Detection of Image Tampering over Diverse information Security Schemata: A State-of-the-Art

Deepali N. Pande
Dept. of Computer Science & Engineering,
GHRIETW 440016
MH., INDIA
zivyi.elsevier@gmail.com

A.R. Bhagat Patil
Dept. of Computer Science & Engineering,
YCCE 441110
MH., INDIA
arbhagatpatil@gmail.com

Antara S. Bhattacharya
Dept. of Computer Science & Engineering
GHRIETW 440016
MH., INDIA
antara.bhattachraya@raisoni.net

ABSTRACT
Many recent technologies in the field of image processing have necessitated the attention to the field of image forensics. Increase in cyber communication system and availability of advanced digital processing tools, in the past decades has given birth to forgery attempts. Irrespective of various approaches used to protect the Image, proving integrity of the image received in communication is a difficult issue. Under such circumstances, no image can be treated secure against breaches. Moreover, knowledge of the manipulation model is a must for detecting a certain type of tampering.

The aim of this paper is to highlight new developments regarding detection of tampering in comparison of various schemata used in the past decades for forgery detection. An assortment of various models used for providing information security to image based on authentication, integrity and confidentiality is presented. Methods of tamper detection have been assessed over the type of attack. An in depth classification of types of image security has been proposed which emphasizes total security issues. The paper puts forward chief developments in schemata of tampering detection.

General Terms
ISS: Information Security Schemata.

Keywords
Digital imaging; Information Security; Image Tampering Detection; Image Authentication; Image Forensics; Passive Image Tampering Detection;

1. INTRODUCTION
We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Digital Image Forgery Detection is a growing sub-field of research in Image Forensics. Many tools for processing the image have been developed over the past decades. Increase in means for Cyber Communication has invoked a thwart to Information Security principles of the transmitted image. The fundamental goal of Image Forensic Science is to check for the alterations that the image has undergone over the communication channel. It aims at scrutinizing the trustworthiness of Images and detection of forgery made to it. Videos and Audios are the major objects of transactions over the internet. Much of the data transmitted consists of large scale of unauthenticated pieces of information in form of raw chunks. Sometimes it proves cumbersome to follow security measures for every transaction, hence such data forms the treasure house to access information, formulate and renovate so that fusing information to various models becomes an easy task. Due to computerization, now-a-days hanging every piece of information to the computer systems has been a routine practice. Most systems due to usage of unauthorized products and services of internet help hackers and intruders to easily trap such information at an early stage off, even when the information is still being processed for transformation into valuable data. Such customs endanger every step of digital processing and thwart the necessitated action of formulating a processed and secured piece of digitized data. The imperil of harnessing such a jeopardized chunk can breach the security of the document or image under formulation, yielding a fully fake image (or document) in spite of application of designed methods of security over it.

Many disciplines like satellite imaging, military, World Wide Web applications, video conferencing, media, publication and law, medical image science and research areas depend on image forensic science for trustworthiness of the work carried out by them. When used for such diversities, the Forensic Science always works for bringing out the repercussions of intentional security practices, whether used are innocent or indicate intentional deception. They always need best tools to undertake these activities. In contrast, various security measures have been proposed by research scientists and are popularly gaining attention. Over the past decades, approaches such as watermarking had been widely used. More techniques like fragile watermarking, semi-fragile watermarking, digital signatures, and conventional cryptographic measures have been developed and materialized. But these do not cease total security issues as to completely uproot the problems associated of construction of document, image or video right from the basis as discussed above. Regardless of this, it has been surveyed that though employing the security strategies at the ultimate stage, various attacks have been made to breach such strategies thus ruining the whole procedure.

To avoid such problems a plan of discussion for security right from basis has been surveyed in this paper. The paper presents a survey of past schemata for detection of image tampering and focus on current trends for tamper detection. A comparative study of various security models have been surveyed for forgery detection. As discussed above, several methods had been used for security but none compliance it. Henceforth, the generalized schemata for highlighting various issues of information security have been proposed. No method

for tampering detection can be unique for all strategies of security methods since detection of tampering proceeds by first investigating the security architecture that was infringed. To bring forward the survey of the same, we proposes the generic schemata for Image forensics implementing detection of forgery by splitting the basis branches of tampering detection namely, active approaches and the passive approaches which represents together the proposed State-of-the-art. An in depth analysis of newsworthy methods for above discussed issues have also been classified.

