

## Review on effectiveness of deep learning approach in digital forensics

Sonali Ekhande<sup>1,2</sup>, Uttam Patil<sup>1</sup>, Kshama Vishwanath Kulhalli<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Jain College of Engineering, Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>Department of Computer Science and Engineering, D. Y. Patil College of Engineering, Shivaji University, Kolhapur, India

### Article Info

#### Article history:

Received Jul 14, 2021

Revised Mar 9, 2022

Accepted Apr 7, 2022

#### Keywords:

Convolutional neural networks

Cybercrime

Cyber forensic

Deep learning

Digital forensic

### ABSTRACT

Cyber forensics is use of scientific methods for definite description of cybercrime activities. It deals with collecting, processing and interpreting digital evidence for cybercrime analysis. Cyber forensic analysis plays very important role in criminal investigations. Although lot of research has been done in cyber forensics, it is still expected to face new challenges in near future. Analysis of digital media specifically photographic images, audio and video recordings are very crucial in forensics This paper specifically focus on digital forensics. There are several methods for digital forensic analysis. Currently deep learning (DL), mainly convolutional neural network (CNN) has proved very promising in classification of digital images and sound analysis techniques. This paper presents a compendious study of recent research and methods in forensic areas based on CNN, with a view to guide the researchers working in this area. We first, defined and explained preliminary models of DL. In the next section, out of several DL models we have focused on CNN and its usage in areas of digital forensic. Finally, conclusion and future work are discussed. The review shows that CNN has proved good in most of the forensic domains and still promise to be better.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Sonali Ekhande

Department of Computer Science and Engineering, Jain College of Engineering, Visvesvaraya Technological University

Hanchetti, Belagavi, India

Email: sonalisurve2007@gmail.com

## 1. INTRODUCTION

Cyber forensic also known as computer forensics is technique for investigation and analysis of digital evidences. The evidence from a particular computing device is collected and preserved in such a way that it is suitable for inclusion in crime investigation and could be presented in a court of law. Cyber forensics is very important in law enforcement community due to number of reasons, one of them is fast growth in computers and internet technology. Cyber criminals use advance tools for various forbidden activities like email scams, distribution of copyrighted works without permission, cyber terrorism, financial fraud, cyber extortion and lot. There has been continuous increase in cybercrimes and white-collar crimes as they are non-violent, give high profits, have low risk of imprisonment, and even if caught and found guilty, it usually results in relatively short prison. In accordance with industrial revolution 4.0, communication between digital devices like cyber physical systems, mobile, internet of things (IoT), storage and network devices has increased the number of cybercrimes [1]. With advancements and increase in cybercrimes, there has always been a need of improved forensic analysis techniques. As per the survey performed by Al Fahdi *et al.* [2] on practitioners and scholars, it was found that anti-forensic, encryption-decryption and cloud computing, are

the top problems that need to be solved for practitioners. For researchers, however, the top priority potential problems were social networking and tool capability along with cloud computing. Future studies must therefore be centered in evolving effective approaches for addressing these issues along with creating a rigorous testing framework to proactively establish forensic-based solutions before they are recognized as problems by practitioners. Forensic capabilities should exist at the beginning of a new technology rather than years after the technology has been introduced and probably misused. Sub disciplines of cyber forensics.

Cyber forensics is a continuously evolving scientific field with many sub-disciplines [3] like:

- Computer forensics: Evidences found on computers and other media are identified, preserved, collected and analyzed for investigations and legal proceedings. In order to clarify the state of digital objects in information systems and electronic documents, it uses elements of law and computer science to apply various phases of digital forensics to computer resources [4].
- Network forensics: In this area, different network activities are monitored, captured, stored and analyzed for finding source of security attacks, intrusion detection, unusual network traffic and security breaches. Network forensics analysis software can support multiple tasks, such as network security investigation, checking integrity of data coming from various sources, possible attack prediction, network traffic analysis, and recording different types of user tool-based traffic analysis. The network forensics division faces a number of issues, like challenges related to data and traffic, network speed, storage capacity, data integrity, data privacy and data extraction. Several frameworks to tackle these problems have been proposed like distributed network frameworks, dynamic network forensics framework, soft computing-based network forensic frameworks and graphic based network forensics frameworks [5].
- Mobile device forensics: It is study of acquisition and analysis of evidences from mobile phones and subscriber identity module cards (SIM cards). Smartphones have a variety of features that allow users to perform almost any activity, such as online banking, photo sharing, from private use to business. In order to help the forensic investigator to identify the person, observe their recent activities, smartphones offer useful information such as recent chats, call logs, location details, and images. Several mobile forensic systems have been proposed, such as the system proposed by Benkhelifa *et al.* [6], and Petraityte *et al.* [7], with the goal of helping forensic investigators examine potential breach scenarios with the minimum time spent.
- Digital image forensics: It deals with the verification of digital photographic image authenticity and integrity. Using advanced devices such as smartphones or digital reflex cameras, anyone can capture digital photographs. Photo editing tools are used to improve them and then upload to social network sites. However, this development in technology is a double-edged sword. Forged images are becoming increasingly common and we can definitely argue that seeing is no longer believing, especially with the use of techniques such as artificial intelligence (AI) and generative adversarial networks (GAN) that can be used to spread false news [8]. Digital image forensics deals with the extraction and verification of the integrity of image metadata.
- Multimedia forensics: In the last couple of years, multimedia forensics has become very relevant in investigations. Two main areas that are focused in multimedia forensics are, first, source identification that deals with finding the source digital devices (cameras, cell phones, and camcorders) using the media they create, and forgery detection which aims to detect signs of tampering by testing the legitimacy of the digital media (audio clips, video clips, and images). It tests, by analyzing and evaluating, whether sound and video recordings are original or manipulated.

Along with these areas recent trends in digital forensics includes cloud forensics, social media forensics, and IoT forensics [9]. These systems are highly complex, carries large amount of data, face challenges of integrity, validity and accuracy of data and thus had caused major threat to its large-scale use. Although cyber forensic spans above mentioned disciplines, we have specifically focused on digital forensic. This paper explores ever increasing area of digital forensics, broadly categorized as biometrics, image forensic, multimedia forensic (audio and video), surveillance (physical security system) and information forensic (steganalysis) as shown in Figure 1. Also, apart from different machine learning methods used in digital forensic, we have focused our study on deep learning (DL), more specifically on convolutional neural network (CNN), as it has proved excellent in most of the digital forensic issues. This paper aims to provide reviewed study of recent work carried out in above mentioned areas and covers the work which have outperformed as compared to previous methods.

