İSTANBUL UNIVERSITY PRESS

Acta Infologica
acin 2023, 7 (2), 348–359
DOI: 10.26650/acin.1282567

Research Article / Araştırma Makalesi

Query by Image Examination: Classification of Digital Image-Based Forensics Using Deep Learning Methods

Görüntü İncelemesine Göre Sorgulama: Dijital Görüntü Tabanlı Adli Görüntülerin Derin Öğrenme Yöntemleri Kullanılarak Sınıflandırılması

İlker Kara[1]

[1](Assist. Prof. Dr.), Cankiri Karatekin University, Eldivan Vocational School of Health Services, Cankiri, Turkiye

Corresponding author : İlker KARA
E-mail : karaikab@gmail.com

ABSTRACT

The continuous increase in the use of information systems and online services has also spurred the forensic examination of digital and image data, which serves as the primary platform for information transfer. In particular, according to the latest reports, the examination of the images obtained from all kinds of recording devices that have the quality of evidence as a result of the forensic case and that can provide the clarification of the incident and the detection of the criminal elements are becoming a critical problem due to the huge amount of data. Our contribution in this study is two-folded. First, we present a new approach that classifies digital images into eight different crime categories using six different models. Second, we have created a new dataset for the classification of crimes and opened it to the public. Throughout the study, we have used our new dataset which has a total of 15,065 image samples from 8 different crime categories including Bet, ChildAbuse, Credit Card and Banking, Drugs, Frightening, Knives, Pornographic and Weapons. In this study, six different models were used to classify crime images. The CNN model was developed by us and five other models used for transfer learning. Pre-trained network model parameters VGG16, VGG19, Xception Model, InceptionResNetV2 and NASNetLarge were used for crime image classification tasks. In addition, the performance of these models is compared using test accuracy and time metrics. Resultly, we achieved prediction accuracy of up to 89.74% using the NASNetLarge model.

Keywords: image processing, deep learning method, image classification, data mining, forensic investigation

ÖZ

Bilgi sistemlerinin ve çevrimiçi hizmetlerin kullanımındaki sonsuz artış, bilgi aktarımı için temel platformlardan biri olan dijital ve görüntü içeren verilerin adli incelemelerini de tetiklemiştir. Adli görüntü inceleme temel olarak bilimsel yöntemlerin ve adli inceleme yazılımlar kullanılarak ilgili görüntüler hakkında delil oluşturulmasını sağlayan bilimsel bir disiplindir. Özellikle, son raporlara göre, adli vaka sonucunda delil niteliği taşıyan ve olayın aydınlanmasını sağlayabilecek her türlü kayıt cihazından elde edilmiş görüntülerin incelenmesi ve suç unsuru olanlarının tespiti artan veri miktarı nedeniyle giderek büyük bir problem haline gelmektedir. Bu çalışmada katkımız iki katkı sunmaktadır. İlk olarak dijital görüntülerin altı farklı model kullanarak sekiz farklı suç kategorisi olarak sınıflandıran yeni bir yaklaşım sunuyor. İkincisi, suçların sınıflandırılması için yeni bir veri kümesinin oluşturarak paylaşıma sunuyor. Çalışma boyunca, Bet, ChildAbuse, kredi kartı ve bankacılık, uyuşturucu, korkutucu, bıçak, pornografik ve silah dâhil olmak üzere 8 farklı suç Kategorisine ait toplam 15.065 görüntü örneğini kapsayan yeni veri setimizi kullanıldı. Suç görüntülerini sınıflandırmak için bu çalışmada 6 farklı model kullanılmıştır. CNN modeli kendimiz ve öğrenmeyi ince ayarlara aktarmak için kullanılan diğer beş model tarafından yaratılmıştır. Görüntü sınıflandırma görevleri için VGG16, VGG19, Xception modeli, InceptionResNetV2 ve NASNetLarge önceden eğitilmiş ağ modeli parametreleri kullanıldı. Ayrıca, bu modellerin performansı test doğruluğu ve zaman ölçümleri kullanılarak karşılaştırılır. Sonuçlar, NASNetLarge modeli kullanarak %89.74'e kadar tahmin doğruluğu elde edilmiştir.

Anahtar Kelimeler: Görüntü işleme, derin öğrenme yöntemi, görüntü sınıflandırması, veri madenciliği, adli inceleme

Submitted : 13.04.2023
Revision Requested : 20.10.2023
Last Revision Received : 14.11.2023
Accepted : 30.11.2023
Published Online : 11.12.2023

1. INTRODUCTION

Data obtained from images represent an effective and natural communication medium in the current age of technology. Unlike the text data, information obtained from the images are helpful in illuminating the forensic cases as the image itself contains evidence for the criminal elements. As such, forensic images are defined as images obtained from any recording device which can provide evidence and therefore enlighten the criminal event. The source of the forensic image, that can be accepted as evidence by the court, can be any kind of recording devices including professional or compact cameras, mobile phones and security cameras (Choodum et al., 2015). The increase in computers and other related computing systems (e.g. mobile devices, IoTs) that we use constantly in our daily lives on the other hand has led to the formation of a large amounts of images (Hafiz et al., 2020). Although the accumulation of image data is helpful in forensic studies, manual analysis of large volumes of digital images is a significantly tedious task. A forensic investigation can take an average of six months with the analysis of more than 300,000 digital images, among which only an average of 100 images are reported to be related to the crime in question (Ferreira et al., 2020). Consequently, using digital imagery as an aid for decision making and as a support for scientific arguments in the forensic investigations is hindered to a great extent. One way to address this issue is to distinguish and classify objects that may be important in the image data, instead of taking into consideration of all the objects available in a given image. The several approaches proposed to determine the authenticity and classification of images and their origins can be classified into two branches, active image forensics and passive image-based forensics. (Birajdar et al., 2013) (See Figure 1).

