which has made securing images uploaded to the Internet extremely difficult. Authentication, tamper detection, detecting the altered region, picture matching, device identification, and other challenges are major issues that need to be overcome in this regard. Image tampering is the act of modifying, removing, or adding sensitive information from an image without leaving any evidence and with malicious intent. It can occasionally be changed with the goal to disparage or foster a false impression of a person or a system, and it is only acceptable if it does not affect the meaning it conveys. These problems are handled by the field of digital forensic science known as digital image forensics. Applying specialized knowledge to evaluate a picture's validity and integrity by explaining its contents is what happens when an image is used as evidence in court cases. In order to identify devices and detect forgeries, it analyses the image's content and metadata.

1.1. Image Tampering Classification:

Images can be altered with simple operations including scaling, rotating, copying, pasting, blurring, adding noise, and cutting. Digital picture forging can be divided into three categories based on the post-processing techniques used to tamper with the image: copy-move assaults, image splicing, and image retouching. One kind of image counterfeiting that typically causes no harm is image retouching. Its motto can be "improving the image to have an eye-catching appearance for news, articles, and magazines." For instance, enhancing a face's brightness increases the accuracy with which the real event is interpreted in a surveillance video; nevertheless, in a photography competition, the same enhancement can be viewed as a counterfeit. One instance of image editing is seen in Figure 1. Depending on the situation, the place, and the method of alteration, changing an image could be acceptable. The process of determining if the image accurately depicts the fact is known as authentication.

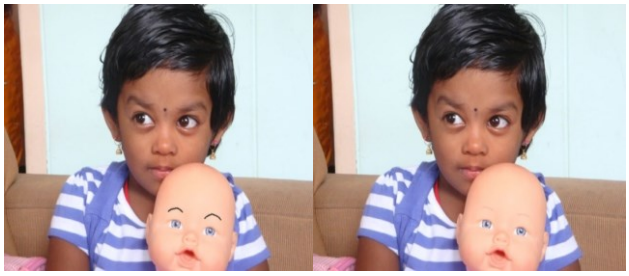

Fig.1. A Retouched Image Example (Left) the initial image (right) edited image

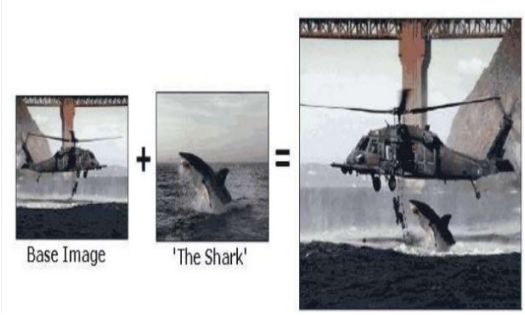

Fig.2. Splicing an Image Example Left: two distinct images; right: a spliced image.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

An image can be made into a fake one by copying and pasting elements from another image using the process known as "image splicing". Photoshop and other advanced software are used to create these images, which are produced through a process known as digital photomontage. An illustration of image splicing is presented in Figure 2 [Sunil Kumar et al., 2015]. Transforming the original image into a bogus one involves duplicating the shark.

Fig.3: Copy-Move Forgery Example

The goal of a copy-move attack is to exaggerate, duplicate, or conceal information by copying, moving, and pasting a specific portion of an image to a particular location inside the original image. To make pasted portions invisible, post-processing techniques like blurring are applied to their edges. Figure 3 illustrates a copy-move altered image. The original image is on the left, and a flight has been copied, rotated, and pasted into the image on the right. These actions are essentially invisible to the human sight, but they can be recognized by examining the statistical irregularities in the image. In order to identify tampering, image authentication must be obtained.

1.2. Classification and Techniques for Image Tamper Detection:

Advanced techniques for manipulating digital images may not create perceptual evidence of the manipulation, but they do introduce evidence in the image's statistical behavior. The image is not immaculate even if these traces are absent. There are several methods available for identifying manipulated images from the originals by taking use of the traces. However, each approach can only resist a limited number of attempts and is limited to a specific type of tampering. Accordingly, research is conducted quickly, and the results are provided here in the form of a report on cutting-edge techniques for detecting digital image tampering.