The review paper is organized; section 2 provides a brief study of DL and its architecture. Section 3 gives detailed study of application of CNN, its variants in the areas of digital forensics i.e., biometrics, image forensic, multimedia forensic (audio and video), surveillance (physical security system) and information forensic (steganalysis). Conclusion and future work are discussed in section 4. The review is based on study of recent and prominent research publications in these areas, although there is lot to make a note of.

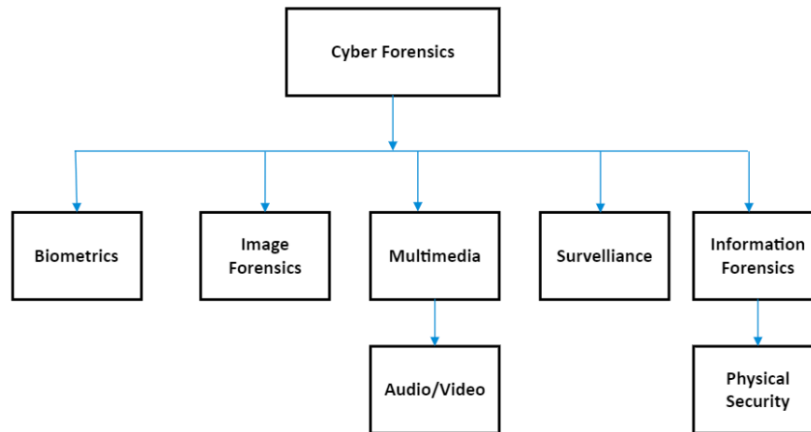


Figure 1. Categories of cyber forensic applications

## 2. DEEP LEARNING

DL as opposed to a task-specific algorithm is a type of machine learning method that learns the representation of data. There are three classes of deep learning i.e., supervised learning, unsupervised learning, and semi-supervised learning. DL computational model has multiple processing layers and abstraction at each layer [10]. DL architectures are multilayer networks where nonlinear function of lower-level features are used to obtain abstract features. Some of the most popular DL models are CNN, recurrent neural networks (RNN), and deep belief network (DBN). DL models have played very significant role in bioinformatics, speech recognition, image identification and natural language processing. Deep learning architecture like CNN, RNN, DBN have produced comparatively good results than human experts in the areas like computer vision, natural language processing (NLP), biometrics, speech recognition, and audio and video recognition. DL structure has number of layers, where each level learns its input data and transforms it to more complex representation at upper layer. The more the number of layers, deeper is the network. There are four fundamental architectures of deep learning as stated: unsupervised pre-trained network, CNN, RNN, and recursive neural network.

### 2.1. Deep learning architecture

Recently deep learning techniques are considered as state-of-the-art method by the researchers for detecting various forgeries. Following subsection covers some DL architectures that are popular among researcher due to its incomparable accuracy in modelling and classifying the data. This includes generative adversarial networks, deep belief network, recurrent neural network and convolutional neural network.

#### 2.1.1. Generative adversarial networks

Generative adversarial networks (GANs) use adversarial process to estimate generative models. It is an unsupervised learning task that automatically discovers and learns the regularities or patterns in input data. It uses two models, namely generator G and discriminator D. Generator G's function is to learn the real data distribution and generate new examples, while discriminator D calculates whether the data is real data coming from domain or it is fake data generated by the generator. The participants attempt to strengthen their methods till the distribution of data and model are similar. This attempts to find Nash equilibrium that compromise between the two participants [11]. It is possible to train the adversarial net using back propagation algorithm. GAN optimization is a minimal problem where G's training technique is to increase the possibility of D producing an error [12].

#### 2.1.2. Deep belief network

Deep belief network (DBN) is a probabilistic generative model that has multiple layers of latent variables. DBN finds a joint probability distribution of output data and labels. The common issues of deep-layered neural networks, viz. requirement of labeled training data set, long time for learning, and inadequate techniques to select the appropriate parameters, are addressed by DBN. In DBN, several restricted Boltzmann machines (RBM) are stacked on one another. RBM [13] captures high-order correlations within visible units. Contrastive divergence (CD) algorithm which is unsupervised greedy layer algorithm is used to pretrain DBN. RBM in the stack is trained by using feature representation output from previous layer. The DBN is first pretrained and then it is fine-tuned using back propagation of error derivatives.

### 2.1.3. Recurrent neural network

Today, RNNs are widely used in natural language processing tasks [14]. The output of RNN from previous step is taken as an input to next step. RNN as the name suggest, performs same task recurrently for every sequence element. RNN has a memory to store previously-calculated information. Let the number of words in a sentence be  $m$ , the probability of observing the sentence is obtained by computing the product of probabilities of each word,  $w_i$ , and its preceding word [15]. If we unroll the network, a single layer for each word is created. i.e., if we have a word sequence of length  $n$ , then the network will contain  $n$ -layer NN. Using the current sequence of words and predicted probabilities, RNN can sample the next possible word.

### 2.1.4. Convolutional neural network

DL algorithm are recognized for solving image recognition problems. CNN process the input in 3D having width, height, and depth. The 3D input at each layer of CNN is transformed to a 3D output of neuron activations [16]. The structure of CNN is composed of three layers, an input layer, an output layer, and multiple hidden layers as depicted in Figure 2. Raw pixel values are fed to the input layer. Hidden layer consists of convolutional layers, pooling layers, and fully connected layer. Convolution layer has several feature maps. Each feature map is obtained by convolving small region of input data with filters or kernels. Next is pooling layer which is also called as subsampling layer. Pooling reduces the number of parameters and training complexity. Sampling is performed along with width and height. The features obtained are robust against noise and distortion. Last layer is fully connected layer and their activations are determined by matrix multiplication and bias offset [17].

