Chapter 2

REVIEW OF LITERATURE

- The Forensic Framework and laws
- Digital Fraud detection techniques
- Watermarking Schemes
- Modern Forgery detection techniques
CHAPTER-2: REVIEW OF LITERATURE

2.1 The Forensic Framework and laws

A security of information is vital for every organization, for a better and efficient management. The assets of information have to be protected for a business as well as private data. The processes required for the protection of the data are dependent on the human behavior. A framework for the reference of information security (Niekerk and Solms, 2010) is essential, because the employees are considered to be a threat to an organization, either due to their dire intentions, through their negligence, or in most of the cases, due to the lack of knowledge. The reference framework suggests the following:

![Figure 2.1: Forensic Framework](image)

**Figure 2.1: Forensic Framework**

BL: Minimum Acceptable Baseline – This line indicates what would be an acceptable minimum security baseline; in other words, a culture whose net effect would meet the minimum requirements for some industry standard.

SL: Nett Security Level – This line indicates the actual net effect of the culture on the overall security effort. This line can be seen as the cumulative effect of the four underlying levels of the culture. The net security level (SL) can either be
more secure (to the right), less secure (to the left), or just as secure (overlapping) as the minimum acceptable baseline (BL).

AF: Artifacts – This node represents the relative strength of the artifact level (AF) of the culture. If this node is to the left of the minimum acceptable baseline (BL), it indicates that the measurable artifacts are not as secure as they should be. A node to the right of the baseline (BL) would indicate artifacts that are even more secure than the acceptable minimum. A node exactly on the baseline (BL) would indicate artifacts that are just as secure as required by this baseline.

EV: Espoused Values – This node represents the relative strength of the organization’s espoused value level (EV). The various policies and procedures comprising this level could be more, less, or just as comprehensive than those recommended as the minimum acceptable baseline.

SA: Shared Tacit Assumptions – This node represents the relative strength of the organization’s shared tacit assumption level (SA). The underlying beliefs or values of the employees could be either more, less, or just as in favor of good secure practices as required by the minimum acceptable baseline.

KN: Knowledge – This node represents how much knowledge the organization’s employees have regarding information security. Employees can be more knowledgeable than a certain minimum level needed to perform their jobs securely, they could be less knowledgeable, or they could have exactly the minimum requisite level of knowledge.

There are ever challenging implications of a data theft present in the jurisdiction and laws in India and many other countries. Such rules come into picture in the recent era, due to the advances in digital technology (Biswas, 2011). The Indian Penal Code (IPC), 1860 have specified that “whoever being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the
Chapter 2: Review of Literature

mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or willfully suffers any other person so to do”.

With an advent of the new devices and software tools for editing the digital documents, there are new rules to be applied after this IPC Act, such as - Computer Misuse Act 1990. This Act punishes unauthorized access to computer material and a person is guilty of an offence if:

(i) he causes a computer to perform any function with intent to secure access to any programmer data held in any computer.

(ii) the access he intends to secure is unauthorized.

(iii) he knows at the time when he causes the computer to perform the function that, that is the case.

The Information Technology Act, 2000 has been amended as well as legislation is introduced before the Rajya Sabha in respect of personal data protection, in the shape of the Personal Data Protection Bill. The laws for other countries with reference to the digital documents are of varying nature.

The security of data can be considered as a third wave of technology (Solms, 2000). There exists a system for automatically detecting the ways in which images have been copied and edited or manipulated (Kennedy and Chang, 2009). The conclusion can be drawn upon these manipulation cues to construct probable parent-child relationships between pairs of images, where the child image was derived through a series of visual manipulations on the parent image. Through the detection of these relationships across a plurality of images, we can construct a history of the image, called the visual migration map (VMM), which traces the manipulations applied to the image through past generations. The VMMs are proposed to be applied as part of a larger internet image archaeology system (IIAS), which can process a given set of related images and surface many interesting instances of images from within the set. In particular, the image
closest to the "original" photograph might be among the images with the most
descendants in the VMM. The images that are most deeply descended from the
original may exhibit unique differences and changes in the perspective being
conveyed.

The system is evaluated across a set of photographs crawled from the web and it
was found that many types of image manipulations can be automatically
detected and used to construct plausible VMMs. These maps can then be
successfully mined to find interesting instances of images and to suppress
uninteresting or redundant ones, leading to a better understanding of how
images are used over different times, sources, and contexts.
Chapter 2: Review of Literature

2.2 Digital Fraud detection techniques

2.2.1 Use of Timestamps

The use of stochastic forensic characteristics is considered to be one of the first steps towards the forgery detection. Such method examines the file system to find out the time at which the files were copied. This technique (Bose et al., 2011) can be implemented by using the stochastic model of the file system and determining the Mac file timestamps, which are exclusively used to check the copy operation. The advantage of the suggested method is that, the detection is possible at any time in future also. Here, the silent features of an image files are extracted successfully by using the concept of stochastic.

The connectivity (Rosenfeld, 1970) and adjacency (Rosenfeld, 1974) in a digital picture is a peculiarity to determine the common elements amongst them. The two simply connected sets that have the same area are IP equivalent (Rosenfeld and Nakamura, 2002).

The properties of the files can be determined using the following features:

(i) File access: Depending on the type of operation performed on the files, a timestamp always suggests the fact. It determines whether there is an update in the time-stamp of file access, and if it is so, it also identifies the set of files with such case. The copy of all files or a portion of the folder can be found. Comparatively, in case of virus check, only specific files such as executables are updated and searching will result into the change in subsequence of the file name.

(ii) Skipped folders and files: Under certain known conditions, few files and folders cannot be determined. These files or folders may be system (OS) files and executables, hidden files, files names starting with '.' (period), Alternate Data Streams and hidden files of NTFS and ‘Thumbs.db’ file in case of Windows OS.
(iii) Method of tree traversal: There are possibilities that a recursion method is applied with either depth first approach or breadth first or another method.

(iv) Visit order of sibling files: The default order of visit is according to file system. However, the alphabetical or date or file type may also be used as a criterion. The order is of importance in a situation where a folder consists of a set of files, as well as folders, and priority can start either with a file or folder.

(v) Speed: It refers to the rate at which the files and folders are accessed by the user. It is also dependent on the number of files and the file size. In case of copying a folder, the change in timestamp of files and folders inside it are noted prior to the actual copy operation.

The approach of using timestamps of a file can also be analysed by using attack of pod slurping (Kavallaris and Katos, 2010). This technique, similar to the one suggested by Grier, also considers the time as a critical factor, and constructs a synthetic metrix from the timestamp of a file system.

In this system, the probability of an unauthorized copy of a file can be determined with an aid of comparison between the rate of file transfer by using USB drive detected through the Windows OS registry (Carvey, 2005) and the rate of transfer previously known from the last access. From the initial stages of identification, it can be concluded that the rate of file transfer is directly dependent on the model and make of USB device, and thus assists the investigator to determine a leakage of files.

