A Survey On Source Camera Identification Using Image Features

Azhar Ashraf Gadoo[1],Mir Mohammad Yousuf*[2],Mamoon Rashid[3], Shanu Khare[4]
[1,4] Research Scholar , ,Department of Computer Science and Engineering, Lovely Professional University, Phagwara, India
[2,3]Assistant Professor,Department of Computer Science and Engineering, Lovely Professional University, Phagwara, India.

Abstract **-**Since digital camera has become an integral part of our lives in today's world, there is a range of camera on the market that can catch the picture more excellently than technology advancement. This becomes the important part to distinguish the original image with the overwhelming verity of photo splicing. Scientists have taken a considerable approach to defining the image using various parameters and strategies such as Support Vector Machine (SVM) classifier, PRNU comparison, Lens Distortion, (GLCM) Garry-level-co-occurrence matrix, (CFA)color Filter Array and prototype icing tools. Experimental results of these approaches show a good outcome in determining the origin camera of the picture most probably Used for PRNU (Photo response non-uniformity pattern) origin camera recognition.

Keywords: Digital forensics, Image processing, Image complexity Sensor pattern noise.

I. INTRODUCTION

The word forensic comes from the forensic Latin expression, meaning "from or before the forum." The origin of the term comes from Roman times, during the word forensic which a criminal charge meant to present the case in the forum to a jury of public persons. Both the accused person and the accuser will give speeches focused on the story's sides**.** This history is the root of the two traditional forensic uses of the word–as a form of legal proof and as a community display classification. For common usage, the word forensics can be considered correct for favor of forensic science, as the phrase forensic is essentially associated with legal and court-related.[4][6][8][10][17].

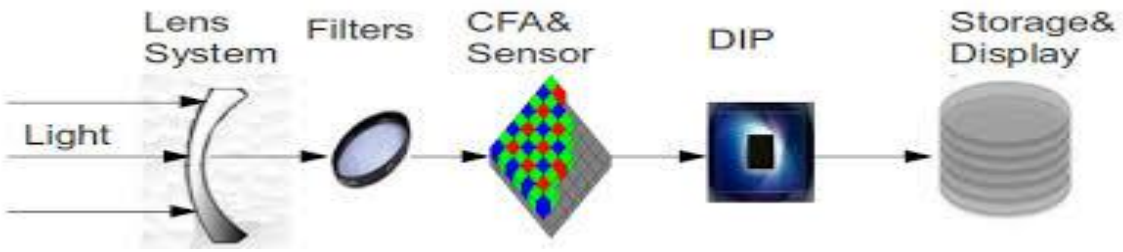

Fig 1. Typical Digital Camera Elements[21].

Digital forensics:

With the development of new technologies, criminals find ways to use these devices to commit crimes. With the proliferation in web technologies, almost all major companies worldwide have a web presence revealing their information to lawful or unauthorized users. Computers have become our life's intrinsic part. Businesses have simplified their activity because of web technologies and products, saving millions of dollars[11][12]. Without these innovations, neither businesses nor customers will survive, it has also become legal evidence in both civil and criminal cases due to the complex role in computer technology in all aspects of our lives. Software proof admitted in court could be any archive or sample retrieved from storage devices such as text, record of viewing, images, photos, and computer files. Such data may be edited or modified. It would require special procedures to recover deleted data.[12][15][16] In a non-destructive manner, computer professionals educated in digital forensics store and obtain evidence. Proof can be retrieved from any storage media mounted in digital devices such as laptops, cameras, PDAs, and cell phones. Any forensic work should be

carried out with caution, including the recording of a valid chain of custody, in order for the facts to be submitted to the court of law. The need to include computer content or traces as part of formal evidence has become inevitable with the proliferation of computers in our daily lives.[1][15] Since the researchers are informatics experts, this paper seeks to provide a concise overview of the system of forensic evidence processing and to examine various methods, techniques and difficulties through forensic analysis and storage.