Figure 2 demonstrates an overall CNN architecture with one convolutional layer, one pooling layer, and one completely linked layer for the classification. The output is a set of extracted features. Activation function is used to increase the nonlinear properties of the decision function and network without affecting the convolutional layer's receptive field. The size of the output volume depends on three hyperparameters, namely depth, stride, and zero-padding. In these hyperparameters, depth is the number of the filters. Stride is used to slide the filter by one or more than one position. Stride reduces the dimension and produce smaller output. Zeros are added around the border of the input volume by using zero padding. In this paper, we have specifically focused on study of CNN in digital forensics due to following reasons: i) they are very well suited when working with images like object recognition and image classifications; ii) they are good in identification of visual data such as faces, peoples, street signs, and platypuses; iii) CNNs are useful in text analysis; and iv) they are also good at analyzing sound. Digital forensics mainly deals with image, sound and text analysis and CNN has proved to be good candidate in dealing with these issues. In the next section we will, in detail cover application of CNN in all subdisciplines of digital forensics.

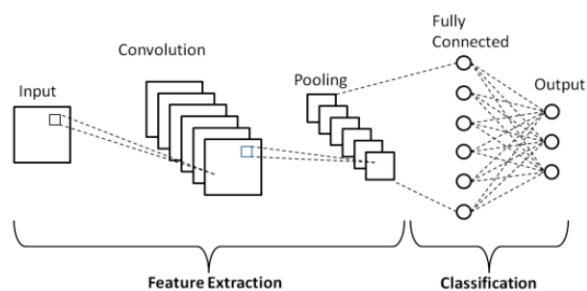


Figure 2. CNN architecture

## 3. CNN IN DIGITAL FORENSIC AREA

Among all other DL techniques, CNN is recognized as a promising performer in solving detection and classification problems for various digital forgeries. This section will study the efficacy of CNN in different digital forensic areas viz biometrics, image forensics, multimedia forensics, physical security system and steganalysis. Characteristics of CNN architectures, database, and results of areas under study are summarized in the form of table for better understanding.

### 3.1. Biometrics

With increase in criminal activities, efficient and accurate identification have become a primary need for forensic applications. Usually, manual identification approach is used in forensic science. But recent development in computational intelligence equipped biometric technology had replaced manual identification

process. Biometrics is among one of the essential verification mechanisms. It identifies people on the basis of their behavioral and physiological features. These features are easily apparent in different forensic identification areas, i.e., fingerprint, voice, iris, face, and handwriting. General recognition process of biometrics includes feature extraction, feature robustness and feature matching. Effectiveness of biometrics system lies in its recognition process i.e. how accurately it can identify an individual. Biometrics authentication is a form of identification and access control [18]. It is used for identifying peoples in a group who are under surveillance. However, there are two issues related with it: first, biometric recognition systems are incredibly complex, and second, biometric recognition requires inherently probabilistic effort. Hence even though the systems are working as designed, there still exist uncertainty and risk of error. Nevertheless, it is found that these systems may perhaps, get tricked or spoofed. Lot of work has been done for spoofing detection. Recent available solution for spoofing detection often depends on domain knowledge, precise biometric reading system and attack types. This subsection focuses on three subareas of biometrics spoofing specifically face spoofing, periocular recognition and contactless fingerprint identification.

The attack on biometric systems can be divided into two groups: direct attack which considers the possibility to generate synthetic biometric samples and indirect attack which consist of seven attacks and requires knowledge about the system. Literature review on earlier anti spoofing related work on iris discovered use of image quality metrics features, different texture patterns, bags of visual words and noise artifacts from recapturing process. Face spoofing was detected through texture patterns (e.g., LBP-like detectors), acquisition telltales (noise), and image quality metrics. Also, the results were varied according to data sets. For fingerprints most of the groups approach the problem with hard-coded features like quality metrics related to the modality that includes ridge strength and directionality, use of general texture patterns in local binary pattern (LBP), multi-scale block local ternary patterns (MBLTP) and local phase quantization (LPQ) methods, and filter learning using natural image statistic [19], [20]. However, some limitation of previous work was, varying results from dataset to dataset, feature extraction dependencies on input type, and requirement of prior knowledge about acquisition level biometric spoofing. With advancements in CNN, recent research in biometrics is focused around CNN based techniques. It is found that spoofing in different biometric modalities can be detected using CNN even when very limited knowledge about spoofing is available. Menotti *et al.* [20] used two general-purpose approaches to build image-based anti-spoofing systems with convolutional networks for several attack types in three biometric modalities, namely iris, face, and fingerprint. The first technique is hyperparameter optimization of network architectures called architecture optimization (AO), while the second one i.e filter optimization (FO) that learns filter weights using back-propagation algorithm. Results obtained were better in eight out of the nine benchmark cases (except biosec). Print attacks are the attacks, in which security of iris recognition system is threatened through use various techniques like printing of iris photographs, use of contact lenses to present to the sensors. These attacks were identified through applying CNN right after iris segmentation and normalization stages of common iris recognition pipeline. The trained model takes eye region and normalized iris images as the input and makes the decision about possible spoofing attack by a single frame. The method showed high efficiency in detection of different kinds of iris spoofing attacks as compared with the literature before.

Next biometric area that was reviewed is periocular recognition. It is biometric identification approach particularly suitable for less constrained environment where face or iris recognition is not appropriate. An attention-based CNN architecture assumes that information within eye region and eyebrow region are significant to periocular recognition, and hence it ought to be more noticed during feature learning and matching. According to the literature survey, earlier methods concentrated on cross-spectrum periocular matching using neural network techniques and exploited periocular image. Dense scale invariant feature transform (DSIFT) characteristics, followed by k-means clustering for dictionary learning and representation, but it was more expensive computationally. A model called the periocular probabilistic deformation model (PPDM) was proposed by Smereka *et al.* [21] in 2015, which provided a sound model for possible deformation between periocular images. For matching periocular pairs, inference of the captured deformation is used using the correlation filter. The selection of discriminatory patch regions for more responsible matching has further strengthened this. These results give promising performance on multiple datasets. But were less resistant to scale variation or misalignment which happened during real deployment. Zhao and Kumar [22] proposed an attention-based CNN architecture for accurate feature learning of periocular region. Fully convolutional network (FCN)-peri and AttNet are attention-based CNN architectures that can specifically detect eyebrow region and eye region as key region of interest (RoI) and makes use of this RoI Information for additional discriminative feature learning. It is found that approach of CNN had considerably outperformed in close and open world verification problem with respect to the previous state of art methods.