Developing methods for detecting and localizing image tampering is the main focus of recent image forgery research. These methods are categorized in Figure 4. Many methods have been devised to use the images past information to determine whether an image is tampered with or unaltered. These methods pertain to the identification of active forgeries. However, there are situations in which previous knowledge is unavailable, such as in court, where an image is used as evidence. Techniques for passive forgery detection can be used in these kinds of situations. Digital signatures and watermarking are two methods for detecting active forgeries.

In order to identify forgery, it is important to possess the original watermark or key for signature verification. These methods are alternatively referred to as Non-Blind methods. Techniques for detecting passive forgeries include splicing detection, resampling detection, and copy-move detection. These image forgery detection techniques are blind and do not rely on previously acquired data.

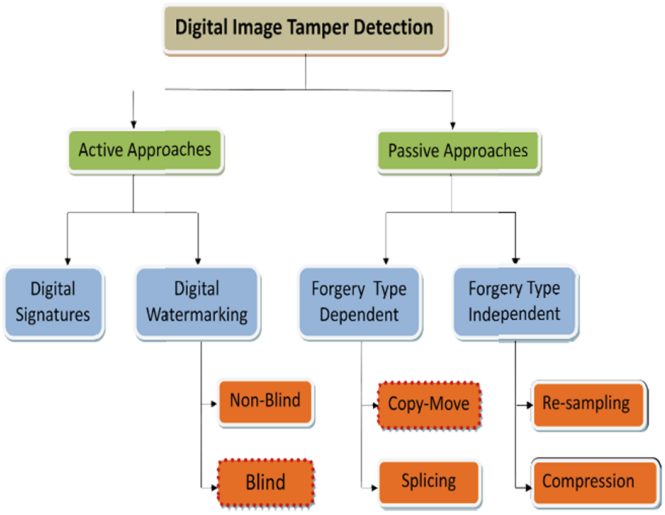

Fig.4. Techniques for Detecting Digital Image Tampering and Classification

II. LITERATURE SURVEY

Image piracy has existed for decades and is not a modern issue. The unreliability of memory is the only thing the researcher investigates. We now have access to the newest image editing software, such as Photoshop, and tools. There are many false images all around us. With these images, you can create a lasting recollection that will stick in our minds since our minds recognize them as real. These false recollections distort our history and influence our actions now and in the future, including how we perceive the world, protest, vote, make decisions, and consume.

Interpolation manipulation has been identified in Lukas et al.'s (2006) discussion of the Colour Filter Array (CFA), which is used to generate RGB by interpolation. The digital image forgery was detected using the CFA as a forensic tool. Each camera produces a unique effect because of CFA. Phase and magnitude information utilized for forgery detection, Chen, W., et al., 2007. Statistical moments of the wavelet sub band have been used to analyse the differences between the original and spliced images. The frequency domain properties are broken by the wavelet sub band.

The Photo Response Non-Uniformity Noise (PRNU) approach for tampering detection was described by Chen, M. et al. (2008). It discovers that each camera produces unique noise. Tampering has had an impact on this noise. The camera's noise functioned as an image fingerprint, aiding in the detection of image manipulation. One such method for detecting picture tampering is the camera limitation technique. Three light sensors are typically replaced with a single light in cameras due to cost considerations.

For the purpose of detecting image forgeries, T. Ahonen et al. (2009) proposed the use of a rotation invariant-based LBP

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

approach and local binary pattern histogram Fourier feature (LBPHF). Frequency features are produced by the Fourier approach. Rotation invariant improves the LBP's performance and gets rid of its limitations. Tan X, Triggs B (2010) talked about the idea of ternary patterns, how local ternary patterns (LTP) are implemented using ternary patterns (0, -1, 1) and binary patterns (0, 1) for LBP.The standard LBP technique's limitations are eliminated by the introduction of LTP. Compared to LBP, it is more dependable.