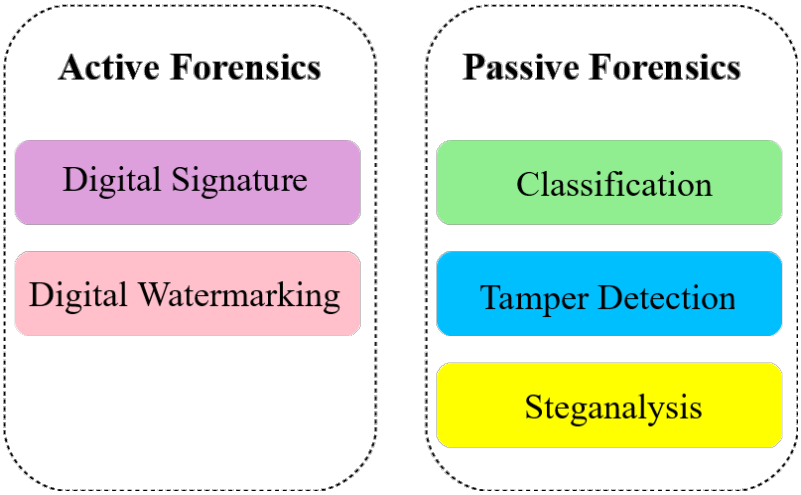

Figure 1. Commonly employed digital image forensics methods in the literature.

Active image forensics require additional priory knowledge of the source of the image. This information requires that the device producing the image contain a digital signature (Birajdar et al., 2013) or a digital watermark (Chandra et al., 2010). Passive image forensics on the other hand is more practical in terms of technology and attempts to determine whether an image is authentic or not based solely on the characteristics of the image without any additional embedded information (Wang et al.,2009). Passive image forensics comes into play once an image has been created and stored in criminal information systems. Depending on the nature of the crime under investigation in digital image forensics, images can be categorized using the passive image forensics approach (Mahalakshmi et al., 2012), image manipulation detection (Thakur et al., 2020), and image source detection (Peng et al., 2013).

Piva, proposed a model for distinguishing and classifying forensic image data and detecting whether the data is manipulated to deceive forensic analysis methods (Piva, 2013). Forensic softwares are needed for the detection and classification of forensic images (Pearson, 2006). Although there are a number of tools designed to classify forensic images, such as Belkasoft (Belkasoft, 2021), X-Ways Forensics (X-Ways Forensics, 2021), most of the time, experts in forensic image analysis experience great difficulties in the examinations made with such forensic software tools due to the irregular and inconsistent data (Cao et al., 2009).

From this perspective, there are several important advantages that serve as a motivating factor for this study in the detection and classification of forensic images. As stated, the differentiation and categorization of forensic image data will offer significant convenience in forensic investigations (Pearson, 2006). Classifying examined digital images based on crime types will also facilitate the detection and identification of evidence. With all this in consideration, we propose

a machine learning-based approach to classify digital images. We employ six different machine learning methods. We propose a robust scheme for classifying eight different crime categories for the samples examined using this approach. To this end, this study mainly presents the three contributions listed below without any commercial concern:

- The method presented in this study concentrates on the categorization of criminal elements in digital images, with a focus on the capture phase.
- We proposed a new dataset of 15,065 items belonging to eight different categories. We also make the proposed dataset publicly accessible for non-commercial purposes (Accessed via link, http://ilkerkara.karatekin.edu.tr/RequestDataset.html).
- We analyzed a new dataset consisting of digital images of different subjects. To be more specific, we have applied six different machine learning methods to classify 15,065 unique 224x224 pixel target images belonging to eight different crime categories, including Illegal Betting, ChildAbuse, Credit Card and Banking, Drugs, Violent, Knives and firearms, Illegal Pornography.

This article is organized as follows: In chapter two, we reviewed several related studies. Chapter three presents the details of the proposed dataset and chapter four presents the applied methods and the experimental results comparing the classification of six unique machine learning algorithms. Chapter five is discussion and chapter six concludes the study and explains possible future directions.

2. RELATED WORK

Due to the increasing amount of forensic evidence in forensic image examinations, the effectiveness of traditional methods is hindered on a high scale. Automated approaches based on machine learning and deep learning models and automatic classification of forensic images are designed to address these problems.

The widely used traditional machine learning models in the classification of forensic evidence include Bayesian algorithms - BayesNet (Grillo et al., 2009; Marturana et al., 2011; Marturana and Tacconi, 2013) and Naïve Bayes (McClelland and Marturana, 2014), Decision Trees (Marturana et al. 2011; Marturana and Tacconi, 2013; Garfinkel et al. 2010), and K-Nearest Neighbor (Gomez, 2012). One of the deep learning models, Convolutional Neural Networks (CNNs) approach is used in forensic image classification. For this purpose, CNN models were created for weapon classification consisting of forensic images (Olmos et al. 2018; Verma and Dhillon, 2017). In the proposed study by Dey et al. a topological signature-based learning scheme was used for the classification of images with an accuracy of 83.2% (Dey et al., 2017). Lin et al used a CNN-based learning method to determine the authenticity of digital images within the scope of forensic analysis (Lin et al., 2018). Similarly, forensic evidence images used the pre-trained Faster R-CNN model approach (Ren et al., 2015).

The study by Karakuş (2018) proposed a model that provides fast and accurate analysis of image data. The proposed model consists of VGG16 network structure and network layers designed for image classification. In the study, a dataset comprising images with a resolution of 300x300 pixels was utilized. Of these images, 2085 were generated using the Kaggle platform, while 915 were obtained from various other sources. The dataset consisted of a total of 3000 image data, with 1500 images depicting guns and 1500 images depicting knives. While 2000 of the images obtained were used for training purposes, 1000 of them were used for verification purposes. An accuracy rate of 97.8% was obtained in the model. (Kara et al., 2018).

Saber et al. (2020), conducted a study on digital image forgery detection and forensic informatics. This study tried to resolve the question of how to ensure the accuracy of images that can serve as evidence in an investigation process. In this study, the advantages and usage areas of existing forensic image technology, comparative studies, the benefits and harms of forgery detection systems including deep learning and convolutional neural networks were examined. These investigations were elucidated within the sections titled "Digital Image Forgery Detection Methods," "Forensic Approaches," and "Comparative Study," bolstered by prior research. It was emphasized that the process was laborious due to the manipulations performed on the image. As a result of the research, it was found that different image processing techniques such as preprocessing, feature extraction, feature selection and classification are also very useful for the precise detection of forgery. Passive methods prove to be highly effective for forgery detection when compared to active approaches. Among these passive methods, copy-move and image fusion are extensively employed by numerous researchers, owing to their benefits of reduced complexity and enhanced accuracy (Saber et al., 2020).