Digital image forensics:

Digital forensic picture is a word used with slightly different definitions in different contexts. Itis often used as a concept in the academic community to denote the study of an image file's validity,

Fig 2. Digital forensic image authentication.[21]

evaluate the existence of forgeries, [7][4][14][13]and decide the machine that created the image. It is meant in a broader context in the field of law enforcement and forensics and is planned as a full-scale inquiry, both on the validity of the picture and on the evaluation of its substance. It is image study or whether they have been blurred or altered. This is achieved using tools such as Photoshop and other specialized applications. In RGB color space or other color spaces, the software would look for anomalies, look for discrete changes in a color level, determine if pixels were manipulated. It could use analysis of Fourier, de-convolution, or other approaches.

For digital image forensics, the growing Use digital images has created a new issue. These pictures Can be used in court as proof in criminal cases. Digital photos, however, they are easy to manipulate and require a method for verifying the authenticity of the image. Identifying the reference camera is one of the processes. [7][8][9]Nevertheless, using traditional desktop computers takes a long time to complete. We aim to increase the system output by integrating It is available in a distributed computer environment in order to tackle the problem. Conditional use likelihood Characteristics and Hadoop Apache, we test the camera identification process.

Photo response non-uniformity pattern:

The Non-Uniformity Photo Answer pattern for an individual camera can be a means for classification and is often found in video images. [4][5][10][20]The PRNU pattern is therefore also called the camera's fingerprint. This pattern can be extracted and used with a high probability ratio to identify the source camera Due to slight variations in the ability of individual pixels to turn photons into electrons, the PRNU is an non-relational property of all digital imaging sensors [1][2][15][13]This series, which plays the role of a fingerprint sensor, is basically an unintended stochastic watermark that escapes processing, such as loss compression or filtering. Specific forensic procedures were developed as a question of evaluating the two-channel theory tackled using the generic likelihood ratio test.

II. LITERATURE REVIEW

Mehdi Kharrazi[1] As photographic evidence can be proved by two methods according to blonds study, one is conventional and the other is advanced since powerful editing programs replace analog cameras with digital cameras by means of several technologies that are present nowadays, the author also listed one of the "burning in" technology by which skin tones in African-American are darkened in other words The most important issue facing forensic experts is chronological information and efforts to use it as a tool of identification in court. [1][4][7][18]The researcher conducted a survey on two Kodak and Epson camera

models to see the best quality camera that can be further used to check the authenticity of these two models. The Epson offers a software called the Image Authentication System (IAS), which transparently applies an electronic watermark to any device that can read JPEG files to check the photo validity. Also, the code can detect any interference, even if a single pixel has been changed the main difference between the Epson cameras and the Kodak cameras is that the Epson is better suited for checking image authenticity because it has an invisible watermark and can detect a change in one pixel.[2][8] All cameras contribute to the original image non- removable distortion. This could be a big problem in getting the court to agree it watermarked picture is an accurate representation of the original image of the scene. After taking the picture with Kodak technology, the watermark icon can be applied. This has restricted use of forensics. No camera can provide incontrovertible proof of the source of the image or its author. In order to deduce the problem, they proposed a new concept for secure digital camera, taking biometric identification (iris image), a cryptographic Key is used to prove that this camera took the image. It also prevents replacement time, date and other relevant EXIF implant. Implanting is by default a hidden camera and information cannot be modified. They had a program in which they were able to generalize photographers, camera data, etc. hash of image and time, date and other relevant data. They use a lossless fixed algorithm to avoid problems associated with the addition of distortion, and there is also a secret key in the process. Because they are unique to each person and are permanent for these reasons, they are accepted in the U.S. court because they have many identification forms such as (simple keyboard entry pass and thumb recognition of fingerprint iris identification etc.) First iris recognition algorithm was introduced by Dagman in 1994, they worked in iris recognition techniques and unique iris patterns. Irises of identical twins, U.S. mixed eye tickets etc. show the ability of the iris to manipulate light and generally make a pure picture of two irises are not the same due to the similarity between iris patterns. They also showed the advantages and disadvantages of iris identification in the work they further studied and observed the works of Wong celli, M. Sharma and Saber Marvel L.M Hartwig Walton and many others all over discussed lossless watermarking that is invisible digital watermark authentication watermarks implanted by a watermarking chip inside the digital camera (e.g. Epson camera).[5][7][8]

For conclude, they gave a new idea of a safe digital camera that offers a solution for digital image problems that the camera implants in the photographers ' iris image the pieces of scene, object, date, time etc. The method of implantation relies on the secret key camera, the implanted data can be collected to check the image integrity of the watermark. Iris is used as a biometric marker defining the electronic custody chain photographer enabling the investigator to use digital biometric signatures, hardwired camera identification. [15][18][19]It's important because it shows the investigator won't manipulate the evidence at any expense in the investigation. The court acknowledged duplicate copies of computer data indicating that this protected digital camera is a replica of the original data which helps to reduce the mistakes in law enforcement procedures, thus increasing the credibility of digital evidence.