Chen, Y. L. and C. T. Hsu (2011) Image forgery modifies the image's original content. Images may occasionally undergo specialized processing such as histogram equalization, resampling, filtering, and contrast enhancement. Recovering the image's processing history is made possible by the forensic examination of these activities. These techniques primarily serve two goals: picture editing and erasing evidence of forgeries or making fabricated photos believable. A system that can identify image splicing must be developed over a variety of post-processing techniques. Certain operations, such as Discrete Wavelet Transform (DWT), Local Binary Pattern (LBP), Rotation Invariant Cooccurrence (RIC-LBP), Local Ternary Pattern (LTP), Enhanced Local Ternary Pattern (ELTP), and Local Binary Pattern (LBP), along with feature extraction approaches, are extremely helpful in identifying forgeries.

The method to identify the traces left behind by JPEG recompression was proposed by Chen et al. (2011). Utilised the image feature of the JPEG format in the transform and special domains. They stand for the reliability and potency of the suggested model. He Z et al. (2011) used a matrix based on edge gradients to determine the run length. The more features are found using DWT. To locate more characteristics, one uses the approximation coefficient (Low-Low) band. To extract more features, DWT implements run length. SVM classification is used to identify forgeries.

He et al. (2012) used the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains to create a Markov based feature extraction method. Support vector machines (SVM) have been used in the classification process to identify instances of tampering. Shi et al. (2012) classified the texture characteristic using a contemporary Steganalysis technique. Cliques, Markov neighbourhoods, LBP, and legal masks are all combined. Steganalysis uses a classifier based on FLD.

R. Nosaka et al. (2012) emphasize the STD filter applied over the image to highlight the image information. The internal statistic of the picture was retrieved using the Rotation-Invariant Co-occurrence (RIC-LBP) operator between neighbouring Local Binary Patterns, and it was classified to identify any forgeries. Li et al. (2013) used a Gaussian model on a JPEG image to build a relationship between local correlation patterns generated by a Colour Filter Array (CFA) to detect image counterfeiting. The CFA's posterior characteristic is used to calculate the frequency of the CFA traces.

In their 2013 study, De Carvalho et al. talked about feature extraction using texture and the image's edge. The image's various faces are subjected to this technique. For the purpose of detecting manipulation, the JPEG format of the images in the CASIA v1.0 data set is utilised. JPEG images are compressed several times to allow for blocking artefact, quantization, and tampering. It is applied to both frequency and special domains, in that order.

In 2013, Li L. et al. developed a revolutionary copy-move forgery detection method. Create an overlapping circular block by dividing using a filter. The RILBP (rotation invariant local binary pattern) approach is used to extract features. For forgery detection, M. Hussain et al. (2014) implemented LBP on a wavelet descriptor and a support vector machine as a classifier. This property is described in terms of frequency using the wavelet approach. The LBP's performance enhanced as a result of the image's frequency band.

The ELTP technique, an advanced LTP approach, was proposed by Yuan JH et al. (2014). The fully enhanced local ternary pattern (CELTP) is used to implement the ELTP in this technique. The threshold was created using an auto-adoptive strategy in place of the conventional grey value of the central pixel. Satpathy et al., (2014) used the Discriminative Robust Local Binary Pattern (DRLBP) with the support of the Discriminative Robust Local Ternary Pattern (DRLTP) to detect the edge and texture of an image for feature extraction, thereby solving the discriminative problem of bright objects with dark backgrounds or dark objects with bright backgrounds.

DCT image splicing using LBP was identified by M. Hariri and F. Hakimi (2014). The input image's chrominance is separated into non-overlapping pieces. The K-Nearest Neighbour (KNN) technique is used to classify the characteristics based on their frequency. Muhammad, G., et al. (2014) applied the local binary pattern approach to an image using a steerable pyramid transform. Using a steerable transform, multiple scale and multiple orientation sub bands are produced over the image's Cb and Cr components. SVM classifier was used to classify the images in order to detect forgeries.