Ferreira et al. (2020), reported that only 148 images containing illegal content (sexual abuse) were found in a database containing more than 300,000 images and 1100 videos. The study focuses on the use of deep learning techniques to identify image manipulation. As a result of the study, it gave satisfactory results in terms of the increase in the time

spent per image and the increase in the margin of error of the analysis due to the manual examination of the images by forensic experts (Ferreira et al., 2020).

Forensics experts develop analysis tools to help them quickly recognize and classify digital images to focus on possible criminal elements in the evidence examined in investigations. In 2012, a commercial analysis tool called ADF Digital Evidence Investigator trained on tensorflow, an artificial intelligence library, to classify digital images especially for crimes of Child Sexual Abuse Material (CSAM) (Adfsolutio, 2021). Since digital image classification is time consuming and ADF tools are often used to quickly qualify exhibits at the crime scene or in the lab, they used a filter (ignoring icons, thumbnails, and other pixel art) and focused only on CSAM crimes classification. Recent developments of new techniques for classification have shown very promising results even in large datasets such as ImageNet (DDS09) (Adfsolutio, 2021).

Alharbi, aims to increase the classification performance of small-sized forensic images in his study (Sharma et al., 2021). For this purpose, the CIFAR-10 dataset containing 60,000, 32x32 color images was used. Principal component analysis (PCA), KNN (K-Nearest Neighbor), and CNN models were used to classify forensic image contents in the study. As a result of the study, the best result was obtained with CNN with a success rate of 74.10%. Although this rate is promising, the margin of error is still too high.

Del Mar-Raave developed a machine learning prototype capable of recognizing weapons in forensic image content (Del Mar-Raave et al., 2021). Given the multitude of weapon types, the dataset used in the study, comprising 608 forensic images, was refined by exclusively selecting realistic photographs of pistols or firearms. In our study, a similar approach was employed by reducing the dataset through the classification of the type of crime committed. Four ImageNet-trained models (InceptionV3, Xception Model, ResNet, and VGG16) were utilized to assess forensic images for weapon identification. Del Mar-Raave et al. achieved the most successful result with the Xception model, attaining an accuracy of 90% in their tests. Despite the promising results, the study's limitation lies in the relatively small dataset used.

It can be concluded that studies on the classification of forensic evidence focus on the creation and optimization of machine learning and deep learning models. Forensic tool development studies for crime categories are rarely used in the classification of forensic evidence. In this study, we have used a similar approach by Del mar, utilizing six distinct machine learning methods to classify 15,065 unique 224x224 pixel target images associated with eight different crime categories.

3. MATERIAL AND METHODS

In this section, we have introduced our approach crime categories, dataset and classification models.

3.1. Dataset

The concept of crime defines the behaviors and actions that are prohibited by the law, defined as crimes by law, and are punished if committed. Combatting crime and delinquency can be assessed in two main facets: the prevention of crime before it occurs and research, detection, and analysis after a crime has taken place. Forensic experts play a crucial role in the latter, elucidating crimes by scrutinizing suspected individuals and providing insights for criminal court decisions. This process depends on the type of the crime that has been committed. However, factors such as the number and the size of the materials examined or the number of qualified specialist personnel are also important. The increasing use of visuals in many applications due to the advances in the technology manifests itself in the human factor in forensic image examinations, revealing the need for expert personnel. To alleviate this problem, tools such as AccessData FTK, EnCase, Belkasoft (McDown et al., 2016) are mainly employed in forensic analysis. Forensic image reviews, inclusive of an analysis of the tools' advantages and disadvantages, are conducted by expert professionals. In principle, although a classification can be made according to file extensions in the examined digital material, they lack the capacity to make decisions regarding content. From this perspective, forensic image analysis offers several important advantages that motivate this study. Automatic classification can be achieved by employing deep learning models that leverage determinative features selected based on crime types discernible in forensic image content. Within this framework, the concept of classifying forensic image content according to specific characteristics during the application phase proves beneficial in terms of alleviating the workload of experts.

The current study focusses on "Illegal Betting, ChildAbuse, Credit Card and Banking, Drugs, Violent, Knives, Firearms, Illegal Pornographic" categories. Illegal Betting, in other words, "Illegal gambling", is any kind of betting action taking place using technology in sports competitions, and is considered to be illegal if a license/permission is not given by the authorities. Criminals create trap virtual environments that harm the economy and affect individuals

socio-psychologically with illegal betting websites that are not subject to taxation. In the European Police Organization (EUROPOL) 2020 Report, it is estimated that the annual cost of illegal sports betting to the world is approximately 1.69 trillion euros (Europol, 2020). The economic loss is seen as a global problem as the illegal betting industry threatens the economy of all countries. Forensic Informatics Specialists usually carry content analysis by focusing on visuals such as coupons, betting odds, promotional advertisements containing sports activities in visual examinations related to this crime.

ChildAbuse, which is an important legal, medical and social problem, is considered as a serious crime in terms of psycho-social and legal aspects due its short and long-term consequences (Kara, 2017). ChildAbuse crime has many dimensions such as physical, emotional, economic or sexual abuse. In the forensic image analysis of child sexual abuse crime, in addition to forensic informatics experts, it is necessary to decide on factors such as the child's age and biological development in the image (Sanap et al., 2015). In addition, accessing content containing child sexual abuse crime has difficulties. Considering this aspect, the study focused on the physical dimension of ChildAbuse crime.

Credit Card and Banking frauds are defined as the crimes of using someone else's bank or credit cards or producing, selling, transferring cards on behalf of someone else illegally. In addition to the availability of developing virtual cards used in online shopping platforms, the number of people who want to take advantage of these cards is substantial on a global scale. In the forensic image analysis carried out on Credit Card and Banking crime, forensic experts generally focus on transactions patterns, transaction documents and banking or credit card images (Wu et al., 2009).