The following conclusions are drawn for the attacks of pod slurping:

- The leakage probability $L$ is negligible when there is no slurping attack. This suggests that false positives would also be negligible.

- The leakage probability $L$ is high (in the range of 0.3 to 1.0), even for a small number of files transferred in the case of a slurping attack.
The leakage probability $L$ decreases monotonically for files accessed after the attack is complete.

With the suggested methods available for file system verification, any of the existing technique can work depending on the particular type, considering the survey of outlier detection methodologies (Hodge and Austin, 2004). An intrusion can also be detected based on the host, by using dynamic and static behavioral models (Yeung and Ding, 2003).

2.2.2 Plastic card fraud detection.

Due to modernization in the banking system, the customers are provided with direct access to their accounts for the deposit, withdrawal and many other transactions through credit or debit cards. A framework suggesting the detection of frauds made through such plastic cards is very useful for our study, since it ultimately focuses to the solution strategies.

A model for plastic card fraud detection (Fawcett and Provost, 2002) systems suggests a useful framework for such fraud.

The hybrid model for fraud detection suggests data-customised approach combines elements of supervised and unsupervised methodologies aiming to compensate for the individual deficiencies of the methods (Krivko, 2010). It demonstrates the ability of the hybrid model to identify fraudulent activity on the real debit card transaction data. The framework also explores the model's efficiency against that of the existing monitoring system of the collaborating bank, using appropriate performance assessment criteria.

Once the model is constructed one can assess the “status” of each account with every new transaction made. The hybrid model produces a suspiciousness score, which is a real number between 0 and 1 associated with each account which is updated as a new transaction occurs. This is then compared with a threshold value in order to assign account “status” to one of two classes: “suspected to be compromised” and “assumed to be legitimate”. The threshold is set up during
Chapter 2: Review of Literature

model training such that it delivers user-specified values of performance measures.
Frauds can be detected by reviewing different statistical methods (Bolton and Hand, 2002).

2.2.3 Biometrics

Biometrics is another security tool most widely accepted for the authorization. This includes the input in form of fingerprints, iris recognition, face detection, ear pattern, voice input and many others.

A novel image hiding approach based on correlation analysis for secure multimodal biometrics proposes methodology based on correlation analysis, which is used to protect the security and integrity of transmitted multimodal biometric images for network-based identification (Grier, 2010). Compared with existing methods, the correlation between the biometric images and the cover image is first analyzed by partial least squares (PLS) and particle swarm optimization (PSO), aiming to make use of the abundant information of cover image to represent the biometric images. Representing the biometric images using the corresponding content of cover image results in the generation of the residual images with much less energy. Then, considering the human visual system (HVS) model, the residual images as the secret images are embedded into the cover image using middle-significant-bit (MSB) method. Extensive experimental results demonstrate that the proposed approach not only provides good imperceptibility but also resists some common attacks and assures the effectiveness of network-based multimodal biometrics identification.

2.2.4 File Systems

A similar approach is also available to check the self-similarity in file systems (Gribble et al., 1998). The attacks made on sensitive data by insider can be indentified through SIDD (Yali et al., 2009): A framework for such detection.
In addition to the timestamps, other properties of files and folders are also useful for determining the history or file forensic. One of the approaches is the use of purpose-built functions and block hashes to enable small block and sub-file forensics (Garfinkel et al., 2010).

There is a growing need for automated techniques and tools that operate on bulk data, and specifically on bulk data at the block level. The reasons for such requirement are as stated below:

- File systems and files may not be recoverable due to damage, media failure, partial overwriting, or the use of an unknown file system.
- There may be insufficient time to read the entire file system, or a need to process data in parallel.
- File contents may be encrypted.
- The trees structure of file systems makes it hard to parallelize many types of forensic operations.

The research work by Garfinkel et al introduces an approach for performing small block forensics. Some of this work is based upon block hash calculations, that is, the calculation of cryptographic hashes on individual blocks of data, rather than on entire files. Other work is based on bulk data analysis and the examination of blocks of data for specific features or traits irrespective of file boundaries.

Standardization for forensic corpora is also anticipated to bring science to digital forensic (Gerfinkel et al., 2009). The statistical analysis can also help the identification of data type (Moody and Erbacher, 2008).

The timestamp of files can also be used with a different perspective, by leaving timing-channel fingerprints (Shebaro et al., 2010) in hidden service log files.

There are three main reasons why, among the many information channels various log files afford, we focus on only timing channels using the timestamps:
Chapter 2: Review of Literature

For legal reasons, standardized methods are preferable to ad-hoc methods, because precedents can be established for well-analyzed algorithms for recovering a footprint. This requires that a single method be used for many services, and, while various services log different data that is application-specific, most contain some sort of timestamp.

Anonymization technologies sometimes hide IP addresses, URLs, and other objects in the log file. For example, when Apache is set up as a Tor hidden service using Proxy, the IP address for all logged requests is 127.0.0.1 due to local proxying. Timing information, on the other hand, is typically preserved.

By using exclusively timing and timestamps for leaving the fingerprint, the other channels of information (e.g., the URL of the document being requested) can be reserved for other information that the fingerprinter may want to preserve in the log. For example, proof of the existence of a file on the server at a given time.

By using TCP timestamps, covert messaging can be performed (Giffin et al., 2002). Wray, J.C. also executed the analysis of covert timing channels in 1991.

The advanced forensic format can also be extended to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow (Cohen et al., 2009). A framework for managing and storing digital evidence is suggested, where existing evidence management file formats are first examined and then their strengths and limitations are outlined. The proposed Advanced Forensics Format (AFF4) framework extends these efforts into a universal evidence management system. A forensic investigation framework can also be proposed based on the event (Carrier and Spafford, 2004). Consequently, advance carving techniques (Cohen, 2007), as well as specialized tool Pyflag, used as advanced network forensic framework (Cohen, 2008) are proposed.

Contemporary fingerprint system uses solid flat sensor which requires contact of the finger on a platen surface. This often results in several problems such as image deformation, durability weakening in the sensor, latent fingerprint issues.
which can lead to forgery and hygienic problems. On the other hand, bio-metric characteristics cannot be changed; therefore, the loss of privacy is permanent if they are ever compromised. Coupled with template protection mechanism, a touch-less fingerprint verification system is further provoked. In this issue, a secure end-to-end touch-less fingerprint verification system is presented (Hieta et al., 2010). The fingerprint image captured with a digital camera is first pre-processed via the proposed pre-processing algorithm to reduce the problems appear in the image. Then, Multiple Random Projections-Support Vector Machine (MRP-SVM) is proposed to secure fingerprint template while improving system performance.