Active and Passive two approaches are employed for image forgery detection (Agarwal, S., Chand, S., 2015). Watermarking or digital signatures are two active techniques used to secure images. It is exceedingly difficult to identify image forgeries using passive (blind) methods since there is no prior knowledge about the image. Splicing method and copy-move are the two subparts of passive technique. With copy-move, only one image is used to create a forged image; certain image elements are copied and pasted into the same image. When two or more photos are combined to create a forged image, a portion of the original image is copied and pasted into another image.

The newest technology and techniques make it possible to create a doctored image at your fingertips. Understanding the post-processing steps is really challenging. A variety of processes, such as filtering, histogram equalisation, resampling, and contrast enhancement, are applied to the photos in order to either conceal the evidence of the forgery or create a realistic-looking false image. The process history of a picture can be recovered and counterfeit detection assisted by forensic analysis of these actions. The suggested work uses passive image fraud detection approaches that make advantage of the device's features to identify encoding attributes, lighting

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

effects, and capturing capabilities. Several innate methods are also applied.

In order to extract features from LBP, Zhang et al. (2015) implemented various sizes discrete cosine transform (DCT). To reduce dimensionality and prevent excessive computational cost, kernel principal component is utilised. SVM is then used for classification in order to distinguish between pristine and fraudulent images. S. Agarwal and S. Chand (2015) developed an Entropy filter and a texture operator based on local phase quantization (LPQ) for forgery detection. The image boundary is highlighted using an entropy filter, and the image's internal statistic is obtained using LPQ. SVM is used to classify images.

A hybrid framework was presented by J. Goh and V. L. L. Thing (2015) to extract all image features and create the optimal feature set. To improve results, features are categorised using a classification algorithm. Chrominance colour channels were used by Hakimi et al. (2015) to partition the non-overlapping block. Wavelet transform is used to apply LBP on the overlapping block. SVM is used to classify the features that are extracted using principal component analysis (PCA).

Splicing, or copy-move, is a technique that Tralic et al. (2016) utilised to detect image tampering. In copy move, a single image is used for forgeries. They suggested a hybrid method that combined LBP descriptors with cellular automata, which, as a result of the hybrid technique's application, enhances LBP performance. According to Agarwal and Chand (2016), the internal statistic of the picture information obtained by rotation-invariant co-occurrence over the neighbouring LBP operator is highlighted by the application of a standard deviation filter, which also helps to identify any discovered forgeries.

Alahmadi et al. (2017) used a small portion of the image to identify image fraud. The characteristics are extracted using the Cb and Cr components. The LBP is used to extract features, while DCT is utilised to create the image's frequency band. The SVM classifies the data in order to detect forgeries. In P. Cavalin et al.'s (2017) implementation of texture description, the local binary pattern (LBP) technique and the conventional grey level co-occurrence material (GLCM) are used. As a fisher vector, CNN and multi-scale patch-based recognition are utilised.

El-Alfy ES and Shah A (2018), an image is considered to be forged if a portion of it is copied and pasted into the original or a different image. The patch piece has been impacted by pasting; it may or may not be altered. In both situations, there has been an impact on the image's internal statistic. When editing, the original image is subjected to smoothing or blurring, which affects how the pixels in the image correlate.

In their study, Abrahim et al. (2018) applied higher-order statistical features, the LBP descriptor, and HOG (Histogram oriented gradient) to various textures and colours. These features were subsequently merged into a feature vector and inputted into an ANN (Artificial neural network) in order to enhance the accuracy rate. In 2018, Shah A and El-Alfy ES used multiple-scale LBP to apply a passive image forgery detection approach. DCT is used in conjunction with LBP to generate the image's frequency. The technique of K-fold cross validation is used to train and test images.