Another area which is comprised in biometrics is fingerprint identification. Along with contact-based fingerprint identification, contactless fingerprints identification has become a need due to advances in sensors. Contactless 2D fingerprint technologies are used to overcome the limitations of contact-based fingerprint. Contactless fingerprints give deformation free acquisition of fingerprint features and are more

hygienic. Billions of fingerprint data in legacy database are contact based fingerprints. Hence, there is need for method that will accurately compare contactless 2D fingerprint images with contact-based fingerprint images. Recent method consists of CNN based framework which is used to match contact based and contact less fingerprint images features like fingerprint minutiae, particular ridge map and specific region of ridge map is used to train multi-Siamese CNN [23]. Deep fingerprint representation is generated using distance aware loss functions. This framework had achieved outperforming results, in matching of contact based to contactless fingerprints, as compared to other methods in the literature.

### 3.2. Image forensics

With advent in social networks, digital visual media has become a primary way of communication. However, its content and originality could be easily counterfeited. Hence, the reliability of digital visual information is under question. Digital image forensic [24] is a research area that tries to authenticate the image by recuperating information about their history, identifying imaging device that is used to capture the image and detecting traces of forgery. There has been continues growth in image forensic community since last two decades, to solve problems like splicing detection, copy move detection, source identification and lot.

Image splicing aims at tampering the image by changing the content of original image. In this, a selected region from another image is inserted into original image by using advance image editing tools. Earlier work for tampering detection focused on use of shallow radial basis function (RBF) network to classify high order statistical features. Rota *et al.* [25] used a DL approach based on CNN for blind classification of forged and original images using patch-based processing. Visual geometry group (VGG) like CNN architecture learns invisible discriminative artifacts from tampered images. Along with detecting forged images, it also localizes tampered region within the images. Results on CASIA TIDE v2 dataset proved better than other methods however the learned model cannot be generalized and gives better result on specific dataset.

Another method used in cut and paste forgery detection is median filtering (MF). MF technique has been very effective in image anti forensics and image editing [26]. Current forensic algorithms detect the features manually, feature extraction and classification are separate and optimized separately, but a median filtering detection technique based on CNN can directly learn the features from the image. The first layer of CNN consists of several filters, with its input as an image and output its median filtering residual (MFR). This method shows high detection rate in cut and paste forgery detection [27]. Discovering the processing history and checking the authenticity are very important in multimedia forensics investigations. There are several forensic algorithms that can successfully detect image manipulations. But this process is time consuming. Also, there was a need for building general purpose forensic algorithm that can detect different image manipulations. Earlier research in multimedia forensic used steganalysis tools with feature extractors like spatial rich model (SRM) and subtractive pixel adjacent matrix (SPAM). However problems were faced like how to design low level feature extractors?; is it possible to directly learn image tampering features?; are there any ways to obtain high level features from low level traces?. Unlike CNN which learns features that are representative of image content, a new layer called constrained convolutional layer adaptively learns manipulation detection features while suppressing image content features. Use of constrained layer in CNN can detect multiples of image editing operations with almost 100% accuracy. Also, it can accurately detect image manipulations where image captured from source camera model used in training data, does not match with source of test image under investigation [28]. Another aspect of image forensic is to distinguish between natural and computer-generated images (CG) images or videos. To distinguish between them, there exist two research directions, first one is subjective which involves psychophysical experiments, and second is objective method which is based on the statistical properties of the two classes. Objective method follows pipeline structure of machine learning, which consists of phases like complicated, discriminative, hand-crafted features designing and training classifiers like support vector machine (SVM), ensembles. This strategy performs well in relatively simple datasets but it often exhibits limited performance in complex datasets containing images of heterogeneous origins [29]. CNN can be used effectively to differentiate between natural photographic images and CG. It uses local to global strategy where it trains small patches from CG images and use simple majority voting rule for classification of entire image. This CNN had fixed depth, a stable structure and good forensic performance. It outperforms existing methods, for images of heterogeneous origin and has good robustness against resizing and JPEG compression [30].

### 3.3. Multimedia forensics

Multimedia forensics deals with scientific analysis of multimedia signals i.e., audio, video and images to recover probable evidences from them. It tries to find history of the digital content by recognizing acquisition device that is used to produce the data. It also performs validation of integrity and captured information from multimedia signals [31]. This sub-section concentrates on audio and video forensic.

With advancements in multimedia software's, video editing has become easier and accessible to anyone. But blind detection of traces left by video processing operation are still at their initial stage. Some of the approaches used by the researchers were video device identification [32], local tampering detection and localization [33], [34], physical inconsistencies detection and computer-generated video identification, video recapture understanding [35], frame addition and removal analysis [36], detection of temporal interpolation [37], fake bit rate detection [38], video codec identification [39], and multiple compression detection [40]. Despite of these many solutions, it was found that accuracy decreases on strong video compression. Because of this side effect, many forensic traces are removed by the encoding operations and forensic analysis is affected. In video temporal splicing, when different videos are temporally concatenated, it is likely that the original videos were encoded with different codecs or qualities. These video codec traces can be captured through CNN. Two different CNN are trained to extract characteristics of the used video codec and used coding quality [41]. Inconsistencies in CNN-extracted feature in the time domain are used to detect temporal splicing. This system has very well detected and localized temporal splicing for video sequences where two different video sequences are concatenated to generate a new one.

Another important area in criminology and forensics is identification of audio recording devices. Audio recording devices are checked to decide whether a certain record is from a proper device and is valid. It plays important role in copyright disputes. However, with advancement in technology, audios are tempered smartly and thus have increased difficulty and complexity of the identification. The results of CNN with noise as the intrinsic features [42] proved that when feature vector is obtained from noise generated by each device and then recognizing it with DL techniques had given good performance in audio identification.

### 3.4. Physical security system

The main purpose of physical security system is to protect targets of interest. It aims on keeping careful watch to identify possible danger or difficulties. It requires long hours of vigilance and thus forms limiting factor when assessed by human components. Effectiveness of these systems is limited because humans lose their vigilance while manning security systems. Second factor in vigilance reduction is false alarm rate which is alarm for non-threat conditions. Hence for an ideal physical security system, there is need of processing layer which will eliminate this nuisance alarm from the information before presenting it to an operator. This section, will explain video surveillance of physical security systems.