An image pattern, as used in many applications such as geoseismic surveys or medical diagnostics, can also be used for improving radiometry of imaging spectrometers by using programmable spectral regions of interest.

Programmable imaging spectrometers can be adjusted to fit specific application requirements that differ from the instrument initial spectral design goals. Sensor spectral characteristics and its signal-to-noise ratio (SNR) can be changed by applying customized online binning patterns (Dell'Endice et al., in press).

The researchers have devised a software utility that generates application driven spectral binning patterns by using an SNR dependent sensor model. The utility,
named BinGO (Binning Pattern Generator and Optimiser), is used to produce predefined binning patterns that either

(a) Allow an existing imaging spectrometer to optimize its spectral characteristics for a specific application.
(b) Allow an existing imaging spectrometer to spectral and/or spatially emulate another instrument.
(c) Design new multispectral or imaging spectrometer missions, which may be space borne, airborne or terrestrial.

The noise distributions for imaging spectrometers can be studied for analysis (Nieke et al., 1999).

When the image forgery is performed, the preservation of connectivity between the pixels becomes questionable issue (Bose et al., 2011). By considering local modification operation on binary images in which black pixel p and a white pixel q are interchanged, the interchange operation can be performed on the current image I to obtain a new image I', where

\[
I'(x) = \begin{cases} 
I(p) & \text{if } x = q \\
I(q) & \text{if } x = p \\
I(x) & \text{otherwise.}
\end{cases}
\]

The exclusive efforts were made in research in form of a Special issue on image and video retrieval evaluation (Hanbury et al., 2010). Each of the work in this special issue deals with various aspects of designing suitable evaluation resources to promote research and development in image and video retrieval systems, along with the technologies required to implement such frameworks in practice. The evaluation ideas being used are – Pictorial information retrieval (Enser, 1995), overview and proposals for performance evaluation in content-based image retrieval (Muller et al., 2001) and Image retrieval evaluation (Smith, 1998).
The audio signals can also be checked to have the similarity using Recursive Nearest Neighbor Search in a Sparse and Multiscale Domain (Sturm and Daudet, 2011). To approximate the cosine distance between the signals, pairwise comparisons are made between the elements of localized sparse models built from large and redundant multiscale dictionaries of time-frequency atoms.

Image processing and analysis are critically important for the medical images also. A tumor can be identified from the given image with an aid of wavelet packet transforms and neighborhood rough set (Zhang et al., 2010).

Tumor classification is an important application domain of gene expression data. Because of its characteristics of high dimensionality and small sample size (SSS), and a great number of redundant genes not related to tumor phenotypes, various feature extraction or gene selection methods have been applied to gene expression data analysis. Wavelet packet transforms (WPT) and neighborhood rough sets (NRS) are effective tools to extract and select features. A novel approach of tumor classification is available, based on WPT and NRS. First the classification features are extracted by WPT and the decision tables are formed, then the attributes of the decision tables are reduced by NRS.

Thirdly, a feature subset with few attributes and high classification ability is obtained. The experimental results on three gene expression datasets demonstrate that the method proposed by Zhang et al is effective and feasible.

SVM-Support Vector Machine is a relatively new type of statistic learning theory. It builds up a hyper-plane as the decision surface to maximize the margin of separation between two-class samples.

K-NN is a most common and non parametric method. To classify an unknown sample x, K-NN extracts k closest vectors from the training set using similarity measures, and makes decision for the table of the unknown sample x using the majority class label of the k nearest neighbors. Here, Euclidean distance is used to measure the similarity of samples.
Chapter 2: Review of Literature

NEC is similar to K-NN, and based on the general idea of estimating the class of unknown sample according to its neighbors, but differing from K-NN, NEC considers a kind of neighbor within a sufficiently small and near area around the sample, in other words, all training samples surrounding the test sample take part in the classification decision process.

The Biomarkers are identified by feature wrappers (Xiong et al., 2001). Equivalent approaches to this technique are neighborhood classifiers (Hu et al., 2008) and Neighborhood operator systems and approximations (Wu and Zhang, 2002).

The survey of almost 300 key theoretical and empirical contributions in the current decade is related to image retrieval and automatic image annotation (Datta et al., 2008). The significant challenges are involved in the adaptation of existing image retrieval techniques to build systems that can be useful in the real world. In retrospect of what has been achieved so far, along with the inference of what the future may hold for image retrieval research.

Ideal Spatial adaptation can be verified by wavelet shrinkage (Donoho and Johnstone, 1994) and Multiresolution analysis (Cohen et al., 1993). The algorithms are devised to contain the optimal results.
2.3 Watermarking Schemes

The digital image can be protected with most popular approach to Watermarking, which contains images with Self-Correcting Capabilities (Fridrich and Goljan, 1999). There are two techniques for self-embedding an image in itself as a means for protecting the image content. After self-embedding, it is possible to recover portions of the image that have been cropped out, replaced, damaged, or otherwise tampered without accessing the original image. The first method is based on transforming small 8×8 blocks using a DCT, quantizing the coefficients, and carefully encoding them in the least significant bits of other, distant squares. This method provides very high quality of reconstruction but it is very fragile. The quality of the reconstructed image areas is roughly equivalent to a 50% quality JPEG compressed original. The second method uses a principle similar to differential encoding to embed a circular shift of the original image with decreased color depth into the original image. The quality of the reconstructed image gradually degrades with increasing amount of noise in the tampered image. The first technique can also be used as a fragile watermark for image authentication, while the second technique can be classified as a semi-robust watermark. The watermark techniques are proposed with following criteria:

- Slippery New age (Walton, 1995)
- General concept (Wolfgang and Delp, 1996)
- Invisible technique (Yeung and Mintzer, 1997)
- Distortion measurement (Zhu et al., 1997)
- Image integrity and Ownership verification (Wong, 1998)
- Tamper Detection (Fridrich, 1998a)
- Methods for Detecting changes (Fridrich, 1998b)

The watermarking approach is considered to be widely accepted, where semi-fragile watermarking is useful for authenticating JPEG visual content (Lin and...
In order to practically implement the approach, effective tool like SARI - Self-Authentication-and-Recovery Image Watermarking System (Lin and Chang, 2001) is accessible. In SARI project, a novel image authentication system is designed, based on semi-fragile watermarking technique. The system, called SARI, can accept quantization-based lossy compression to a determined degree without any false alarm and can sensitively detect and locate malicious manipulations. It is the first system that has such capability in distinguishing malicious attacks from acceptable operations. Furthermore, the corrupted area can be approximately recovered by the information hidden in the image. The amount of information embedded in our SARI system has nearly reached the theoretical maximum zero-error information hiding capacity of digital images. The software prototype includes two parts - the watermark embedder that is freely distributed and the authenticator that can be deployed online as a third-party service or used in the recipient side. This is an example of implementation of concepts in form of software, which is common in our current research.