For encoding tampering across a new historical data collection, Asghar, K. et al. (2019) presented a robust binary pattern. When compared to new historical datasets, the forgery detection performance improved. Support vector machine, or SVM, the classifier was employed to categorise the faked image. With a new dataset, this is doable. A study by Gan Yanfen et al. (2019) suggests using the VGG-11 convolution neural network to automatically spot video frame hacking and video intra-frame forgery detection. This algorithm first breaks down the films into frames, then determines the motion residual map for each frame and extracts the steganography features. The neural network's training set is built using these example sets of steganography features. Video manipulation was detected using these training sets. This method improves detection performance by requiring additional network structure optimisation in the model's convolution and pooling layers.

The Otsu optimum threshold approach is employed in place of mean absolute deviation, as explained by Kanwal, N. et al. in 2020. OELTP is the main characteristic of every block; its energy is utilised to minimise dimensionality and simplify the process.

Sujatha G. et al. (2021) have presented the Difference hashing algorithm, also known as D-hash. This method uses the difference in pixel intensities between each frame to calculate D-hash in tampered video frames.

III. PROPOSED METHODOLOGY

When it comes to determining the authenticity of a picture through features, footprints, digital signatures, and digital watermarking, the state-of-the-art methods for image tamper detection have their own limits. This makes it extremely difficult to create a framework for detecting picture manipulation based on the suggested authentication technique, which establishes the image's integrity and validity in order to identify any altering.

The suggested approach is divided into two stages. An image authentication system is created in the first step with the possibility of integrating it into the current picture acquisition model. A few extra stages are included in this process to help establish the image's legitimacy by adding a verification code. In order to create an authorized digital image, the verification code is self-generated using the Godelization Technique, added to the image's metadata, and embedded in the image using the suggested Location Decision Embedding Technique. An image generating process with an integrated authentication mechanism is provided by this step.

A mechanism for detecting and localizing copy-move tampering is presented in the second phase. When an image is presented as evidence in court, it follows the steps of the suggested detection procedure, as seen in Figure 5, to demonstrate its nativity. It then uses the verification code to confirm its legitimacy. When a tampered image is detected, the tampered area is located using the copy move tamper localization process.

Image authentication mechanism: An autogenous verification code [Mani et al., 2018a] is incorporated into the image to authenticate and ensure its integrity, thereby establishing an effective authentication mechanism.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

The "Location Decision Embedding Technique (LDET)" [Mani et al., 2014] is a newly developed embedding method that perceptually invisible embeds the verification code in the image at the moment of capture. There is a way to prove your identity built into the General Image Acquisition Model [Mani et al., 2018b]. Verification code is created utilizing the Godelization approach during the post-processing stages of image capture and then embedded in the image using the suggested Location Decision Embedding approach (LDET). Without requiring the original image, the verification code functions as the image's in-camera fingerprint and aids in detecting image manipulation.

Image Tamper Localization Mechanism: After an image is found to have been altered, its tampered area has to be located. This is accomplished by employing the SURF feature detection and extraction technique to extract the image's features. The suggested feature matching algorithm matches these features in order to identify the image's copy move tampering area.

IV. CONCLUSION

The scholarly literature consistently emphasizes the challenge of identifying image modification due to the wide range of software applications currently accessible. Each feature exhibits a high degree of susceptibility to interference processes. Hence, a crucial element of the tamper detection method is identifying characteristics inside the process of picture tampering. In the realm of forgery assaults, encompassing splicing, compression, rotation, resampling, copy-move, and other variants, the existing approaches have yet to achieve a level of precision that can be deemed great.

The utilization of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) serves as the fundamental basis for the current progress in computer vision pertaining to the development of approaches for detecting semantic tampering. Furthermore, it has been determined that the acquisition of more precise outcomes necessitates the development of a proficient feature extraction mechanism based on Deep Learning, which can successfully learn the correlations among pixels. Convolutional neural networks (CNNs) have gained significant popularity in the domain of image forensics over the last decade. The fundamental objective of these methods has been to train Convolutional Neural Networks (CNNs) in order to effectively discern and classify distinct camera models based on optimal feature identification. One advantage of utilising Convolutional Neural Networks (CNN) is that they may directly extract features from the image dataset. The primary advantage of CNN-based approaches is in their ability to autonomously extract classification features from image input. Furthermore, recent findings have revealed that convolutional neural network (CNN) methods employed for the purpose of detecting tampering exhibit a high level of efficacy in precisely discerning several occurrences of tampering.