Drugs are habitual or addictive due to their chemical structure; Drugs and stimulants that cause physical, mental, social and judicial problems are seen as a social problem. Criminals are able to supply drugs of many types to almost all social layers of the society by actively using the newly available technological platforms. Forensic experts in forensic analysis of drugs, generally focus on the drug types (cannabis, amphetamines, Ecstasy, heroin, cocaine/crack, stimulants, Ecstasy, sedatives, hallucinogens, opioids, inhalants, and other substances (Isnard et al., 2001).

Violence includes physical or mental suffering, inhumane acts incompatible with human dignity. Intimidation, insults, threats or sexual harassments can be classified as violence. Forensic informatics experts generally focus on the content of images that have been subjected to violence, physically damaged, and whose bodily integrity has been disrupted in forensic image analysis related to violent crime (Del Mar-Raave et al., 2021).

Injury or death as a result of violent attacks are mostly committed with the use of weapons. The concept of a weapon can be defined very broadly to include knives, swords, handguns, rifles, shotguns, machine guns, anti-aircraft missiles, anti-tank missle/rocket launcher, or chemical weapon. The most frequently used weapons in crimes are firearms and knives. Firearms and knives damage the integrity of the body which can result in injury or even death intentionally or unintentionally. For this reason, the study focused on image analysis containing knives and firearms (de Castro et al., 2010).

Illegal pornography, or "Obscenity," refers to publications, images, or other forms of media that serve the purpose of arousing sexual impulses and are contrary to moral values. The characterization of a product as illegal pornographic in investigations is based on the following criteria: i) it dehumanizes sexuality and renders it brutal, and ii) it diminishes the human being to a psychological-impulse-reaction formation, transforming individuals into explicit objects of sexual lust (Seigfried et al., 2008). However, child pornography is evaluated by opening a different heading in terms of psycho-social and legal aspects (Del Mar-Raave et al., 2021). Forensic Informatics Experts focus on the existence of the above-mentioned qualities in the examinations made on pornographic materials and decide whether the content should be regarded as illegal.

3.2. Gathering Digital Data

The importance of a well curated and correct dataset is vital for data-driven studies. As an attempt to build such a suitable dataset, we cooperated with an information security company located in Turkey. The mentioned company possesses a dedicated team and system for gathering a substantial number of forensic digital image samples. They have generously shared authentic forensic digital images with us. There are 15.065 images in the dataset which belong to 8 different crime categories including Illegal betting, Child Abuse, Credit Card and Banking, Drugs, Violent, Knives and firearms, Illegal Pornographic. Images were collected from real forensic cases classified according to the category of the crime. In the context of related crimes, potentially criminal images were identified on a suspicious computer subjected to forensic case analysis. The suspects in these images were made anonymized in the shared dataset, and the images were presented without violating copyright and privacy principles. The images in the dataset were labeled using CVAT (Computer Vision Annotation Tool) within the company and subsequently manually reviewed by the authors to identify and rectify any inconsistent or noisy data (Figure 2). This process is done to increase the success rate for deep learning models. Moreover, the collected data were analyzed and classified by the authors one by one. While labelling

the images, care was taken that the images were taken from real crime scenes. The dataset used in this study is available via the link given in the introduction section. Therefore, another contribution of this study is the newly created dataset for classification of crimes by using images.

Figure 2. The images in the dataset are labeled with all categories using the CVAT tool. a) Illegal Betting, b) Child Abuse, c) Credit Card and Banking, d) Violent, e) Drugs, f) Knives, g) Firearms, h) Illegal Pornographic.

3.3. Classification Models

In order to classify crime images 6 different models used in this study. The CNN model is created by ourselves and the five other models used for transfer learning to fine-tuning. VGG16, VGG19, Xception Model, InceptionResNetV2 and NASNetLarge pre-trained network model parameters are used for image classification tasks. Further, the performance of these models are compared using test accuracy and time metrics.

VGG16 is a convolutional neural network model proposed by K. Simonyan and A. Zisserman (Zhang et al., 2015). VGG16 achieved a 92.7% test accuracy rate in ImageNet. It is an improved version of AlexNet with changing the kernel-size. VGG19 (Simonyan et al., 2015) is also a network trained on ImageNet dataset but the difference between VGG19 and VGG16 is that the former has 19 deep layers whereas the latter employs 16 deep layers. The Xception Model was presented by Francois Chollet in 2017 (Chollet, 2017). Xception Model is an improved version of inception architecture by changing the standard Inception modules into depth wise Separable Convolutions. InceptionResNetV2 (Szegedy et al., 2017) is another convolutional neural network that was trained using the ImageNet dataset. The network contains 164 deep layers and has learned a rich features of a large dataset of images with the input image size of 299x299 for this model. NASNetLarge (Zoph et al., 2018) was also trained by using the ImageNet dataset with the input image size of 331x331.

The NASNetLarge model has the highest accuracy rate. When evaluated according to time and accuracy criteria, the model with the closest accuracy rate to this model is the Inception ResNetV2 model. While the accuracy is 1.4% lower for the Inception model, the NASNetLargemodel is five times more expensive in terms of time. Therefore, for datasets with many images where time is more important, the InceptionResNetV2 model can be used instead of NASNetLarge.

In this study, we fine-tuned these five pre-trained models to train and test our crime image dataset, selecting them based on their highest accuracy rate in "Top-5 Accuracy" (Zoph et al., 2018). Moreover, we have analyzed the effect of deeper networks on image classification tasks.

3.3.1. CNN Algorithm

CNN (Convolutional Neural Network), one of the deep learning algorithms, is a type of artificial neural network. This algorithm, which gives successful results in many areas such as image processing, voice recognition, natural language processing, is especially effective in analyzing and processing visual data.