Reversible fragile watermarking is used for locating tampered blocks in JPEG images (Zhang et al., 2010). It proposes a fragile watermarking scheme for JPEG images, in which two watermark bits are embedded into each block using a reversible data-hiding scheme. On the receiver side, after attempting to extract the watermark data and to recover the original content, the number of mismatches between the watermark data extracted from the received image and derived from the recovered contents is used to judge whether a block has been tampered. If the content replacement is not serious, we can always identify the blocks containing fake contents and perfectly recover the original information of the remaining blocks. Similarly, the watermarking schemes such as - Secret and Public key (Wong and Memon, 2001) and Gradient image for improved localization (Suthaharan, 2004) detects the image forgery.
Chapter 2: Review of Literature

The Secure hybrid approach against tampering and copy attack (Deguillaume et al., 2003) is known to be effective method. Imperceptibility and robustness of Genetic watermarking can be verified with the study of the effect DCT and DWT domains (Shaamala et al., 2011). The more common and easily implemented method, which is also comparable to forgery detection referred in Chapter-4, is a watermarking based on DCT-domain of three RGB color channels (El-Fegh et al., 2009).

Watermarking using genetic algorithm for the optimization of the tread-off between the watermarking requirements has attacked the attention of researchers; amongst the watermarking requirements, the imperceptibility and robustness is one of the main requirements. The image adaptive watermark is generated based on image features, which allows the sharp detection of microscopic changes to locate modifications in the image (Shefali et al., 2007).

Further, the scheme utilizes the multipurpose watermark consisting of soft authenticator watermark and chrominance watermark, which has been proved fragile to some predefined processing like intentional fabrication of the image or forgery and robust to other incidental attacks caused in the communication channel. The invisible watermarking in an image is implemented, as shown in Figure 2.3.

![Figure 2.3: Invisible Watermarking in an image.](image-url)
A hierarchical digital watermarking method can also be used for image tamper detection and recovery (Lin et al., 2005). The method is efficient as it only uses simple operations such as parity check and comparison between average intensities. It is effective because the detection is based on a hierarchical structure so that the accuracy of tamper localization can be ensured. That is, if a tampered block is not detected in level-1 inspection, it will be detected in level-2 or level-3 inspection with a probability of nearly 1. This method is also very storage effective, as it only requires a secret key and a public chaotic mixing algorithm to recover a tampered image. The experimental results demonstrate that the precision of tamper detection and localization is 99.6% and 100% after level-2 and level-3 inspection, respectively. The tamper recovery rate is better than 93% for a less than half tampered image. The method is not only as simple and as effective in tamper detection and localization, it also provides with the capability of tamper recovery by trading off the quality of the watermarked images about 5 dB.

Watermarking scheme can detect the tamper as well as provide recovery mechanism (Lin et al., 2007). The main goal is to detect and recover the tampered region accurately. In addition, the proposed method has robustness to resist the attacks of JPEG compression and cropping.

Watermarking techniques can be classified as robust, semi-fragile and fragile. Robust watermarks are designed to survive intentional (malicious) and unintentional (non-malicious) modifications of the watermarked image, Semi-fragile watermarks are layout for detecting any unauthorized alteration, and allowing in the same time some image processing operations. On the contrary, a watermarking technique that cannot robust against noise or attacks is called fragile technique. Fragile watermarking techniques are concerned with complete integrity verification. Furthermore, watermarking techniques can be classified as blind and non-blind, Blind watermarking techniques do not require access to the
original un-watermarked data of image, video, audio, etc. to recover the watermark. In contrast, non-blind watermarking technique requires the original data needed for extraction of the watermarked. In general, the non-blind scheme is more robust than the blind watermark as it is obvious that the watermark can be extracted easily by knowing the un-watermarked data.
Chapter 2: Review of Literature

2.4 Modern Forgery Detection Techniques

2.4.1 Data Hiding

The major challenge to the processing of digital images is retaining the image into its original form. The method used for adaptive reversible data hiding scheme based on integer transform (Peng et al., 2012) is suitable for high capacity.

It is based on integer transform and adaptive embedding, and proposes a new reversible data hiding algorithm. By tuning parameter in integer transform, data can be embedded adaptively according to the block type determined by the pre-estimated distortion. In this way, it avoids large distortion generated by noisy blocks and can embed more data into smooth blocks, and thus image quality is improved compared with the previous integer-transform-based algorithm. For future work, reversible data hiding can be designed in a more meaningful way, to further enhance capacity-distortion performance while keeping low computational complexity. Moreover, investigating practically and theoretically, the maximum embedding capacity with reversibility for natural image is also an interesting problem.

As there are several methods for information hiding (Petitcolas, 1999), a steganography method is useful for images by pixel-value differencing (Wu and Tsai, 2003). The reversible data embedding is implemented by using difference expansion (Tian, 2003).

The software tools, which successfully implement the ideas, are considered to be more powerful for the image processing or forensic detections. One of such example is DART, software to analyse root system architecture and development from captured images (Bot et al., 2010).

Image analysis is used in numerous studies of root system architecture (RSA). To date, fully automatic procedures have not been good enough to completely replace alternative manual methods. DART (Data Analysis of Root Tracings) is
freeware based on human vision to identify roots, particularly across time-series. Each root is described by a series of ordered links encapsulating specific information and is connected to other roots. The population of links constitutes the RSA. DART creates a comprehensive dataset ready for individual or global analyses and this can display root growth sequences along time. It exemplifies individual tomato root growth response to shortfall in solar radiation and analyses the global distribution of the inter-root branching distances.

Similar to DART, EZ-RHIZO is integrated software for the fast and accurate measurement of root system architecture (Armengaud, 2008).

The Learning approach is useful in form of one of the several ideas of Artificial Intelligence. Based on this fact, Sparsity-based Image Denoising (Dong et al., 2011) can be determined via Dictionary Learning and Structural Clustering. Image denoising can be carried out with a non-local algorithm (Buades et al., 2005), while image restoration is carried with non-local sparse models (Mairal et al., 2009).

The concept presents a variational framework for unifying the two views and propose a new denoising algorithm built upon clustering-based sparse representation (CSR). Inspired by the success of 11-optimization, it formulates a double-header 11-optimization problem where the regularization involves both dictionary learning and structural structuring.

Considering the geoseismic applications for digital images, the analysis of images aid us in our study to check the similarities. The process of Co-registration and correlation of aerial photographs for ground deformation measurements (Ayoub et al., 2009) is one of such approach.

The technique requires the digitization of the film based photographs with a high spatial and radiometric resolution scanner. Digital photography is not considered in this study as aerial photography archives are mainly film based.
However, the technique described by them could be used with digital frame cameras as well.