REFERENCES

[1] Abrahim, AR, Rahim and MSM, Bin SG (2018). “Splicing image forgery identification based on artificial neural network approach and texture features” Cluster Compute: 1-14. https://doi.org/10.1077/s10586-017-1668-8.

[2] Agarwal, S., Chand, S., (2015), “Image forgery detection using multi scale entropy filter and local phase quantization” International Journal of Image, Graph Signal Process 8:64-74. https://doi.org/10.5815/ijigsp.2015.10.08.

[3] Alahmadi A, Hussain M, Aboalsamh H, Muhammad G, BebisG, Mathkour H (2017).“Passive detection of image forgery using DCT and local binary pattern” SIViP11 (1):81–88. https://doi.org/10.1007/s11760- 016-0899-0

[4] Asghar, K., Sun, X., Rosin, P.L. (2019). “Edge–texture feature-based image forgery detection with cross-dataset evaluation” Machine Vision and Applications30, 1243–1262 (2019). doi.org/10.1007/s00138-019-01048-2

[5] Agarwal, S. and Chand, S. (2016). “Texture operator based image splicing detection hybrid technique” IEEE International conference on computational intelligence and communication technology, https://doi: 10.1109/cict.2016.31.

[6] Cavalin P, Oliveira LS (2017). “A review of texture classification methods and databases” In: 2017 30th SIBGRAPI Conference on graphics, patterns and images tutorials (SIBGRAPI-T).IEEE, pp1–8

[7] Chen, M., Fridrich, J., Goljan, M., & Lukas, J. (2008). “Determining image origin and integrity using sensor noise” IEEE Transactions on Information Forensics and Security, 3(1), 74–90.doi:10.1109/TIFS.2007.916285

[8] Chen, W., Shi, Y. Q., & Su, W. (2007). “Image splicing detection using 2-dphase congruency and statistical moments of characteristic function” Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, 6505, 26.

[9] Chen Y. L., & Hsu, C.T. (2011). “Detecting recompression of JPEG image via periodicity analysis of compression artifacts for tampering detection” IEEE Transactions on Information Forensics and Security, 6(2), 396–406.doi:10.1109/TIFS.2011.2106121

[10] Chierchia, G., Poggi, G., Sansone, C., &Verdoliva, L. (2014). “A bayesian-MRF approach for PRNU-based image forgery detection” IEEE Transactions on Information Forensics and Security, 9(4), 554–567.doi:10.1109/TIFS.2014.2302078

[11] Chi-ho Chan, Josef kittler, Kieron Messer. (2007). “Multi-scale local binary pattern histograms for face recognitions” Springer-verlag berlin Heidelberg, vol. 4642, (pp. 809-818). doi: https://doi.org/10.1007/978-3-540-74549-5_85.

[12] Cortes C, Vapnik V (1995). “Support-vector networks” Mach Learn 20(3):273–297.

[13] De Carvalho, T. J., S., Riess, C., Member,A., Angelopoulou, E., Pedrini, H. H., & Rocha, A. D. R. (2013). “Exposing digital image forgeries by illumination color classification” IEEE Transactions on Information Forensics and Security, 8(7), 1182–1194.doi:10.1109/TIFS.2013.2265677.

[14] Dong, J., Wang, W., & Tan, T. (2013). “CASIA Image Tampering Detection Evaluation Database” In 2013 IEEE China Summit and International Conference on Signal and Information Processing, 422–426.doi:10.1109/ChinaSIP.2013.6625374.

[15] F. Hakimi, M. Hariri and F. G. Baghi, (2015)."Image splicing forgery detection using local binary pattern and discrete wavelet transform" 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), 2015, pp. 1074-1077, doi: 10.1109/KBEI.2015.7436195.