Husrev T Sencur et al[2] In their study, the author's wants to convey about recognizing a camera model when an image is given to it, proposing various features that can be useful throughout blindly identifying the source camera, providing different experiments and correlations between two and five different cameras. In the next section we defined the pipeline structure of digital cameras after the light has reached the lens, multiple filters are used to capture the light and transform it into digital data.[9][13][16][17] After this processing, in which color interpolation is done as gamma color comparison processing, white point correction and compression, these are all stages that vary as the camera's product or value varies from one another. There are several approaches as according to this research one is to identify the features of the camera and also because there is a belief that an image is greatly affected by two features of CFA setup and prototype algorithm and second Color processing / transformation offers 34 features that can support the comparison of RGB camera template pairs(3 features), Neighbor mass delivery center(3 features), RGB pair energy ratio(3 features), wavelet domain statistics(9 features), IQM "Image Quality Metrics"(13 features).[2]

In the first experiment two cameras Sony DSC-P51 and NIKON E2100 with configuration of 2- megapixel

resolution and scale of 1600x1200, they performed two experiments to identify images originating from digital camera.[4][10] The camera settings set the default 150 image data set collected and provided the SVM classifier an accuracy of 98.73 percent. They also noticed that each camera's quantization table was the same even if it did not differ in the same camera design, so they re- compressed the image value array to 75 using JPEG compression. In the second experiment, five camera two are of the above configuration and the remaining models (S100, S110, S200) are canon shot camera and 150 image data set given to the SVM classifier with 88.02 percent accuracy.

Through looking at the simplified, the researchers explored the question of digital camera classification based on features they obtained a satisfactory accuracy in compressed and re- compressed in the same experiment in the case of second experiment, another significant direction of research is to develop features that can increase the accuracy of the classifier.[8].

Lukas et al[3] In their research, the author put forward a method to recognize the camera fingerprint by using the same method to identify the camera brand and model by classifying the image set into different pattern classifiers each class determines the different camera model set. PRNU is an imperfection which comes into contact during camera manufacture, it has a random likelihood and is special to each sensor when the PRNU is measured as a raw sensor output in TIFF or JPEG formats, we call it a sensor fingerprint which carries camera brand and model data. In its pattern identification, the author used various features to identify the camera brand and template from the fingerprint by variance in CFA (color filter array), demos icing algorithm, and the transmission of the sensor signal. The various features used are Statistical Moments Cross-correlation Block covariance Cross-correlation linear pattern.[5][7][9][20].

For this study, 45 images were taken on which all these features were added to the camera brand and the model was extracted from the EXIF image format that the author took only landscape- oriented images at ±90 rpm, the data set was extracted from a web portal "www.flickr.com" and only those camera models were used on which at least 100 different users could be accessed. To train the binary classifiers, the following method was used to train the binary classifiers. First, it randomly selected 70 estimated fingerprints for testing and the left the rest for screening. The features that include measuring PCA are tested on the union of both learning datasets. The major components were extracted separately for each binary classifier. Using that approach, 28 features unique to the binary classifier are collected. They reduced the number of features using the BAHSIC selection method suggested by Song et al to avoid possible overtraining. It allowed them to select different features for different binary classifiers. Eventually, the classification of the SVM classifier with the RBF kernel was used.[2][3][4][18].

The aim in this paper was to identify the camera brand and model originally proposed to identify a specific camera from the fingerprint of the PRNU-based camera. The approach focuses on distinguishing devices with fingerprints. We record 90.8 percent of an average camera product likelihood. The following result was obtained by using a large number of different physical cameras in order to avoid the possibility of over-training in a cluster of cameras.