2.4.2 Geographical images

The triggered aseismic fault slip from nearby earthquakes may be static or dynamic (Du et al., 2003). The optimal imagery is used for monitoring of earth surface dynamics (Leprince et al., 2008).

De-Noising with the traditional orthogonal, maximally-decimated wavelet transform sometimes exhibits visual artifacts; we attribute some of these, for example, Gibbs phenomena in the neighborhood of discontinuities to the lack of translation invariance of the wavelet basis. One method to suppress such artifacts, termed cycle spinning (Coifman and Donoho, 1998), is to average out the translation dependence. For a range of shifts, one shifts the data (right or left as the case may be), De-Noises the shifted data, and then unshifts the de-noised data.

Prior to comparison, images are co-registered through their ortho-rectification on a common reference system. Cumulative uncertainties on both the acquisition parameters and topography lead to mis-registrations between the ortho-rectified images to be compared. The co-registration is therefore improved by optimizing the acquisition parameters of the second image as slave, with respect to the first ortho-rectified image as master.

Ortho-rectified and precisely co-registered images are then correlated using a sliding window. At each step, horizontal offsets along the East or West and North or South directions are measured and stored.

The proposal of determining the noise from an image is exceptionally good criterion to aid forensic. The blind image forensic approach is applied (Mahdian and Saic, 2009) by using noise inconsistencies.
2.4.3 Blind Methods

Existing digital forgery detection methods are divided into active and passive blind approaches. The blind approach is regarded as the new direction and interest in this field has rapidly increased over the last few years. In contrast to active approaches, blind approaches do not need any explicit priori information about the image. They work in the absence of any digital watermark or signature. Blind approaches have not yet been thoroughly researched by many. The forgeries can be reduced by using writer-independent off-line signature verification through ensemble of classifiers \cite{Bertolini2010}. In this work, two important issues of off-line signature verification are addressed. The first one regards feature extraction. A new graphometric feature set is developed, that considers the curvature of the most important segments, perceptually speaking, of the signature. The idea is to simulate the shape of the signature by using Bezier curves and then extract features from these curves. The second important aspect is the use of an ensemble of classifiers based on graphometric features to improve the reliability of the classification, hence reducing the false acceptance.

The statistical properties are another set of data useful in forensic. The distance between histograms of image \cite{Cha2002} exposes many of the forensic characteristics.

Pondering the digital technology, the digital documents or files, similar to digital images, also carry the same signal properties. A signature of an individual saved in form of digital document, can be verified offline by using fuzzy modeling \cite{Hanmandlua2005}. Such models are based on decisions to be derived in form of probability of forgery. The computer verification of Handwritten system is performed through multi-resolution \cite{Hunt1995} approach.

The neighboring color analysis can be performed through Steganalysis for palette-based images using generalized difference image and color correlogram \cite{Zhao2011}. In this notion, an attempt was made to propose a novel blind
steganalysis algorithm for palette-based images. First, the generalized difference images between adjacent pixels were constructed, and then the moments of characteristic functions of histograms of difference images were extracted as features. Second, in order to measure the dependencies of neighboring colors, color correlogram technique is used to capture the global distribution of local spatial correlation of colors. The center of mass of the characteristic function of color correlogram and the absolute moments of autocorrelogram were extracted. Total of 13 dimension features were classified with machine learning technique. Number of experiments on several existing GIF steganography algorithms indicated that the proposed scheme is effective and gets good performance, especially when the embedding rate is not less than 20%. Experimental results also show that the average accuracy of our proposed scheme for different GIF steganography algorithms outperforms Lyu’s algorithm more than 20%. It also showed that the proposed scheme achieved similar performance with Fridrich’s scheme and higher accuracies comparing to Du’s algorithm and biologically inspired features.

A generalized Benford’s law \cite{Jolion2001} is useful for JPEG coefficients and its applications in image forensics \cite{Fu2007}. The statistical distribution of image DCT coefficients \cite{Eggerton1986} is also functional to image forensic.

Forensic Detection of Image Tampering is conducted by using Intrinsic Statistical Fingerprintsin Histograms \cite{Stamm2010}. To test the performance of global contrast enhancement detection algorithm, database of 341 unaltered images consisting was used, which contains many different subjects and images captured under varying light conditions. These images were taken with several different cameras and range in size from 1500 × 1000 pixels to 2592 × 1944 pixels. To simplify the testing process, it used the green color layer of each of these images to form a set of unaltered grayscale images. Next, a set of contrast
enhanced grayscale images as created by applying the power law transformation.

2.4.4 Similar Block Matching

The similarity in image blocks can be determined with Sequential Straightforward Clustering for Local Image Block Matching (Sekeh et al., 2011). The idea concentrates on computational time and proposes a local block matching algorithm based on block clustering to enhance time complexity. Time complexity of the proposed algorithm is formulated and effects of two parameter, block size and number of cluster, on efficiency of this algorithm are considered. The experimental results and mathematical analysis demonstrate that this algorithm is more cost-effective than lexicographically algorithms in time complexity issue when the image is complex.

It suggests a novel statistical model based on Benford’s law for the probability distributions of the first digits of the block-DCT and quantized JPEG coefficients is presented. A parametric logarithmic law, i.e., the generalized Benford’s law, is formulated. Furthermore, some potential applications of this model in image forensics are discussed in this paper, which include the detection of JPEG compression for images in bitmap format, the estimation of JPEG compression Q-factor for JPEG compressed bitmap image, and the detection of double compressed JPEG image. The results of our extensive experiments demonstrate the effectiveness of the proposed statistical model.

A simple method to detect image tampering operations that involve sharpness or bluriness adjustment is available (Sutchu et al., 2007). The approach is based on the assumption that if a digital image undergoes a copy-paste type of forgery, average sharpness or blurriness value of the forged region is expected to be different as compared to the non-tampered parts of the image. The method of estimating sharpness value of an image is based on the regularity properties of wavelet transform coefficients which involves measuring the decay of wavelet...
transform coefficients across scales. The preliminary results show that the estimated sharpness scores can be used to identify tampered areas of the image. The Tamper detection techniques are based on artifacts created by Color Filter Array (CFA) processing in most digital cameras (Dirik and Memon, 2009). The techniques are based on computing a single feature and a simple threshold based classifier. The efficacy of the approach was tested over thousands of authentic, tampered, and computer generated images. Experimental results demonstrate reasonably low error rates.

The steady improvement in image and video editing techniques has enabled people to synthesize realistic images or videos conveniently. Some legal issues may occur when a doctored image cannot be distinguished from a real one by visual examination. Realizing that it might be impossible to develop a method that is universal for all kinds of images and JPEG is the most frequently used image format, we propose an approach that can detect doctored JPEG images and further locate the doctored parts, by examining the double quantization effect hidden among the DCT coefficients (He et al., 2006).