[16] Gottschlich, C., Marasco, E., Yang, A.Y., & Cukic, B. (2014). “Finger print liveness detection based on histograms of invariant gradients” In Biometrics (IJCB), 2014 IEEE International Joint Conference (pp.1– 7). IEEE. Retrieved from doi:10.1109/BTAS.2014.6996224.

[17] He Z, Sun W, Lu W, Lu H (2011). “Digital image splicing detection based on approximate run length” Pattern Recognition Letter 32(12):1591–1597.https://doi.org/10.1016/j.patrec.2011.05.013

[18] He, Z., Lu, W., Sun, W., & Huang, J. (2012). “Digital image splicing detection based on Markov features in DCT and DWT domain” Pattern Recognition, 45(12), 4292– 4299.doi:10.1016/j.patcog.2012.05.014

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 02, February 2024

[19] Hsu, Y. F., & Chang, S. F. (2006). "Detecting image splicing using geometry invariants and camera characteristics consistency" 2006 IEEE International Conference on Multimedia and Expo, ICME 2006—Proceedings, 2006, 549–552.

[20] Hussain, M., Muhammad, G., Saleh, S. Q., Mirza, A. M., & Bebis, G. (2013). "Image forgery detection using multi-resolution weber local descriptors" Eurocon 2013 (pp.1570–1577).Zagreb, Croatia: IEEE.doi:10.1109/EUROCON.2013.6625186.

[21] J. Goh and V. L. L. Thing, (2015). "A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection" International journal of electronic security and digital forensic, vol. 7, no. 1, pp. 76-104, 2015, doi:10.1504/IJESDF.2015.067996.

[22] J. Zhang, Y. Zhao, and Y. Su, (2009). "A new approach merging Markov and DCT features for image splicing detection," Proc. - 2009 IEEE Int. Conf. Intell. Comput. Intell. Syst. ICIS 2009, vol. 4, no. 9, pp. 390–394, 2009.

[23] Kanwal,N., Girdhar, A., Kaur, L. et al. (2020)."Digital image splicing detection technique using optimal threshold based local ternary pattern" Multimedia Tool Appl 79, 12829-12846 (2020). https://doiorg/10.1007/s11042-020-08621-2

[24] Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J. F., &Pan, J.-S. (2013). "An efficient scheme for detecting copy move forged image by local binary patterns" Journal of Information Hiding and Multimedia Signal Processing, 4(1), 46–56.

[25] Li, L., Xue, J., Wang, X., &Tian, L. (2013). "A robust approach to detect digital forgeries by exploring correlation patterns" Pattern Analysis and Applications, 18(2), 351– 365.doi:10.1007/s10044-013-0319-9.

[26] Lukas, J., Fridrich, J., & Goljan, M. (2006). "Detecting digital image forgeries using sensor pattern noise" Proceedings of the SPIE, 6072, 60720 Y–60720Y–11.x

[27] M. Hariri and F. Hakimi, (2014) "Image-splicing forgery detection based on improved LBP and Knearest neighbors algorithm," Electronic information and planning, vol. 3, 2015.

[28] M. Hussain, S. Qasen, G. brdis,G. M., H.A.,H. M. (2014). "Evaluation of image forgery detection using multi scale weber local descriptors" International journal on artificial intelligence tools. 24 (4), 1540016, 2015. 23, 2015, doi: 10.1142/01218213015400163.

[29] R. Nosaka, C. H. Suryanto and K. Fukui (2012), "Rotation invariant co-occurrence among adjacent LBPs," in proceedings of the Asian Conference on Computer Vision, Korea, pp.15 -25,2012.

[30] Satpathy, A., Jiang, X., & Eng, H. L. (2014). "LBP-based edge-texture features for object recognition" IEEE Transactions on Image Processing, 23(5), 1953-1964

[31] Shah A, El-Alfy ES (2018) "Image splicing forgery detection using DCT coefficients with multiscale LBP" In: 2018 International Conference on Computing Sciences and Engineering. ICCSE 2018 - Proceedings, pp 1–6,https://doi.org/10.1109/ICCSE1.2018.8374214

[32] Yang, B., & Chen, S. (2013). "A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image" Neurocomputing, 120, 365-379.