Zeno J Gerard's[4] This research paper proposed the various methods to identify the images acquired by digital cameras as the methods proposed. Pixel array defects and lens corrections for these flaws, pixel array inconsistencies, file formats used, Watermarking of the camera manufacturer's photos. They used the test band cameras from Sony and the mivica camera. For actual cameras, the first system with CCD defects is investigated and tested.[5][7][19][20] This approach is considered to be used for camera however they have not found the refrence for the other cameras like mivica camera of Sony. In their research they focused on remaining cameras to identify the images acquired by them, they examined different CCD-camera's. The inexpensive cameras were brand trust, and the more costly the cameras were the brand Sony. The pixel defects could be determined in the trust band cameras.in 12 different trust brand cameras, they tested the errors. There were at least 5 pixels with pixel defects in each sensor, and pixel defects in each CCD are found elsewhere. When comparing five images obtained by the same lens, they counted these pixel defects. It seemed to be a Sharp LZ23BP2-chip. The data sheets are available online. Because data sheets also indicated

that defects often depend on temperature, the cameras were cooled down to zero degrees Celsius, and fewer pixel defects tended to appear. It seems that when the temperature rose to 40 degrees Celsius, more pixel defects could be seen. After the snack, The defects of the pixels were visible in the same position. They have used the camera Photo cam camera in which they make the pixel defects visible. However, they could not make the pixel defects visible in Sony cyber shot, Sony mavica and Sony FD83and Sony handycam, However, they also compressed the images but they see position of the pixel doesn't change until 50 percent compression was used. They also used the other methods in which they compare the files to find a serial number in hex headers . .But they couldn't notice any variations for the file headers. They also saw the difference in noise level between two Sony mavica cameras and they didn't see any watermarks in the examined camera. All twelve trust cameras they tested seemed to have visible pixel defects, but in expensive cameras they had fewer errors that were not visible. Nevertheless, it is not noticed that even with the cameras used, if other cameras have the same pixel defects in the same place.[17].

Sevinc Bayram et al[5] The objective is to identify the digital camera used to capture images in this paper. Each digital camera encodes camera model, size, date and compression information in the header of the image so that data cannot be authenticated. In this regard, the source of the blind image authentication technique depends on the validity of the assumption that despite the captured scenes, All images show certain features that are unique to the camera due to its proprietary pipeline of image formation. In previous work, some problems were addressed-defining collection of image features by combining image quality metrics-based features, lower image order statistics, variations in the specified image function. Another approach is made by Lucas et al, in his work, Sensor pattern noise is characterized by denouncing wavelet image.[10][14][19]

Their approach is inspired by Popescu et al's technique, he gave the expectation / maximization algorithm to find out which parts went to recycle two steps — Expectation step helps to present variable to predict unknown parameters — Maximizing step gives new parameters. These two steps had to be repeated continuously until convergence. In a single system, both steps were combined to make them one step. The EM algorithm generates two outputs- One is a two-dimensional data array called the interpolation coefficient of probability map & second estimates.

The classifier used to check the efficacy of the proposed features in their study. Two Sony DSC-P51 & Nikon E-2100 camera models have 2MP resolution. Images were taken with 1600X1200 pixels maximum resolution size, auto focus, no focusing & other default setting. We were taken from the same perspective of the two cameras. 140 Pictures of each prototype lens. For the classification of the unseen 4/5 objects, one fifth used for training & built classifier is used. Experiment with 75x75 pixel image bits. First, for both Sony and Nikon cameras, they extract 3x3 interpolation kernel features. The accuracy is measured at 89.3%. They then extract 4x4 features and increase the accuracy to 92.86% In 5x5 neighborhoods we replicate the same test and the reliability is improved to 95.71 percent. These results show that the interpolation kernel's actual size is not smaller than the size considered to be true. After that, when considering three cameras, they test how the proposed feature works, they also take 140 Canon Powershot S200 images. These images were taken randomly from the internet and consist of various sceneries, and SVM & SFSS is used to classify three cameras and extract features from 5x5 neighborhoods.[2].