Review of state of art work in physical security assessment revealed that transfer learning has been widely used and has improved the accuracy over previous methods. In transfer learning, already known knowledge is extracted and is applied to new domain. If transfer learning is used on CNN, it is found that training time is significantly reduced as well as accuracy of detecting physical security related target is also high [43]. A more ideal physical security system would have a processing layer that eliminates the majority of nuisance alarms prior to presenting the information to an operator. In CNN based approach, construction of background scene is independent of temporal data. Instead, concerned target are able to halt their motions for an indefinite period and yet, are detected. Deep CNN through transfer learning is also implemented for image detection and classification problems in X-ray baggage security imagery [44]. In this pre-trained CNN is later on optimized as a secondary process. This has overcome the issue of restricted availability of object of interest with respect to previous work based on the bag of visual words model (BoVW) and techniques such as sparse representations.

### 3.5. Steganalysis

Since few years, Information hiding has been a hot research area. It is widely used in military and intelligence agencies, law enforcement and counterintelligence. Lot of research has been done on steganography which is used to establish secret channel between two parties. The goal of steganography is to insert within an innocent looking cover medium (image, audio, and video) a message so that visual inspection of the resulting medium will not disclose the presence of message. Steganalysis is the discovery of the existence of hidden information. The goal of steganalysis algorithms is to detect stego image from clean image. Currently the best image steganalyzers are feature-based steganalyzers specifically using [45] and machine learning techniques. They share the same pipeline namely, noise residuals computation, feature extraction and binary classification. However, this pipeline can be alternately implemented by a deep CNN that learns the optimized deep hierarchical representations for image steganalysis. CNN can extract complex statistical dependencies from high-dimensional inputs and learn deep representations from intermediate concepts. CNN based steganalysis model for spatial domain steganography [46] having high pass filters, two convolutional layer and two fully connected layers gives quite promising results over other methods. In [47] a new framework based on transfer learning is proposed for steganalysis. The learning of features within CNN is improved by using following strategy, first a CNN model is retrained with training set consisting, stego images of high payload and cover images, and then the obtained feature representations are transferred to normalize the model by detecting stego images with low payload. Another approach is the use of deep

residual network [48] for steganalysis. It is claimed to give better performance than the classical rich model technique. In this, basic high pass filter sets of, which are used in calculations of residual maps, are applied to first layer of CNN and truncated linear unit is used as activation function. This gives better classification accuracy for a low SNR. The overall study can be summarized as in Table 1.

Table 1. Characteristics of CNN Architectures, database and results of areas under study

Area of Study	Applications	Architecture	Database	Result
Biometrics	Iris, face and fingerprint spoofing detection [20]	Spoofnet (3-layer architecture): i) two convolution layers with four stages that convolves with bank of filters, activation function is rectified linear activation, spatial pooling and local normalization and ii) dense layer is followed by SoftMax classifier.	Warsaw, Biosec, MobBIOfake (IRIS) Replyattack (Face) Biometrika, Crossmatch (Fingerprint)	Accuracy: Iris-99.84% Face-98.75% Fingerprint-96.50%
	AttNet Architecture: i) It has 4 convolution units. Each unit has 2 convolution layer, ReLu activation function and Max pooling. Unit 2 and 4 captures information from RoI and ii) Fully connected layer of size 64.	UBiPr, FRGC, FOCS, CASIA.v4-dist, UBIRIS.V2, VISOB	False accept rate EER-2.26 (UBiPr), 8.59 (FRGC) 7.69 (FOCS) 4.9 (CASIA)	AttNet Architecture: i) it has 4 convolution units. Each unit has 2 convolution layer, ReLu activation function and Max pooling. Unit 2 and 4 captures information from RoI and ii) Fully connected layer of size 64.
	Sub-Net architecture: i) four convolution layers with Max pooling in first 3 layers. Concat layer is introduced after 1 <sup>st</sup> layer and ii) fully connected dense layer.	Ubc Patch, AT&T Face dataset, Feret dataset, PolyU	FP Rate at 95% Recall: -8.04% (Distance-Aware loss) 12.34%	Sub-Net architecture: i) four convolution layers with Max pooling in first 3 layers. Concat layer is introduced after 1 <sup>st</sup> layer and ii) fully connected dense layer.
Image Forensics	Image forensic analysis [25]	VGG like CNN architecture: i) two convolution blocks. Each block has two convolution layers with ReLu activation, pooling layer and Dropout layer and ii) two fully connected layer.	CASIA TIDE V2.0	Accuracy: 97.44% (Original) 68.11 (QF=90) 69.29 (QF=80)
	Image manipulation detection [28]	MISLNet architecture 4 different conceptual blocks. First block has only constrained convolution layer. Second block has three convolution layers followed by batch normalization, activation function and pooling layers. Third block has 1x1 convolution layer. Fourth block has two FC layer and SoftMax classifier.	IEEE IFS-TC Forensic challenge dataset	Identification rate: 99.58% for Median filtering 99.74% for Gaussian Blurring 99.82% for additive voice gaussian noise (AVGN)
Multimedia Forensic	Median filtering Forensic [27]	i) First layer is filter layer to obtain MFR of image, ii) 5 convolution layers with ReLu activation and pooling (Max/Average), and iii) two fully connected layers followed by SoftMax classifier.	BOSSbase1.01, UCID, BOSS RAW, Dresden Image, NRCS	Detection Accuracy: 85.14%(JPEG_70) 94.04%(JPEG_90)
	Distinguish between natural and CG images [30]	Network has ConvFilter layer, three convolution groups, two FC Layer and SoftMax layer. Convolution layer has Batch Normalization, Max pooling and ReLU activation.	PRCG Database, Colombia Photographic images	Classification Accuracy: 98.50% (PRCG)
	Video codec forensic [41]	i) It is 12 layers architecture having 10 convolution layers with stride 1 <sup>st</sup> , 3 <sup>rd</sup> , 6 <sup>th</sup> and 9 <sup>th</sup> layer is followed by SELU activation function and ii) 11 <sup>th</sup> layer is Fully connected layer (FC) followed by SELU activation and 12 <sup>th</sup> layer is FC Layer followed by SoftMax activation.	Video sequences were taken from <a href="https://media.xiph.org/video/derf/">https://media.xiph.org/video/derf/</a> [49]	Perfect detection rate: 0.520 for quality-based feature 0.736 for codec-based CNN 0.856 for combined
Physical Security System	Audio recording device identification [50]	i) Background noise extraction using wavelets, ii) hidden layer having multilayer perceptron (MLP), and iii) SoftMax regression.	Segments from audio files from 9 devices	Detection accuracy is Approx. 92%
	Physical security assessment [43]	It used transfer learning taking AlexNet, GoogleNet and SVM with quadratic kernel as pre trained models.	ImageNet Database	Accuracy: AlexNet 100% GoogleNet 99.5% SVM 76%
Steganalysis	Object detection within X-Ray Baggage [44]	It used CNN Configuration of AlexNet. Parameters of network were fine-tuned using transfer learning through layer freezing. Features of last fully connected layer were used to train SVM	Dbp2, Dbp6, FFOB, FPOB	Accuracy: 96%
	Deep learning hierarchical representation for image steganalysis [46]	It has 10 layers. First layer has 30 filters with values initialized from SRM. Eight convolution layers has activation function ReLU except truncated linear unit (TLU) is used in first layer. Average pooling is used.	BOSSBase, BOWS2	Error rate for 0.5 bpp WOW (9.06) S-UNIWARD (10.0) HILL (13.05)
	Learning and transferring representation for image steganalysis using CNN [47]	It has one preprocessing layer Five convolution layers with Gaussian activation function and average pooling and two completely connected layer followed by SoftMax.	BOSSBase	Error rate for 0.4 bpp WOW (21.95) S-UNIWARD (22.05)
	Steganalysis via deep residual network [48]	It has 3 sub networks: i) HPF sub network extract noise residual from input images; ii) deep residual learning sub network has pre-processing layer consisting of a convolution layer with 64 convolution filters, a batch normalization layer, a ReLU activation layer and a maximum pooling layer. Residual learning layer, and iii) Fully connected layer.	BOSSBase	Detection Error Rate HUGO-BD 4.1% WOW 4.3% S-UNIWARD 6.3% HILL 10.4% MiPOD 4.9%