[33] Yao H, Wang S, Zhang X, Qin C, Wang J (2017). "Detecting image splicing based on noise level inconsistency" Multimedia Tools App l76 (10):12457–12479. https://doi.org/10.1007/s11042-016-3660-3. 20.

[34] Yuan JH, Zhu HD, Gan Y, Shang L (2014). "Enhanced local ternary pattern for texture classification" In: International conference on intelligent computing. Springer, pp443–448, vow 8588, springer, cham. https://doi.org/10.1007/978-3-319-09333-8_48.

[35] Zhang, Y., Zhao, C., Pi, Y., Li, S., &Wang, S. (2015). "Image-splicing forgery detection based on local binary patterns of DCT coefficients" Security and Communication Networks, 8(14), 2386–2395.doi:10.1002/sec.721.

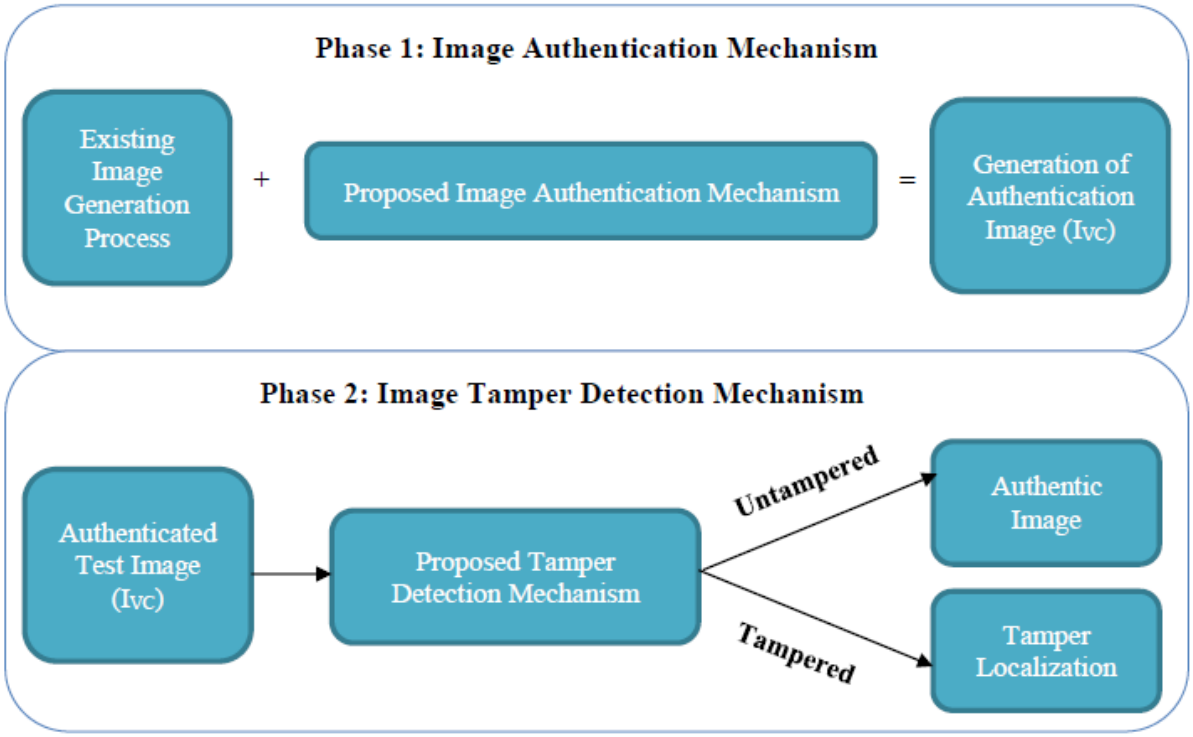

Fig. 5. Proposed Methodology