Amel TUAMA et al[6] Photo formation involves several phases such as network of lenses, color filter array, processor of image sensors. All of these phases add objects to the quality of the image that provide specific identification process features. Among previous researchers, using these objects to collect these features, Khazari uses 3 sets of features to classify camera template in the machine learning process. He uses 34 features such as color characteristics, image quality, matrix wavelet domain statistics Celiktutan he uses khazari features to identify cell phone camera identification and he uses binary similarity features to get 592 features as well. Filler implements CMI using 28 characteristics related to quantitative motion and linear sequence comparison, Gloe uses Khazari features to shape 82 features with extended textile color. Xu and Shi used the characteristics of 354 local binary patterns. As a set of features, Wahab uses conditional

probability. Use 8x8 DCT transform to classify camera model to get 72 conditional probability. Marra et al collected 338 spam characteristics from rich models based on residual image matrix co-occurrence. Bayram et al implement the CFA interpolation method to remove the color band correlation structure used to identify images.[9][13][18][1].

References are set in their research, references from images are obtained by taking series of images from known camera, and this reference is used to identify whether or not the unknown resource image is captured from the camera. Several images are denoted and combined to obtain the camera's fingerprint, approximately 50 images are taken through which reference point is used to identify the identified camera. The residual image extract features are decomposed into 3 colors. Residual is extracted from the image itself by subtracting the denounced version of image I. Co-occurrence matrix is used to define adjacent data's high-order statistics. Co-occurrence consists of a mutual distribution of likelihood of neighboring residual and horizontally adjacent samples after quantization. Based on linear noise residual patterns, we measure local dependencies & adjacent sample periodicity. The normalized correlation is determined from the 3-color channel noise residual around estimated linear.[8][12][17].

Several experiments on camera models from the Dresden image database are evaluated by different methods. 14 single-device camera models from each model, 200 full-size images are used for each camera. A wavelet denoising filter is used to extract noise residual from all images.

Based on extraction function & machine learning, camera model is defined in order to identify the level they use strong static tool. Three set of features used; using the wavelet denoising filter, noise residual is obtained. Images from 14 camera are used belonging from Dresden database classified by SVM. The experiment shows 98.75% accuracy in the correlation-based method that reached 97.5%.

A large database with multiple devices of the same model will be used in the future work.

Nilambari Kulkarni et al[7] The techniques for image recognition are metadata, lens distortion, picture features, icing demonstrative artifacts and sensor imperfection. They selected sensor imperfection as the SPN extraction method provides the best possible source identification results. In this paper, to identify the source camera, they survey various research papers. We use innovative techniques in their work to remove sensor noise from the "Dresden Image Database" and then use a method called feature extraction to obtain the characteristics In the preprocessing stage a hybrid gradient-based operator & Laplacian operator are used to produce a third image with the edges and noise present in a hybrid system consisting of the best results from the two operators above. For each image plane and extracted edge of the image base, canny masks are applied in pre-processing phase.[7][11][16][20] The edges are removed by using an image noise threshold, and this noisy image is then provided with a GLCM extraction module. Based on the homogeneity, contrast, correlation or entropy, the GLCM is used to extract various functions. Entropically to the enlargement of the image, a high entropy value is a homogeneous scene while a low means inhomogeneous scene, contrasted measures the number of local variations present in the picture, homogeneity implies that the distribution of elements within the GLCM is very similar to the GLCM diagonal. False negative frequency and percentage category and accuracy of detection. The GLCM function removes the sensor pattern noise and is used to match the test set to match it. The hybrid system used to remove noise from the sensor pattern and the GLCM feature performs better. The technology proposed would greatly improve efficiency and identification. The results achieved for the false positive and false negatives rates are 0%, with a maximum value of 15,74%, which has been best achieved in sensor imperfection technology up to now.[6][10][15][19].

For digital image forensics there will be more scope and many more challenges in the future. Videos are more complex than images and many methods for video forensics will be used in future.

Kai Sen Choi et al[8]The writers "Kai Sen Choi, Edmund, Wong" are examining the lens footage left on the photos in this study, which identifies the optical digital image reference camera. The researchers were influenced by the earlier work that used sensor imperfection to detect the source lens. They propose that the lens distortion be used as features on the pictures to identify the source camera. The lens distortion on the images is used for the identification of the source camera and a lens distortion-based classification system

is developed and used to determine how efficient this function is. Two sets of experiments are carried out. In the first set of feasibility trials, [5][9][14][18]lens distortion is used in the object identification and in the second set of experiments, we check that their solution is statistically better than the alternatives by using only an image inquiry.