#### 4. DISCUSSION AND FUTURE WORK

Through the study of most recent researches in cyber forensics, it could be derived that deep learning (DL); specifically, CNN had outperformed in most of state of art methods in forensic analysis. To demonstrate this, we would like to discuss our work. Our work is in the area of universal steganalysis for Jpeg images. We performed experiments on BOSSbase and ALASKA database containing clean and steganographed images using Steghide, JpHide&Seek, JMipod, JUNIWARD steganographic algorithms. The experiments were performed on two classification algorithms. First, we used SVM. In this approach, a statistical model of first and higher-order magnitude statistics were extracted from multiscale, multi-orientation wavelet decomposed image, next feature selection strategy like analysis of variance (ANOVA) was used to obtain relevant features for training. Data was trained on nonlinear SVM with RBF kernel. The trained model was tested and the result shows average accuracy of 78.33% on validation set [51] and secondly, in our ongoing work, we are using CNN with transfer learning on EfficientnetB4. Our model consists of using average pooling layer, rectified linear unit (ReLU) activation function and dropout layer. So far obtained result shows accuracy of 89.8% on validation set, which may further improve on finetuning the model. From the above result, we can say that CNN had outperformed SVM in terms of accuracy and complexity. Also, we need not have to concentrate on handcrafted feature extraction as required in SVM.

However, some of the key points and questions that are observed during study are: Is more data leads more accuracy? In DL, more the number of samples, more well-trained is the network. However, architecture optimization is able to learn meaningful features from small sample size. Also, use of other biometric modalities could be considered for better identification.

Which features CNN should learn? Concentrating on rate-of-injection (ROI) information, CNN was able to learn more discriminative feature and results in improved performance also; it is observed that network which is enforced to learn dissimilar features is able to give excellent results as in splicing detection. Hence, we can say that proper selection of filter and number of layers in CNN may lead to proper feature representation.

Fine tuning of convolutional neural network (CNN): In image manipulation detection, use of constrained convolutional layer had forced CNN to learn content-independent image manipulation forensic features and is able to identify several types of image tampering. Fine tuning of pre-trained CNN along with understanding about what a CNN has learned had improved the performance in differentiating natural images and computer-generated images.

Use of transfer learning: transfer learning takes pre-trained CNN which is trained on dataset that lies outside to its feature space and then it fine tunes the network by using smaller dataset within its feature space. In physical security system and steganalysis, transfer learning had significantly reduced training time and improved detection accuracy and had achieved better performance than classical methods.

However, we also found certain gaps during the study: i) although, deep learning has outperformed, its robustness is not studied. General users have no idea of how these deep neural network (DNN) models used in forensic tools are trained, implemented and how reliable are they, ii) most of the work done is specific to the training dataset. It is necessary to generalize it on real time input, and iii) characteristics of DNN based model possess some questions like is the architecture, weights, and implementation of the model open and reproducible? Does the data set have enough representation of all classes? Is the training set poisoned? Does the training set have inherited bias? Are the real error rates model experiences close to development process estimate? Does the error rate increase over time? How much stable outputs are when the training set changes? Is model resistant to information leak and fair w.r.t. predictions? These question needs to be answered while designing the application [31]. Hence, there is need of framework which test the security and robustness of these forensic tools. With these points in view, the future work could be concentrated on: i) developing generalized forensic tool for detecting different forensic problems with good accuracy and ii) method for checking whether these forensic tools are secure and robust itself.

#### 5. CONCLUSION

In this paper, we first had, defined and explained preliminary models of DL. Next cyber forensic problems are categorized as per their applications and domain as biometric, image forensic, multimedia forensic, surveillance and information forensic. Out of several deep learning models, we have specifically focused on CNN and its usage in areas of digital forensic in detail. We have discussed key points about variants of CNN, gaps observed and future work. The review shows that CNN has proved good in most of the forensic domains and still promise to be better. However, it is found that deep networks exhibit vulnerability and are prone to attack, hence there is need of framework that would test robustness of forensic tools.