In order to check the aboriginality and integrity of a digital photograph, a blind forensics scheme for detecting blur manipulation exists. A cost-effective local blur estimator is designed to measure the blurriness of each pixel along a doubted edge. Consistency metric of such a blurriness sequence is constructed based on the deviation from its linear fitting. Then the metric is used as evidence for identifying blur operation. Experimental results both on synthetic and natural images have shown the efficiency of our proposed blur forensics scheme (Cao et al., 2009).

The biggest problem and challenge in digital image forgery is how to ensure that intellectual assets in digital form are authentic and to tampered and their entire contents are authentic and consistent, the provenance of consistency,
integrity authenticity (CIA) can only assure the digital intellectual assets origin and originality (Math and Tripathi, 2010).

Chinese Remainder Theorem (CRT)-based technique for digital watermarking in the Discrete Cosine Transform (DCT) domain is robust to several common attacks (Patra et al., 2010). It compared the performance of the proposed technique with recently proposed Singular Value Decomposition (SVD)-based (Chung et al., 2007) and spatial CRT-based watermarking schemes. Experimental results have shown that the technique successfully makes the watermark perceptually invisible and has better robustness to common image manipulation techniques such as JPEG compression, brightening and sharpening effects compared to the spatial domain-based CRT scheme. The scheme is able to achieve a Tamper Assessment Function (TAF) value of less than 10% when the watermarked image undergoes JPEG compression between a range of 50 to 70%, where-as, the spatial CRT-based scheme produce TAF value of more than 35% and the SVD-based scheme produces TAF value between 10 to 40% depending on the host image, for the same range of compression.

Digital signature methods offer an interesting alternative to classical watermarking techniques, in so far there is no longer a limitation in terms of capacity, nor a problem of robustness, thus offering better localisation of the manipulated areas, better quality reconstruction, and a limited risk of false alarms. Moreover, there is already a high level of expertise in the area of community security. However, the major drawback of these techniques is that the image alone is not self-sufficient. Therefore, the benefits of watermarking are reduced and it becomes necessary to be able to guarantee the authenticity of the image or signature pair. Moreover digital signature methods are not very practical to use with multimedia documents. Finally, future developments should not exclude methods based on the combination of robust watermarking and external signature methods. Watermarking would just be an identifier which
would allow a trusted user access to the registered signature (Rey and Dugelay, 2002).

A solution to the real world problem of Digital Document Forgery is through a 1D hash algorithm coupled with 2D iFFT (irreversible Fast Fourier Transform) by encryption of digital documents in the 2D spatial domain (Cheddad et al., 2009). Further by applying an imperceptible information hiding technique we can add another security layer which is resistant to noise and to a certain extent JPEG compression.

Data hiding based on the similarity between neighboring pixels with reversibility (Li et al., 2010) is the technique which recovers the original image from a stego-image without distortion, once the hidden data are extracted. A natural image usually contains several smooth areas. The difference between two adjacent pixels has a high probability of being a small value. Therefore, this study proposed a novel reversible data hiding method, Adjacent Pixel Difference (APD), which employs the histogram of the pixel difference sequence to increase the embedding capacity. Experimental results reveal that APD achieves a high embedded capacity and still maintains a high stego-image quality. Furthermore, the stego-image quality and embedded capacity of the APD method outperform other existing methods.

Image Manipulation can also be detected with Binary Similarity Measures (Bayram et al., 2005). It proposed a method for digital image forensics, based on Binary Similarity Measures between bit planes used as features. It contains the design of several classifiers to test the tampered or un-tampered status of the images. The performance results in detecting and differentiating a host of attacks were encouraging as it is able to discriminate a doctored image from its original, with a reasonable accuracy. The methods are accessed with vis-à-vis the closest competitor image forensic detector. This method outperform Farid’s detector especially in contrast enhancement and brightness adjustment attacks. On the
other hand, while it gives better performance at stronger levels of manipulations, Farid outperforms this technique at weaker levels. In this respect, the two schemes seem to be complementary; hence fusion of forensic detectors at feature level or decision level must be envisioned.

A lossless data, like file formats other than JPEG, can be embedded by joint neighboring coding (Chang et al., 2009). Similarly, the biometric templates can be securely transmitted with hiding and secure content (Khan et al., 2007). Considering an iris as input for verification, the pattern can be authenticated based on the user-specific feature (Qi et al., 2008).

The image tampering can be detected by use of Blind Deconvolution (Swaminathan et al., 2007). The proposed method is based on the observation that many tampering operations can be approximated as a combination of linear and non-linear components.

A classifier design approach proposes a framework (Avcibaş et al., 2004), where the following results are derived:

<table>
<thead>
<tr>
<th>Image Alternation</th>
<th>False Positive</th>
<th>False Negative</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scaling -10%</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Rotation, 5 Degree</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Brightness Adjustment</td>
<td>1%</td>
<td>1%</td>
<td>99%</td>
</tr>
<tr>
<td>Histogram Equilisation</td>
<td>0%</td>
<td>5%</td>
<td>97.5%</td>
</tr>
<tr>
<td>Mixed Process</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
</tr>
</tbody>
</table>

The correlation between the bit planes as well the binary texture characteristics within the bit planes will differ between an original and a doctored image. This change in the intrinsic characteristics of the image can be monitored via the quantal-spatial moments of the bit planes. These so-called Binary Similarity Measures are used as features in classifier design (Bayram et al., 2005). It has
been shown that the linear classifiers based on BSM features can detect with satisfactory reliability most of the image doctoring executed via Photoshop tool. Consequently, the image manipulation is exposed through feature selection (Bayram et al., 2006). The feature selection process was implemented with the sequential forward floating search, □ SFFS method. The SFFS method analyzes the features in ensembles and can eliminate redundant ones. The floating search method (Pudil et al., 2003) claims that the best feature set is constructed by adding to or removing from the current set of features until no more performance improvement is possible. The SFFS procedure can be described as follows:

- Choose from the set of K features the best two features; i.e., the pair yielding the best classification result.
- Add the most significant feature from those remaining, where the selection is made on the basis of the feature that contributes most to the classification result when all are considered together.
- Determine the least significant feature from the selected set by conditionally removing features one by one, while checking to see if the removal of any one improves or reduces the classification result. If it improves, remove this feature and go to step 3, otherwise do not remove this feature and go to step 2.
- Stop when the number of selected features equals the number of features required.

Hány Farid is considered to be the foremost person in developing many algorithms and concepts related to digital image forensic. As an overview of all techniques suggested for image forensic, following are the methods surveyed (Farid, 2009):

Pixel-Based: The legal system routinely relies on a range of forensic analysis ranging from forensic identification (Deoxyribonucleic acid -DNA or fingerprint)
Chapter 2: Review of Literature

to forensic odontology (teeth), forensic entomology (insects), and forensic geology (soil).