To check the effectiveness of radial lens distortion in the classification of digital camera images. Two tests were performed. They use 3 different cameras, which are recent models produced by 3 renowned manufacturers in their experiment. Camera C used to generate 2560x1920 images. But the images are non-flash, autofocus, no manual zoom, best JPEG compression performance, and other settings were set to the default values. The first two cameras were used for 1600x1200 photos. After the pictures were captured, for each image the measures proposed were calculated. In the first test, lens distortion in the image classification is used to test the feasibility. Next, all images are given with the lens distortion parameters k1 & k2. The tests and training are conducted using the following SVM classification: 40 photos are selected randomly to train a classifier and then the remaining photos are tested.[4][8][13][17] Both steps, step 1 and step The average classification accuracy is achieved and repeat250 times. The classification rate for camera A is 97.8%; for camera B it is 92%; for camera C it is 84.8%. 91.53% of the average accuracy is achieved. By adding radial distortion to the proposed statics of Kharrazi, they investigate the improvement in precision in comparison with procedures that use only image intensities, their approach improves from 87.38 percent to 91.53 percent, improving accuracy by 4.15 percent.

For future work, it seems that in many different situations this method is still useful, such as pictures taken by SLR camera with a primary lens and images taken by zoom lens without manual zooming.

Zhonghai Deng et al[9] In this article, the company aims to use the auto-white balance method as a new way of identifying the origin lens. Approximating the auto-white balance algorithm inside the camera determines the source camera. This experiment is carried out with a large data set and the proposed method is shown to be very efficient. However, the number of different cameras does not deteriorate the prediction accuracy, which determines this method to be scalable. For the first time, a method of defining an origin camera is based on AWB.[4][7][9][10][11][14] Finally, the proposed method shows that the various devices of the same type or brand can differentiate themselves. Most of the digital camera displays some sort of white balance inside the lens, as if the AWB is still being switched off. The suggested approach is based on an experiment where the vectors follow the radial base function kernel to test the efficiency of its features. Most white balance algorithms have minimal or no effects on the picture when applied to the picture for the second time. In the experiment, they first identify the camera using different brands of the camera. For each camera unit, you only use the first 169 frames, which is the minimum available number of images. You use this file, because each image takes the same lightning picture of the same scene. All pictures used are in JPEG format and select 60% of images as samples by random means and 40% rest for testing. In the first experiment, the average accuracy of cameras from different brands was 99.26%, the lowest at 96.38% and the highest 100%. In this case, Glove et al reported a correct overall performance of 97.79% with a performance of 99.26%. In a second experiment we measure the quality of all 17 Dresden Image models, a camera from various models. The median reliability is 98,61%, which is 96.97% lower and 99.57% higher. In the third experiment cameras of the same model have an average accuracy of 98.57% with the lowest working accuracy of 96.47%, with the highest image randomly selecting 60% to train them. We also track the robustness of their model, with 97.79% average precision with the lowest precision 94.12% and the highest precision 99.41%. From this experiment, they demonstrated that their method is robust to white Gaussian noise and therefore the images taken three years earlier are still classified in the same category as today. We also measure resistance to resize and also play with original images with bi-cubic interpolation at the initial stage. They use features from their re-dimensional pictures when checking. Experiments only show an accuracy of 75,61%, which indicates much more perturbations, but this poor precision can be resolved by using the resized picture for training, with an average accuracy of 98,59%.

Luca Bondi, et al[10] A new approach to solving the camera design recognition problem is employed in this article. They use coevolutionary neural networks to overcome camera design problems. We use a neural network to automatically capture and use SVM to classify these camera-specific objects. They use a well-