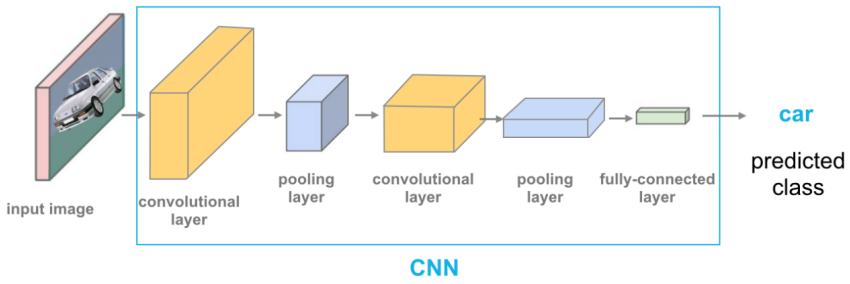

Figure 3. Structure of CNN Algorithm (Paluszek et al., 2020).

3.3.2. VGG16 and VGG19 Models

These models use a multilayer neural network architecture and convolutional neural networks (CNN) for feature extraction. The VGG16 model was developed by the Visual Geometry Group (VGG) at Oxford University. In VGG16, small filters (3x3) are used in the convolution layers. VGG16 consists of 13 convolution layers and 3 fully connected layers. There are 5 max pooling layers with 2x2 dimensions. The last layer is softmax. With the softmax layer, the incoming input data is classified. ReLu is used as the activation function. VGG19 consists of 16 convolution layers and 3 fully connected layers. VGG19, like VGG16, consists of 5 pooling layers and softmax as the last layer. While VGG16 contains 138 million parameters, VGG19 contains approximately 144 million parameters.

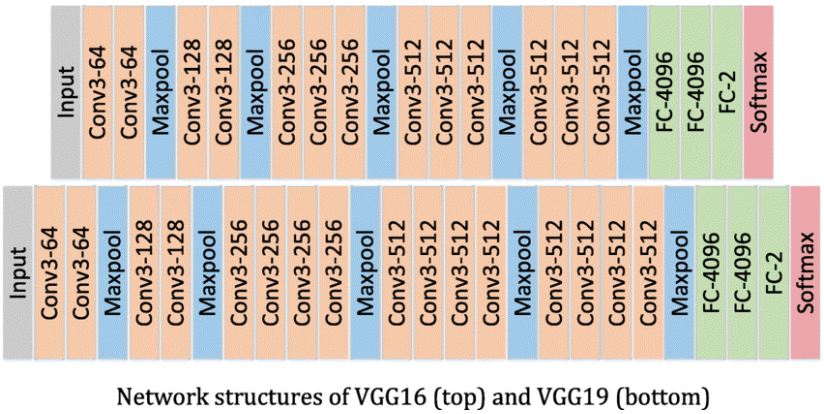

Figure 4. Structure of VGG16 and VGG19 Network Models (Tammina, 2019).

3.3.3. InceptionResNetV2 Model

This model, developed by Google, has a combined architecture between Inception v4 and ResNet. Among the optimisations and innovations made in Deep Networks, the most different one is the ResNet structure where 'residual' connections are made. It has been observed that Inception v4 provides better accuracy but uses fewer parameters. The InceptionResNetV2 model was trained on the ImageNet dataset consisting of more than 5 million images.

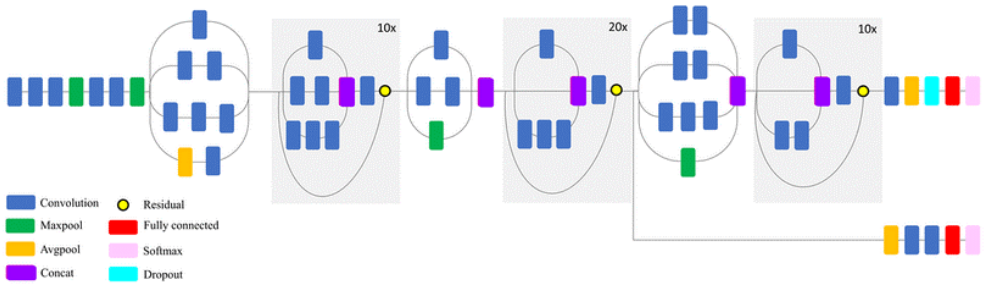

Figure 5. Structure of InceotionResNetV2 Model (Peng et al., 2022).

3.3.4. NASNetLarge Model

This model, developed by Google, is a scalable CNN architecture consisting of basic building blocks (cells) that are fine-tuned through reinforcement learning. It was built using automated machine learning (AutoML). The NASNetLarge model, trained on the ImageNet dataset, exhibits higher accuracy rates compared to other models.

3.3.5. Xception Model

This model, developed by Google, is a hypothesis based on the Inception module, which provides fully decomposable cross-channel and spatial correlations within CNN feature maps. This model is designed to solve the depth problem in convolutional neural network architecture. The Xception model, trained on the ImageNet dataset, demonstrates superior accuracy rates compared to other models.

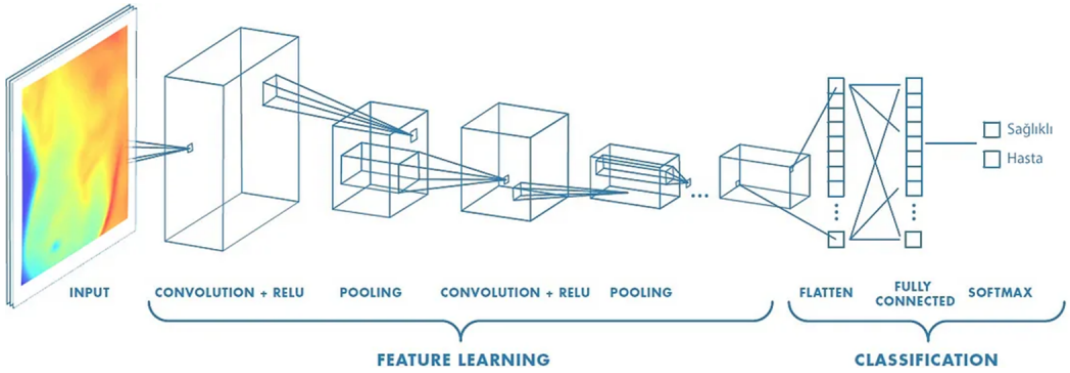

Figure 6. Structure of the Xception Model (Sharma et al., 2018)

4. APPROACH

In this section, the workflow of classification models, phases and conclusion of experiments are presented.