**Cloning:** Two computationally efficient algorithms have been developed to detect cloned image regions, viz. DCT and PCA.

**Resampling:** This process requires resampling the original image onto a new sampling lattice, introducing specific periodic correlations between neighboring pixels.

**Splicing:** A common form of photographic manipulation is the digital splicing of two or more images into a single composite. When performed carefully, the border between the spliced regions can be visually imperceptible.

**Statistical:** The statistical model is composed of the first four statistical moments of each wavelet subband and higher-order statistics that capture the correlations between the various subbands.

**Format based:** The unique properties of lossy compression such as JPEG can be exploited for forensic analysis.

**JPEG Quantization:** Given a three-channel color image (RGB), the standard JPEG compression scheme proceeds as follows: The RGB image is first converted into luminance/chrominance space (YCbCr). The two chrominance channels (CbCr) are typically subsampled by a factor of two relative to the luminance channel (Y). Each channel is then partitioned into 8x8 pixel blocks. These values are converted from unsigned to signed integers. Each block is converted to frequency space using a 2-D discrete cosine transform (DCT). Depending on the specific frequency and channel, each DCT coefficient is then quantized by a quantized amount q. This stage is the primary source of compression.

**Double JPEG:** At a minimum, any digital manipulation requires that an image be loaded into a photo-editing software program and resaved. Since most images are stored in the JPEG format, it is likely that both the original and manipulated
images are stored in this format. In this scenario, the manipulated image is compressed twice.

**JPEG Blocking:** It characterizes the blocking artifacts using pixel value differences within and across block boundaries.

**Camera based:** Inconsistencies in the artifacts of a camera can then be used as evidence of tampering.

**Chromatic Aberration:** In an ideal imaging system, light passes through the lens and is focused to a single point on the sensor. Optical systems, however, deviate from such ideal models in that they fail to perfectly focus light of all wavelengths. Specifically, lateral chromatic aberration manifests itself as a spatial shift in the locations where light of different wavelengths reaches the sensor.

**Color Filter Array:** Most CFAs employ three color filters (red, green, and blue) placed atop each sensor element. Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image.

**Camera Response:** Because most digital camera sensors are very nearly linear, there should be a linear relationship between the amount of light measured by each sensor element and the corresponding final pixel value.

**Sensor noise:** As a digital image moves from the camera sensor to the computer memory, it undergoes a series of processing steps, including quantization, white balancing, demosaicking, color correction, gamma correction, filtering and, usually, JPEG compression. This processing introduces a distinct signature into the image.

**Physics based:** Differences in lighting across an image can then be used as evidence of tampering.

**Light Direction and environment:** The required 3-D surface normals are determined by leveraging a 3-D model of the human eye.
Metric measurements: Several tools from projective geometry allow the rectification of planar surfaces and under certain conditions, the ability to make real-world measurements from a planar surface. A study performed by Farid is as below:

![Figure 2.4: (a) Number plate not legible (b) Result of planar rectification](image)

There exist some basic tamper detection methods (Fridrich, 1998). He provides a comprehensive overview of steganography techniques for tamper detection and authentication of digital images. The techniques are divided into several categories according to their ability to identify changes. Fragile watermarks can detect changes to every pixel and provide accurate information about the image integrity. However, it is not possible to distinguish small, innocuous changes due to common image processing operation from malicious changes, such as feature removal or addition. Semi-fragile watermarks are more robust and allow "authentication with a degree". It is possible to set a threshold in those techniques so that images after high quality JPEG compression, or contrast or brightness adjustment will still be considered authentic to a high degree. In the third category, it provides techniques that attempt to authenticate image features. Such techniques are even more robust and enable robust distinction between innocuous and malicious modifications at the expense of losing the sensitivity to small changes and sometimes the ability to localize modifications.
There are many ways to categorize the image tampering based on various points of view, where the blind methods can also be used (Mahdian and Saic, 2008a). Generally, we can say that the most often operations in photo manipulation are:

- Deleting or hiding a region in the image.
- Adding a new object into the image.
- Misrepresenting the image information.

In blind methods, as they are regarded as a new direction and in contrast to active methods, they work in absence of any protecting techniques and without using any prior information about the image or the camera that took the image. To detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes (e.g., statistical changes).

The main drawback of existing methods is highly limited usability and reliability. This is mainly caused by the complexity of the problem and the blind character of approaches. But it should be noted that the area of Blind Methods (Mahdian and Saic, 2008b) is growing rapidly and results obtained promise a significant improvement in forgery detection in the never ending competition between image forgery creators and image forgery detectors.

A copy-move forgery in a digital image can be detected through few of the below mentioned methodologies also:

- Wavelet representation (Mallat, 1989)
- Digital watermarking (Yeung, 1998)
- Multi stage region merging (Brox et al., 2001)
- Gradient vector diffusion (Yu and Bajaj, 2002)
- Blur moment invariants (Mahdian and Saic, 2007)

A successful approach is proposed to detect the forgery by analyzing the Color Filter Array values (Popescu and Farid, 2005) or Higher Order Wavelet statistics (Farid and Lyu, 2003).
Chapter 2: Review of Literature

It quantifies the specific correlations introduced by CFA interpolation, and describes how these correlations, or lack thereof, can be automatically detected in any portion of an image. It shows the efficacy of this approach in revealing traces of digital tampering in lossless and lossy compressed color images interpolated with several different CFA algorithms.

When creating a digital composite of, for example, two people standing side-by-side, it is often difficult to match the lighting conditions from the individual photographs. Lighting inconsistencies (Johnson and Farid, 2005) can therefore be a useful tool for revealing traces of digital tampering. Borrowing and extending tools from the field of computer vision, we describe how the direction of a point light source can be estimated from only a single image. We show the efficacy of this approach in real-world settings.

In such approach, the direction of projected light source can be estimated automatically (Nillius and Eklundh, 2001) in order to verify if the lighting conditions are consistent in an image or not.

Several statistical techniques are suggested for detecting traces of digital tampering (Popescu and Farid, 2004a) in the absence of any digital watermark or signature. In particular, statistical correlations are quantified that result from specific forms of digital tampering, and detection schemes are devised to reveal these correlations. The forgeries can be exposed by detection of duplicated regions (Popescu and Farid, 2004b).