## REFERENCES

- [1] K. S. Singh, A. Irfan, and N. Dayal, "Cyber forensics and comparative analysis of digital forensic investigation frameworks," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, Nov. 2019, pp. 584–590, doi: 10.1109/ISCON47742.2019.9036214.
- [2] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," in *2013 Information Security for South Africa*, Aug. 2013, pp. 1–8, doi: 10.1109/ISSA.2013.6641058.
- [3] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, 2019, doi: 10.14569/IJACSA.2019.0100880.
- [4] A. Al-Dhaqin *et al.*, "CDBFIP: common database forensic investigation processes for internet of things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017, doi: 10.1109/ACCESS.2017.2762693.
- [5] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: a survey," in *2016 Cybersecurity and Cyberforensics Conference (CCC)*, Aug. 2016, pp. 28–34, doi: 10.1109/CCC.2016.22.
- [6] E. Benkhelifa, B. E. Thomas, L. Tawalbeh, and Y. Jararweh, "Framework for mobile devices analysis," *Procedia Computer Science*, vol. 83, pp. 1188–1193, Jan. 2016, doi: 10.1016/j.procs.2016.04.246.
- [7] M. Petraityte, A. Dehghantanha, and G. Epiphaniou, "Mobile phone forensics: an investigative framework based on user impulsivity and secure collaboration errors," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Elsevier, 2017, pp. 79–89.
- [8] P. Yang, D. Baracchi, R. Ni, Y. Zhao, F. Argenti, and A. Piva, "A survey of deep learning-based source image forensics," *Journal of Imaging*, vol. 6, no. 3, Mar. 2020, doi: 10.3390/jimaging6030009.
- [9] D. P. Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *Advances in Intelligent Systems and Computing*, 2019, vol. 815, pp. 701–708, doi: 10.1007/978-981-13-1580-0\_67.
- [10] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the ACM Conference on Computer and Communications Security*, Oct. 2015, vol. 2015, pp. 1310–1321, doi: 10.1145/2810103.2813687.
- [11] K. Wang, C. Gou, Y. Duan, Y. Lin, X. Zheng, and F.-Y. Wang, "Generative adversarial networks: introduction and outlook," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 4, pp. 588–598, Oct. 2017, doi: 10.1109/JAS.2017.7510583.
- [12] E. Martin and C. Cundy, "Parallelizing linear recurrent neural nets over sequence length," *ICLR 2018 Conference*, 2018.
- [13] P. Canuma, "What are RBMs, deep belief networks and why are they important to deep learning?," *The Startup*. 2020, Accessed: Jan. 08, 2022. [Online]. Available: <https://medium.com/swlh/what-are-rbms-deep-belief-networks-and-why-are-they-important-to-deep-learning-491c7de8937a>.
- [14] H. Shao, H. Jiang, X. Li, and T. Liang, "Rolling bearing fault detection using continuous deep belief network with locally linear embedding," *Computers in Industry*, vol. 96, pp. 27–39, Apr. 2018, doi: 10.1016/j.compind.2018.01.005.
- [15] J. Nabi, "Recurrent neural networks (RNNs)," *Towards Data Science*. 2019, Accessed: Jan. 08, 2022. [Online]. Available: <https://towardsdatascience.com/recurrent-neural-networks-rnns-3f06d7653a85>.
- [16] S. Mahdaviifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, Jun. 2019, doi: 10.1016/j.neucom.2019.02.056.
- [17] S. Hijazi, R. Kumar, and C. Rowen, "Using convolutional neural networks for image recognition," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8925, pp. 572–578, 2015.
- [18] M. Saini and A. K. Kapoor, "Biometrics in forensic identification: applications and challenges," *Journal of Forensic Medicine*, vol. 1, no. 2, pp. 1–6, 2016, doi: 10.4172/2472-1026.1000108.
- [19] D. Yadav, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, and K. W. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 851–862, May 2014, doi: 10.1109/TIFS.2014.2313025.
- [20] D. Menotti *et al.*, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 864–879, Apr. 2015, doi: 10.1109/TIFS.2015.2398817.
- [21] J. M. Smereka, V. N. Boddeti, and B. V. K. V. Kumar, "Probabilistic deformation models for challenging periocular image verification," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1875–1890, Sep. 2015, doi: 10.1109/TIFS.2015.2434271.
- [22] Z. Zhao and A. Kumar, "Improving periocular recognition by explicit attention to critical regions in deep neural network," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 2937–2952, Dec. 2018, doi: 10.1109/TIFS.2018.2833018.
- [23] C. Lin and A. Kumar, "A CNN-based framework for comparison of contactless to contact-based fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 662–676, Mar. 2019, doi: 10.1109/TIFS.2018.2854765.
- [24] W. Lu, W. Sun, J.-W. Huang, and H.-T. Lu, "Digital image forensics using statistical features and neural network classifier," in *2008 International Conference on Machine Learning and Cybernetics*, Jul. 2008, vol. 5, pp. 2831–2834, doi: 10.1109/ICMLC.2008.4620890.
- [25] P. Rota, E. Sangineto, V. Conotter, and C. Pramerdorfer, "Bad teacher or unruly student: can deep learning say something in image forensics analysis?," in *2016 23rd International Conference on Pattern Recognition (ICPR)*, Dec. 2016, pp. 2503–2508, doi: 10.1109/ICPR.2016.7900012.
- [26] H.-D. Yuan, "Blind forensics of median filtering in digital images," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1335–1345, Dec. 2011, doi: 10.1109/TIFS.2011.2161761.
- [27] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1849–1853, Nov. 2015, doi: 10.1109/LSP.2015.2438008.
- [28] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: a new approach towards general purpose image manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, doi: 10.1109/TIFS.2018.2825953.
- [29] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, Jun. 2016, pp. 5–10, doi: 10.1145/2909827.2930786.
- [30] W. Quan, K. Wang, D.-M. Yan, and X. Zhang, "Distinguishing between natural and computer-generated images using convolutional neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2772–2787, Nov. 2018, doi: 10.1109/TIFS.2018.2834147.