4.1. Workflow

A total of 6 different models, CNN, VGG16, VGG19, Xception Model, InceptionResNetV2 and NASNetLarge, were used on the dataset consisting of Illegal Betting, Child Abuse, Credit Card and Banking, Drugs, Violence, Knives and firearms, Illegal Pornographic images.

The dataset of 15,065 images collected from digital environments through applications such as AccessData FTK, EnCase, Belkasoft was resized to 224x224 resolution. After resizing the images, labelling was performed on the dataset in 8 different categories using the CVAT (Computer Vision Annotation Tool) program. The labelled data were divided into 80% training and 20% testing.

The preprocessed dataset was given as input to the network and 3 dense layers were added to increase the learning capacity of the model. The activation function "softmax", which is used in the last layer of multiclass classifications, and the loss function "categorial_crossentropy", which measures the difference between the actual class labels and the classes predicted by the model, were used as activation functions.

In this research, for all computational works “Python 3.8” is used as the programming language and “Keras library” with “TensorFlow” backend used for Deep Learning algorithms. Additionally, we used “Spyder 4.2.5” on the “Anaconda 2.0.4” platform, meanwhile we used “Lenovo ThinkPad P1 Gen3” with “Intel Core i7-10750H” CPU, “Nvidia Quadro T2000 Max-Q 4GB” and memory of “64 GB DDR4-3200” hardware components. Figure 3 shows the whole steps of the classification process.

4.2. Table of Various Settings

In this study, six different deep learning models are compared to obtain the highest accuracy rate in classifying crime images. CNN, VGG16, VGG19, Xception Model, InceptionResNetV2 and NASNetLarge deep learning models are well known and proven in the literature. Apart from these models, a different CNN model was also used in the project.

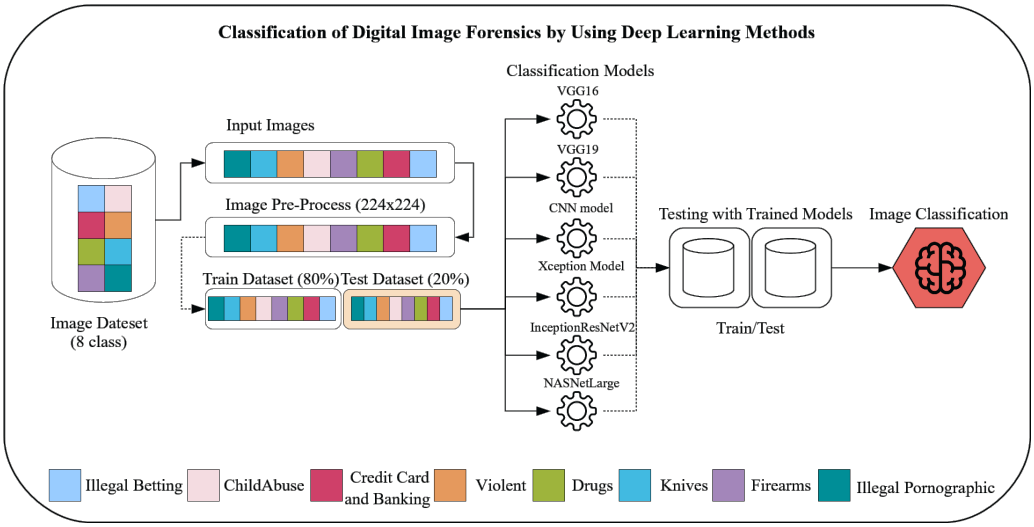

Figure 7. Classification of image dataset.

In the CNN model, it was desired to observe how it would work and result in this study. In this model, which is not expected to give a high accuracy rate, 3 Convolutional layers were applied to emphasize certain features on the pattern and 2 Intensive layers were applied to produce results using features from previous layers. Among the other models used, it gave the lowest result with a running time of 29 minutes and a test accuracy rate of 66.18%. NASNetLarge has the highest result with 91.74% test accuracy rate with pre-trained parameters and 45 minutes running time. When ranking the other models utilized in the project based on the test accuracy rate, VGG19 secured the first position with 81.07%, followed by VGG16 at 83.52%. The Xception Model claimed the third spot with an 88.78% test accuracy rate, while the InceptionResNetV2 model ranked fourth, achieving a test accuracy rate of 90.37%. The accuracy rates and run times of the models tested using 3,013 images and the accuracy rates of the models trained using 12,052 images from the dataset are presented in Table 1.

Table 1. Comparison of deep learning models.

Model	Training Accuracy	Test Accuracy	Time
VGG16	98.73%	83.52%	00:05:15
VGG19	98.12%	81.07%	00:05:16
CNN Model	98.07%	66.18%	00:29:07
Xception Model	97.90%	88.78%	00:22:38
InceptionResNetV2	97.24%	90.37%	00:08:35
NASNetLarge	98.75%	91.74%	00:44:57

5. DISCUSSION

As the number of evidences increase, studies that classify Forensic Images using deep learning methods will benefit experts in forensic investigations in resolving the crimes. The method proposed in this study not only provides an avenue for innovation but also possesses the flexibility to be updated. This adaptability stems from its capacity to extend its application to various crime types, allowing for the integration of different deep learning models tailored for classification.

In addition, through the method proposed, the need for the human factor in the classification of Forensic Images can be reduced, and thus may keep the human errors at a minimum level. It is aimed that the proposed method will help forensic experts by automatically classifying the forensic image analysis process that may contain criminal elements,

just like a smart assistant. In this way, it will contribute to shortening of the decision-making process of the forensic expert by quickly examining the evidence.

Classification of forensic images using the deep learning method also includes complications. Objects defined according to the applicable crime categories may not always contain an element of crime. For example, it would not be healthy to talk about a murder or injury crime in every knife image. Again, the decision on this issue should be up to an expert. The proposed method is not in the position of a decision maker, but in the task of an intelligent assistant that helps the decision maker and accelerates their work. Also, samples such as images obtained from low-resolution security cameras are a major disadvantage for object recognition algorithms. The models trained with low resolution images may not achieve the same rate of success compared to high resolution images. Moreover, no matter how high the resolution is, there is always a margin of error in the algorithms that classify Forensic Images using the deep learnig method.