A bibliography on all blind methods for image fakery detection (Mahdian and Saic, 2010) suggests the following factors as criterion:

- Near Duplicated image regions
- Interpolation and geometric transformations
- Image Splicing
- Computer Graphics and paintings
- JPEG and Compression properties
Chapter 2: Review of Literature

- Lighting
- CFA and inter pixel correlation
- Local noise
- Chromatic Aberration
- Blur and Sharpening
- Projective Geometry

Common sense reasoning (CSR) is a unique approach to detect the false captioning (Lee et al., 2006). Many previous signal-processing techniques are concerned about finding forgery through simple transformation (e.g. resizing, rotating, or scaling), yet little attention is given to examining the semantic content of an image, which is the main issue in recent image forgeries. Here, we present a complete workflow for finding the anomalies within images by combining the methods known in computer graphics and artificial intelligence. CSR finds perceptually meaningful regions using an image segmentation technique and classify these regions based on image statistics. Consequently, it uses AI common-sense reasoning techniques to find ambiguities and anomalies within an image as well as performs reasoning across a corpus of images to identify a semantically based candidate list of potential fraudulent images. Our method introduces a novel framework for forensic reasoning, which allows detection of image tampering. This method works on an assumption of photo forgery performed on the following techniques:

- Deletion of details: removing scene elements.
- Insertion of details: adding scene elements.
- Photomontage: combining multiple images.
- False captioning: misrepresenting image content.

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to
detect image areas that are same or extremely similar. Several methods exist
(Bayram at al., 2008) to achieve this goal. These methods in general use block-
matching procedures, which first divide the image into overlapping blocks and
extract features from each block, assuming similar blocks will yield similar
features. Later, a matching step takes place where the aim is to find the
duplicated blocks based on their feature vectors.
A forgery detection decision is made only if similar features are detected within
the same distance of features associated to connected blocks. It examines several
different block based features proposed for this purpose in relation to their time
complexity and robustness to common processing scaling up or down,
compression, and rotation.
The Digital Forgery in the images is possible to be exposed for JPEG and Bitmap
files (Sunderrajan, 2009), as follows:
- Use of DCT coefficient quantization for JPG image.
- Sum of squared distances for BMP image.
The Copy-Paste forgery can be detected using the concept of BAG – Block
Artifact Grid extraction (Li et al., 2008). The forensics approach is to locate the
BAG firstly, and then check whether the BAG mismatches or not. Once a BAG
mismatch is affirmed, then the image can be authenticated as doctored.
The Copy-move Image Forgery can be detected based on DWT-PCA (Zimba and
Xingming, 2011). According to this criterion, an improved algorithm was
proposed based on Discrete Wavelet Transform (DWT) and Principal
Component Analysis Eigen value Decomposition (PCA-EVD) to detect such
cloning forgery. Furthermore, for academic purposes and via a simplified, toy
image we demonstrate how such algorithm works in detecting cloning forgery.
Experimental results show that the proposed scheme accurately detects such
specific image manipulations as long as the copied region is not rotated or
scaled.
Chapter 2: Review of Literature

Similar to DART suggested earlier, specialized software RepFinder is useful for finding Approximately Repeated Scene Elements for Image Editing (Cheng et al., 2010). It proposes framework where user scribbles are used to guide detection and extraction of such repeated elements. This detection process, which is based on a boundary band method, robustly extracts the repetitions along with their deformations. The algorithm only considers the shape of the elements, and ignores similarity based on color, texture, etc. Subsequently, it uses topological sorting to establish a partial depth ordering of overlapping repeated instances. Missing parts on occluded instances are completed using information from other instances. The extracted repeated instances can then be seamlessly edited and manipulated for a variety of high level tasks that are otherwise difficult to perform. It demonstrates the versatility of framework on a large set of inputs of varying complexity, showing applications to image rearrangement, edit transfer, deformation propagation, and instance replacement.

1. Initialize $B = \{p\}$, the set of all boundary pixels;
2. Initialize queue $Q = \emptyset$;
3. For each boundary pixel $p \in B$ do
   
   mp = tangent vector of the boundary image, at $p$;
   push all neighbors $q$ of $p$ onto $Q$ for which $q \in B$;
   end for

4. Initialize $i = |B| \times b$,
   where $|B|$ is the size of set $B$
   and $b$ is a width parameter;
5. while $i > 0$ and $Q = \emptyset$ do
   Pop $p$ from $Q$;
   mp = 0, num = 0;
   for each already-initialized neighbor $q$ of $p$ do
     if $|mp + mq| > |mp - mq|$ then
       mp = mp + mq;
     else
       mp = mp - mq;
     end if
     num = num + 1;
   end for
   mp = mp/num;

A comparison study on Copy-Cover Image Forgery Detection (Shih and Yuan, 2010) describes and compares the techniques of copy-cover image forgery detection. It is organized as follows. It suggests four copy-cover detection methods, including Principal Component Analysis (PCA), Discrete Cosine Transform (DCT), spatial domain, and statistical domain. It compares the four copy-cover detection methods, and provides the effectiveness and sensitivity under variant additive noises and lossy Joint Photographic Experts Group (JPEG) compressions.

The duplicate regions of a digital image can be identified by using SURF (Shivakumar and Baboo, 2011). The task of finding point correspondence between two images of an object or same scene is part of many computer vision applications. Recently Herbert Bay et al. proposed fast detectors and descriptors, called SURF - Speeded Up Robust Features. SURF’s detector and descriptor is said to be faster and at same time robust to noise, detection displacements and geometric and photometric deformations.

With the existing DCT algorithms for copy-paste detection, the time complexity can be reduced (Khan and Kulkarni, 2010). The algorithm proposed for the same, is as mentioned in Figure-2.5.

Algorithm 2.1: Building the BBM from a boundary image.

Push each uninitialized neighbor of p in the band onto Q;
i = i - 1;
end while

6. For each remaining uninitialized pixel p,
set mp = 0;
Many image processing applications make use of MATLAB for analysis of images used by the system. The image processing capabilities of MATLAB are very useful for all types of Image forgery detection. The photogrammatic mapping carried out using MATLAB tool, which can also be used in traffic surveillance (Madeira et al., 2010).

Open-source software including an easy-to-use graphical user interface (GUI) has been developed for processing, modeling and mapping of gravity and magnetic data. The program, called Potensoft (Arisoy and Dikmen, 2011), is a set
of functions written in MATLAB. The most common application of Potensoft is spatial and frequency domain filtering of gravity and magnetic data. The GUI helps the user easily change all the required parameters. One of the major advantages of the program is to display the input and processed maps in a preview window, thereby allowing the user to track the results during the ongoing process. Source codes can be modified depending on the users' goals. It represents the main features of the program and its capabilities are demonstrated by means of illustrative examples.

One of such applications being geographical data is Seascorr (Meko et al., 2011). It is a MATLAB program for identifying the seasonal climate signal in an annual tree-ring time series, uses is identification of the monthly or seasonal climate signal in an annual time series of indices of ring width.

All the copy-paste detection methods discussed here are useful in particular case of forgery, and no common framework or widely used suggested method is available.