- [31] A. K., S. Grzonkowski, and N. A. Lekhac, "Enabling trust in deep learning models: a digital forensics case study," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 1250–1255, doi: 10.1109/TrustCom/BigDataSE.2018.00172.
- [32] S. Bayram, H. T. Sencar, and N. Memon, "Video copy detection based on source device characteristics: A complementary approach to content-based methods," in *Proceedings of the 1st International ACM Conference on Multimedia Information Retrieval, MIR2008, Co-located with the 2008 ACM International Conference on Multimedia, MM'08*, 2008, no. May 2014, pp. 435–442, doi: 10.1145/1460096.1460167.
- [33] L. D'Amiano, D. Cozzolino, G. Poggi, and L. Verdoliva, "Video forgery detection and localization based on 3D patchmatch," in *2015 IEEE International Conference on Multimedia and Expo Workshops (ICMEW)*, Jun. 2015, pp. 1–6, doi: 10.1109/ICMEW.2015.7169805.
- [34] D. D'Avino, D. Cozzolino, G. Poggi, and L. Verdoliva, "Autoencoder with recurrent neural networks for video forgery detection," in *IS and T International Symposium on Electronic Imaging Science and Technology*, 2017, pp. 92–99, doi: 10.2352/ISSN.2470-1173.2017.7.MWSF-330.
- [35] A. Hajji-Ahmad, S. Baudry, B. Chupeau, G. Doerr, and M. Wu, "Flicker forensics for camcorder piracy," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 89–100, Jan. 2017, doi: 10.1109/TIFS.2016.2603603.
- [36] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, 2012, doi: 10.1109/TIFS.2012.2205568.
- [37] M. Baştan, "Multi-view object detection in dual-energy X-ray images," *Machine Vision and Applications*, vol. 26, no. 7–8, pp. 1045–1060, Nov. 2015, doi: 10.1007/s00138-015-0706-x.
- [38] S. Bian, W. Luo, and J. Huang, "Exposing fake bit rate videos and estimating original bit rates," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 12, pp. 2144–2154, Dec. 2014, doi: 10.1109/TCSVT.2014.2334031.
- [39] P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Codec and GOP identification in double compressed videos," *IEEE Transactions on Image Processing*, vol. 25, no. 5, pp. 2298–2310, May 2016, doi: 10.1109/TIP.2016.2541960.
- [40] S. Milani, P. Bestagini, M. Tagliasacchi, and S. Tubaro, "Multiple compression detection for video sequences," in *2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP)*, Sep. 2012, pp. 112–117, doi: 10.1109/MMSP.2012.6343425.
- [41] S. Verde, L. Bondi, P. Bestagini, S. Milani, G. Calvagno, and S. Tubaro, "Video codec forensics based on convolutional neural networks," in *2018 25th IEEE International Conference on Image Processing (ICIP)*, Oct. 2018, pp. 530–534, doi: 10.1109/ICIP.2018.8451143.
- [42] X. Lin, J. Liu, and X. Kang, "Audio recapture detection with convolutional neural networks," *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1480–1487, Aug. 2016, doi: 10.1109/TMM.2016.2571999.
- [43] J. J. Stubbs, G. C. Birch, B. L. Woo, and C. G. Kouhestani, "Physical security assessment with convolutional neural network transfer learning," in *2017 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2017, pp. 1–6, doi: 10.1109/ICCST.2017.8167800.
- [44] S. Akcay, M. E. Kundegorski, C. G. Willcocks, and T. P. Breckon, "Using deep convolutional neural network architectures for object classification and detection within X-Ray baggage security imagery," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2203–2215, Sep. 2018, doi: 10.1109/TIFS.2018.2812196.
- [45] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012, doi: 10.1109/TIFS.2012.2190402.
- [46] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017, doi: 10.1109/TIFS.2017.2710946.
- [47] Y. Qian, J. Dong, W. Wang, and T. Tan, "Learning and transferring representations for image steganalysis using convolutional neural network," in *Proceedings-International Conference on Image Processing, ICIP*, 2016, no. 61303262, pp. 2752–2756, doi: 10.1109/ICIP.2016.7532860.
- [48] S. Wu, S.-H. Zhong, and Y. Liu, "Steganalysis via deep residual network," in *2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*, Dec. 2016, pp. 1233–1236, doi: 10.1109/ICPADS.2016.0167.
- [49] "Xiph.org video test media [derf's collection]," *Xiph.org*. <https://media.xiph.org/video/derf/> (accessed Jul. 17, 2022).
- [50] S. Qi, Z. Huang, Y. Li, and S. Shi, "Audio recording device identification based on deep learning," in *2016 IEEE International Conference on Signal and Image Processing (ICSIP)*, Aug. 2016, pp. 426–431, doi: 10.1109/SIPROCESS.2016.7888298.
- [51] S. S. Ekhande, P. S. P. Sonavane, and D. P. J. Kulkarni, "Universal steganalysis using feature selection strategy for higher order image statistics," *International Journal of Computer Applications*, vol. 1, no. 19, pp. 53–56, 2010, doi: 10.5120/404-600.

## BIOGRAPHIES OF AUTHORS







**Sonali Ekhande**    received B.E degree in Computer Science and Engineering in 2000 and M.E in Computer Science and Engineering in 2009 from Shivaji University, India. She is currently working as Assistant Professor at D. Y. Patil College of Engineering, Kolhapur and Ph.D candidate at JCE, VTU, Belagavi. Her research interests are in the area of information and forensic security, machine learning, deep learning and evolutionary computing. She can be contacted at email: sonalisurve2007@gmail.com.



**Uttam Patil**     received the B.E. and M.Tech. degree from Visvesvaraya Technological University (VTU) in 2008 and 2012 respectively, Ph.D. in Faculty of Computer and information sciences from VTU in 2020. He is presently an Associate Professor and Head of the department of Computer Science and engineering in Jain College of Engineering Belgaum, Karnataka, India. His research interests include Artificial Intelligence, Cognitive computing, Deep Learning. His work has been documented in more than 12 papers. He can be contacted at email: [uttampatil@jainbgm.in](mailto:uttampatil@jainbgm.in).



**Kshama Vishwanath Kulhalli**     is Working as Professor in CSE Dept. in D. Y. Patil College of Engineering and Technology for the last 37 years. She has done BE (E&C) from Karnataka University, M. S from BITS Pilani and PhD from Shivaji University. Her research interests are AI and ML, Computer Vision, Image Processing and Mobile Computing, Biomedical engineering. She has 3 Patents and has published more than 40 papers in High reputed Journals. She can be contacted at email: [kvkulhalli@gmail.com](mailto:kvkulhalli@gmail.com).