In this study, we use a new CNN learning-based strategy for classification of criminal elements in digital images within the scope of forensic investigations. Existing experiments demonstrate that digital images do not establish a solid foundation for classification. The rationale behind this argument stems from the capability of digital images in forensic investigations to pinpoint where to focus within images, automatically identifying the most distinctive regions. However, our dataset is limited to 8 crime type classes, and we believe our experimental setup require larger datasets to support this argument more strongly. Another noteworthy consideration is the potential of deep learning methods that can be harnessed for various applications. In conclusion, we believe that the use of modern CNN architecture methods can contribute to the classification of digital images based on feature extraction and capturing of the criminal elements.

6. CONCLUSION

In a forensic case, the abundance of data and documents to be extracted from digital materials naturally impacts the analysis process. Furthermore, the human factor in the analysis process is directly proportional to attention and knowledge, which in turn affects the quality of the analysis conducted. In this context, it can be observed that when data is not examined in depth and the volume of data is massive, these processes become practically impossible.

In this study, we conducted a study to classify and categorize digital images, which are sources of information in forensic investigations, according to eight different crime categories using six different models. In this sense, we propose an approach to classify and categorize digital images in forensic investigations. Experiments based on CNN learning indicate that utilizing criminal elements in forensic investigations is a viable method for classification, particularly based on the capture phase.

In support of this study, we prepared and published a publicly available dataset of our new dataset, which includes a total of 15,065 image samples from eight different crime categories used in the study. We also investigated the effect of various CNN learning-based methods and found that the NASNetLarge model gave the best results.

In conclusion, the proposed approach with an accuracy of 91.74% shows promising results, offering a reasonable detection time of 00:44:57 seconds. We believe that the digital forensics will gain more popularity in the near future due to the increase in digital image cases.

In future work, we plan to explore approaches that have better classification capabilities based on CNN learning and improve accuracy, in which different crimes include detection of different crime categories and possible manipulations.

Another interesting idea we are planning to test is an automated digital image analysis approach, which could allow us to automatically generate image properties of the examined digital forensic images.

Peer Review: Externally peer-reviewed.

Conflict of Interest: The author has no conflict of interest to declare.

Grant Support: The author declared that this study has received no financial support.

ORCID ID of the author / Yazarın ORCID ID'si

İlker Kara 0000-0003-3700-4825

REFERENCES

adfsolutio, nshttps://www.adfsolutions.com/, 2021.

Belkasoft, https://belkasoft.com/, 2021.

Birajdar, G.K., & Mankar, V.H. (2013). Digital image forgery detection using passive techniques: *A survey. Digital investigation*, 10(3), 226-245.

Cao, H., & Kot, A.C. 2009. Accurate detection of demosaicing regularity for digital image forensics. IEEE Transactions on Information Forensics and Security, 4(4), 899-910.

Chandra, M., Pandey, S., Chaudhary, R. (2010). Digital watermarking technique for protecting digital images. *In 2010 3rd International Conference on Computer Science and Information Technology* 7, 226-233. IEEE.

Choodum, A., Boonsamran, P., NicDaeid, N., Wongniramaikul, W. (2015). On-site semi-quantitative analysis for ammonium nitrate detection using digital image colourimetry. *Science & Justice*, 55(6), 437-445.

Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1251-1258).

Coulibaly, S., Kamsu-Foguem, B., Kamissoko, D., Traore, D. (2019). Deep neural networks with transfer learning in millet crop images. *Computers in Industry*, 108, 115-120.

Europol, (2020). How Are Organised Crime Groups Involved in Sports Corruption?. https://www.europol.europa.eu/newsroom/news/how-areorganised-crime-groups-involved-in-sports-corruption.

de Castro Polastro, M., da Silva Eleuterio, P.M. (2010). Nudetective: A forensic tool to help combat child pornography through automatic nudity detection. *In 2010 Workshops on Database and Expert Systems Applications*, 349-353. IEEE.

Del Mar-Raave, J. R., Bahşi, H., Mršić, L., Hausknecht, K. 2021. A machine learning-based forensic tool for image classification-A design science approach. Forensic Science International: Digital Investigation, 38, 301265.

Dey, T., Mandal, S., Varcho, W. (2017). Improved image classification using topological persistence. *In Proceedings of the conference on Vision, Modeling and Visualization*, 161-168).

Ferreira, W.D., Ferreira, C.B., da Cruz Júnior, G., Soares, F. (2020). A review of digital image forensics. *Computers & Electrical Engineering*, 85, 106685.

Hafiz, R., Haque, M. R., Rakshit, A., Uddin, M. S. (2020). Image-based soft drink type classification and dietary assessment system using deep convolutional neural network with transfer learning. *Journal of King Saud University-Computer and Information Sciences*. 34(5), 1775-1784.

Garfinkel, S.L., Parker-Wood, A., Huynh, D., Migletz, J. (2010). An automated solution to the multiuser carved data ascription problem. *IEEE Transactions on Information Forensics and Security*, 5(4), 868-882.

Grillo, A., Lentini, A., Me, G., Ottoni, M. (2009). Fast user classifying to establish forensic analysis priorities. *In 2009 Fifth International Conference on IT Security Incident Management and IT Forensics*, 69-77. IEEE.

Gomez, L. S. M. (2012). Triage in-Lab: case backlog reduction with forensic digital profiling. *In Proceedings of the Argentine Conference on Informatics and Argentine Symposium on Computing and Law*, 217-225.

Isnard, A., Council, T. C. (2001). Can surveillance cameras be successful in preventing crime and controlling anti-social behaviours. In Character, Impact and Prevention of Crime in Regional Australia Conference.

Kara, I. (2017). A Review About Child Abuse Crimes Committed Through Internet In Turkey. *Int J Forensic Sci Pathol*, 5(3), 337-340.