known database for more than 13,000 images from 18 camera models[10]. There is no analytical modeling algorithm, because due to simple assumptions or simplified modeling it is less possible for errors.[3][6][8][9][10] The approach can also operate on tiny object patches with 93 per cent accuracy. They conduct several experiments in various operational scenarios during their research. The algorithms compare first and foremost the newest music. They pick two computer-based Chen et al & Marra et al methods.[11][14] Two methods are chosen. With the "The Dresden Ist Dataset" report, the only pictures chosen for a total of 13,000 pictures are JPEG images from versions of a camera system that include more than one example. This photo consists of 74 camera cases with 27 designs. Following that experiment, the overall classification accuracy is 93 percent, and ultimately, for each patch only 128 features created by the overall neural network are under one-tenth compared to 1372 produced by chen et al & under half as opposed to 388 produced by marra et al. In the second phase, it tests the capacity to generalize the proposed neural network, as well as the NVIDIA digits 4.0 system manages the cycle of CNN training with its Caffe 0.15.9 module for deep learning New cameras are considered, and only SVM needs to be retrained.[13][15][17][19][20] I use a data set referred to as 10-model Flickr dataset for this experiment. This dataset was created by gathering 20 photos from different camera models in full resolution, and this data set divides into FT with 10 shots per model & FE with 10 shots remaining. For extraction function, they select CNN models, which have been tested previously during Dresden Image Dataset experiment, and the total accuracy is 93%. This demonstrates that features extracted from a previous Dresden image data set experiment are capable of generalizing unknown camera models. CNN model trained At the end of the day, this confirms that the trained network can be used as other hand-crafted approaches and does not require training from scratch every time.

Table-1: Collate summary list and table of inequalities.

S.no.	Title	Problem Discussed	Techniques used
1.	Method for identification of images acquired with digital camera	Camera identification	Different techniques
2.	Secure digital camera	Digital picture credibility	lossless watermark
3.	Using sensor Pattern noise for camera model identification	camera sensor	PRNU
4.	Mobile camera identification using demos-acing features	Blindly recognize mobile source cameras by combining three types of demo features extracted from the test image.	Demos-acing filter
5.	Source camera identification based on CFA interpolation	increase the process of image acquisition	CFA interpolation
6.	Camera model identification based on machine learning approach with high order statistics features	Used machine learning to classify camera	Machine learning
7.	Source camera identification using GLCM	Targeted at restoring lost	GLCM
8.	Source camera identification Using footprint from lens aberration	Try classifying images that are produced by a	Lens aberration

		limited number of camera types.	
9.	Source camera identification using Auto-white balance approximation	To define the source camera by approximating the camera's AWB algorithm.	AWB algorithm
10.	Frist step towards camera model identification with CNN(convolution neural networks.	To resolve the recognition of image using data driven algorithm.	Machine learning.
11.	Source camera identification using photo response non-uniformity on whatsapp.	Transmit an image from one medium to another to improve image compression when the quality of the image is concerned.	PRNU compare 2.2

III. METHODOLOGY

Different techniques and tools use different parameters to identify the camera, the pixel variance and the sensor of the camera which is unique for every camera during manufacturing and most of the techniques use this sensor noise or imperfection that is printed on the image itself when the photo is captured The main focus of all the techniques is to retrieve the original image and the source camera of that particular image, depends upon the tools accuracy to identify the image and present it before the court of law.

i. **SVM Classifier:** The main objective of each algorithm used is to evaluate the accuracy in obtaining the original image the support vector machine is a class of recognition which categorizes the data by a hyper line, this approach is primarily used as far as supervised learning is concerned, the data set is used to train the system and distinguish the data based on previous training.[2][3][7][14][17].

ii. **PCE Peak to Correlation Energy:** For two distinct stimuli, the peak-to-correlation energy ratio (PCE) is a similarity indicator. PCE is particularly suitable for 2-dimensional camera fingerprints because PCE decreases due to the existence of concealed periodic patterns (a latent origin of false identification). This application requires the use of FFT to easily calculate cross-correlation.[4][6][8][19][11].

iii. **SSIM Structural Similarity Index Matrix:** To calculate the resemblance between two SSIM images, the Structural Resemblance Index SSIM is used. This relies on visible images of artifacts and is a graphical metric which quantifies decrease of image quality that can be due to processing such as data compression or failures in data transmission. Normally, the generated picture is condensed. For example, a reference picture can be retrieved by saving it as a JPEG (at any level of quality) and then reading it back in. In the film business, SSIM is best known, but still has extensive applications in photography.[3][7][9][20].

IV. CONCLUSION:

In this paper The PRNU patterns of the natural objects were linked to the PRNU reference patterns of each camera to classify the source camera by measuring the Peak to Correlation Power. Mostly PCE (peak to comparison energy) is used in literature to evaluate object trends of PRNU- reference and PRNU-patterns under examination. The trouble with PCE is that compression of the image degrades.

V. REFERENCES:

[1]. Blythe, Paul, and Jessica Fridrich. "Secure digital camera." In Digital Forensic Research Workshop, pp. 11-13. 2004.