Karakuş, S., Kaya, Ö. Ü., Ertam, Ö. Ü. F., Talu, M. F. (2018). *Derin Öğrenme Yöntemlerinin Kullanılarak Dijital Deliller Üzerinde Adli Bilişim İncelemesi*.

Keras, https://keras.io/api/applications/, 2021.

Kuhle, L.F., Oezdemir, U., Beier, K.M. (2021). Child Sexual Abuse and the Use of Child Sexual Abuse Images. In Pedophilia, Hebephilia and Sexual Offending against Children (pp. 15-25). Springer, Cham.

Lin, X., Li, J.H., Wang, S.L., Cheng, F., Huang, X.S. (2018). Recent advances in passive digital image security forensics: A brief review. Engineering, 4(1), 29-39.

Mahalakshmi, S.D., Vijayalakshmi, K., Priyadharsini, S. (2012). Digital image forgery detection and estimation by exploring basic image manipulations. *Digital Investigation*, 8(3-4), 215-225.

Marturana, F., Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, 10(2), 193-204.

Marturana, F., Me, G., Berte, R., Tacconi, S. (2011). A quantitative approach to triaging in mobile forensics. *In 2011IEEE 10th International Conference on Trust, Sec* urity and Privacy in Computing and Communications (pp. 582-588). IEEE.

McClelland, D., Marturana, F. (2014). A Digital Forensics Triage methodology based on feature manipulation techniques. *In 2014 IEEE International Conference on Communications Workshops* (ICC) (pp. 676-681). IEEE.

McDown, R.J., Varol, C., Carvajal, L., Chen, L. (2016). In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes. *Journal Of Forensic Sciences*, 61, S110-S116.

M Kirchner& R. Böhme (2007). Tamper hiding: Defeating image forensics In International Workshop on Information Hiding, Springer, Berlin, Heidelberg. (2007), pp.326-341.

Olmos, R., Tabik, S., Herrera, F. (2018). Automatic handgun detection alarm in videos using deep learning. *Neurocomputing*, 275, 66-72.

Paluszek, M., & Thomas, S. (2020). Practical Matlab deep learning. A Project-Based Approach, Michael Paluszek and Stephanie Thomas.

Pearson, H. (2006). Forensic software traces tweaks to images. *Nature*, 439(7076), 520-522.

Peng, F., Liu, J., Long, M. (2013). Identification of natural images and computer generated graphics based on hybrid features. *In Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security* (pp. 18-34). IGI Global.

Peng, C., Liu, Y., Yuan, X., & Chen, Q. (2022). Research of image recognition method based on enhanced inception-ResNet-V2. *Multimedia Tools and Applications*, 81(24), 34345-34365.

Piva, A. (2013). An overview on image forensics. International Scholarly Research Notices, 2013.

Rahimzadeh, M., Parvin, S., Safi, E., Mohammadi, M.R. (2021). Wise-SrNet: A Novel Architecture for Enhancing Image Classification by Learning Spatial Resolution of Feature Maps. arXiv preprint arXiv:2104.12294.

Ren, S., He, K., Girshick, R., Sun, J. (2015). Faster r-cnn: Towards real-time object detection with region proposal networks. *Advances in neural information processing systems*, 28, 91-99.

Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Fei-Fei, L. (2015). Imagenet large scale visual recognition challenge. *International Journal of Computer Vision*, 115(3), 211-252.

Saber, A. H., Khan, M. A., & Mejbel, B. G. (2020). A survey on image forgery detection using different forensic approaches. *Advances in Science, Technology and Engineering Systems Journal*, 5(3), 361-370.

Sharma, M., & Vig, L. (2018). Automatic classification of low-resolution chromosomal images. *In Proceedings of the European Conference on Computer Vision (ECCV) Workshops* (pp. 0-0).

Sanap, V.K., & Mane, V. (2015). Comparative study and simulation of digital forensic tools. *Int J Comput Appl*, 975, 8887.

Seigfried, K.C., Lovely, R.W., Rogers, M.K. (2008). Self-Reported Online Child Pornography Behavior: A Psychological Analysis. *International Journal of Cyber Criminology*, 2(1).

Sharma, A., Singh, A., Choudhury, T., Sarkar, T. (2021). Image Classification using ImageNet Classifiers in Environments with Limited Data.

Simonyan, K., Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.

Szegedy, C., Ioffe, S., Vanhoucke, V., & Alemi, A.A. (2017). Inception-v4, inception-resnet and the impact of residual connections on learning. In Thirty-first AAAI conference on artificial intelligence.

Tammina, S. (2019). Transfer learning using vgg-16 with deep convolutional neural network for classifying images. *International Journal of Scientific and Research Publications (IJSRP)*, 9(10), 143-150.

Thakur, R., Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Science International*, 312, 110311.

Verma, G.K., Dhillon, A. (2017). A handheld gun detection using faster r-cnn deep learning. *In Proceedings of the 7th International Conference on Computer and Communication Technology* (pp. 84-88).

x-ways, https://www.x-ways.net/, 2021.

Wu, L.T., Parrott, A.C., Ringwalt, C L., Yang, C., Blazer, D.G. (2009). The variety of ecstasy/MDMA users: results from the National Epidemiologic Survey on alcohol and related conditions. *The American Journal on Addictions*, 18(6), 452-461.

Zhang, X., Zou, J., He, K., Sun, J. (2015). Accelerating very deep convolutional networks for classification and detection. *IEEE transactions on pattern analysis and machine intelligence*, 38(10), 1943-1955.

Zoph, B., Vasudevan, V., Shlens, J., Le, Q.V. (2018). Learning transferable architectures for scalable image recognition. *In Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 8697-8710).

Wang, W., Dong, J., Tan, T. (2009). A survey of passive image tampering detection. *In International Workshop on Digital Watermarking* (pp. 308-322). Springer, Berlin, Heidelberg.

Dateset, https://ilkerkara.karatekin.edu.tr/RequestDataset.htmlekle dataset, 2021.

How cite this article

Kara, I. (2023). Query by image examination: classification of digital image-based forensics using deep learning methods. *Acta Infologica, 7*(2), 348-359. https://doi.org/10.26650/acin.1282567