[2]. Kharrazi, M., Sencar, H.T. and Memon, N., 2004, October. Blind source camera identification. In 2004 International Conference on Image Processing, 2004. ICIP'04. (Vol. 1, pp. 709-712).IEEE.

[3]. Filler, T., Fridrich, J. and Goljan, M., 2008, October. Using sensor pattern noise for camera model identification. In *2008 15th IEEE International Conference on Image Processing* (pp. 1296-1299). IEEE.

[4]. Cao, H. and Kot, A.C., 2010, May. Mobile camera identification using demosaicing features. In *Proceedings of 2010 IEEE International Symposium on Circuits and Systems* (pp. 1683-1686). IEEE.

[5]. Bayram, S., Sencar, H., Memon, N. and Avcibas, I., 2005, September. Source camera identification based on CFA interpolation. In *IEEE International Conference on Image Processing 2005* (Vol. 3, pp. III-69). IEEE.

[6]. Tuama, A., Comby, F. and Chaumont, M., 2016, August. Camera model identification based machine learning approach with high order statistics features. In *2016 24th European Signal Processing Conference (EUSIPCO)* (pp. 1183-1187). IEEE.

[7]. Kulkarni, N. and Mane, V., 2015, June. Source camera identification using GLCM. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1242-1246). IEEE.

[8]. Choi, Kai San, Edmund Y. Lam, and Kenneth KY Wong. "Source camera identification using footprints from lens aberration." Digital photography II. Vol. 6069. 2006

[9]. Deng, Zhonghai, Arjan Gijsenij, and Jingyuan Zhang. "Source camera identification using auto-white balance approximation." *2011 International Conference on Computer Vision*. IEEE, 2011.

[10]. Bondi, L., Baroffio, L., Güera, D., Bestagini, P., Delp, E.J. and Tubaro, S., 2017. First steps toward camera model identification with convolutional neural networks. *IEEE Signal Processing Letters*, *24*(3), pp.259-263.

[11]. Meij, C. and Geradts, Z., 2018. source camera identification using Photo Response Non-Uniformity onWhatsApp. *DigitalInvestigation*, *24*,pp.142-154.

[12]. Lukas, J Fridrich, M Goljan, Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensic Secur. **1**(2), 205–214 (2006)

[13]. Chen, J Fridrich, M Goljan, J Lukáš, in Proc. of SPIE 6515 Electronic Imaging 2007. Source digital camcorder identification using sensor photo response non-uniformity, (2007), pp. 65051–65051. International Society for Optics and Photonics.

[14]. W-H Chuang, H Su, M Wu, in *IEEE International Conference on Image Processing (ICIP)*. Exploring compression effects for improved source camera identification using stronglycompressed video (IEEE, Brussels,2011), pp. 1953–1956.

[15]. Z Wang, AC Bovik, HR Sheikh, EP Simoncelli, Image quality assessment: from error

visibility to structural similarity. IEEE Trans. Image Process.**13**(4), 600–612 (2004).

[16]. M Chen, J Fridrich, M Goljan, J Lukáš, Determining image origin and integrity using sensor

noise. IEEE Trans. Inf. Forensic Secur. **3**(1), 74–90 (2008).

[17]. M. C. Stamm, Min Wu, and K. J. R. Liu, “Information Forensics: An Overview of the First

Decade,” IEEE Access, vol. 1, pp. 167–200, 2013.

[18]. I. Avcibas, M. Kharrazi, N. Memon, B. Sankur, "Image Steganalysis with Binary Similarity Measures," EUROSIP Journal of Applied Signal Processing, 17, 2749-2757, 2005

[19]. F. Mosleh (Kodak), "Cameras in Handsets Evolving from Novelty to DSC Performance, Despite Constraints," Embedded.com, 2008.

[20]. Filler, T., Fridrich, J. and Goljan, M., 2008, October. Using sensor pattern noise for camera model identification. In 2008 15th IEEE International Conference on Image Processing (pp. 1296-1299). IEEE.

[21]. Swaminathan, A., Wu, M. and Liu, K.R., 2007. Nonintrusive component forensics of visual sensors using output images. IEEE Transactions on Information Forensics and Security, 2(1), pp.91-106.