The paper is organized into two parts part-I and part- II. Under part-I Literature Assessment is performed comprising of three minor sections. The first section presents a brief history of photography. The second section presents the need for standardization of tools. The third section gives brief assortment of digital image generation process emphasizing constructs for forensics. The second part part-II presents "A State-of-the-Art". A generic schema for diverse information security techniques is presented. Various techniques used for protection of the image from past decades till recent have been assessed. Attacks have been classified according to the type of security. The method of working uses recent algorithms of the root classes of tampering detection namely active tampering detection and passive tampering detection has been rationalized. A brief mathematical model implementing passive image tampering detection has been proposed. Analysis of various algorithms which work over certain attacks has been implemented in a tabular form.

2. LITERATURE ASSESSMENT: Part-I

Due to burgeoning science of digital photography, the art of photography has become an interface to digital imagery. The advancement in the relationship between digital imagery and photography was put in practice by the property that analog photograph can be converted into digital format by scanning it to perform digital imaging operations over it by which the smooth curves and tone modifications are translated into digital format. Digital photographs have vivid applications in various fields of medical and astronomical and many more dependent ones which led digitization into a boom.

3. History of Photography

3.1 Photo chemicals

The former most photography used light-sensitive chemicals like silver and photographic emulsion which were platted on glass or paper to form negatives from which the layer bearing the image was uncovered and transferred to a thick gelatin support that proved hardest to security.

3.2 Films

The latter approach used a system for photo-shooting brought film based cameras into practice. These were used to record non-visible ultraviolet and infrared radiations of pictures flashed on them to form latent image which were then subjected to photographic processing. These systems were dependent on watermarking as the principle for security.

4. Taxonomy of Image Acquisition Tools: A Prerequisite for Standardization

4.1 Digital Camera Pipeline

The digital cameras consist of lens system, sample filters, color filter array, imaging sensor and digital image processor. With the advancements in electronic technology, imaging sensors like charged coupled device (CCD) and CMOS (Complementary Metal-Oxide Semiconductor) were used everywhere with the motive of digitization of analogue platform wherefrom the science of photorealistic computer graphic generated images (PRCG) solely rely on them. Henceforth, sensor fingerprint using photo-response non-uniformity (PRNU) property became a platform for passive image forensics by the fact that a copied region of an image will show an unmatched fingerprint on it. PRNU assessments have been a fundamental in analyzing the trustworthiness of image's integrity. Relating to this theory, the source identification became completely dependent on joint inspection of PRNU and color filter array. The Camera-models are differentiated based on differences in processing techniques and component technologies. The distortions due to type of lens, choice of color filter array and corresponding demosaicing algorithms, color processing algorithms, size of imaging sensor are detected. These are then quantitatively characterized by analysis of the image. The shortcomings in such techniques lie under the fact that many models and brands use components of similar manufacturers. The processing algorithms remain relatively same. Therefore, reliable identification of source camera model depends on characteristics of model dependent features.

PRNU is a unique property of any acquisition tool. But mostly, it has been observed that devices of same brand have similar PRNUs. Therefore after analyzing the above taxonomy for image acquisition it can be judged that tools used in image acquisition should be standardized into Type/ Brand/ Device/Model. The standardization in such manner will curb difficulties in correct identification of sensor fingerprints.

5. Digital Imaging: The Root of Component Forensics

The saga of digital imaging is represented as an organization of various steps to form major three phases like acquisition, coding, and editing. A vital part over these set of structures in imaging process is that they usually strand innate traces called footprints as also fingerprints (in each phase), throughout the processing which forms the core of investigations for forensic science. Figure (1) emphasizes the use of imaging process as a reverse engineering tool for detection of image tampering. It can be helpful for component forensic science.

It is here, wherefrom the pivot of image integrity commence. As shown in the block diagram of figure1, it can be seen that the light coming from real scene is focused by the lenses on camera sensors by which a digital signal is generated in the image acquisition phase. The light filters through CFA (Color Filter Array) which selectively permits certain components of light to pass through. This signal undergoes various internal processing like white balancing, color processing, gamma correction, contrast enhancement, image sharpening. As far as the issue of security is concerned, intrinsic fingerprints of source camera are used to achieve the said goal since every component which modifies the input leaves certain internal fingerprints in the output. The processed signal is stored in camera memory in a compressed form. These compression techniques, usually lossy in nature leave certain footprints which can be related to specific architecture of coding for forensics. This technique is commonly known as coding fingerprints. So, it becomes the root of component forensics. Any forgery created can be traced by comparing these traces of fingerprints. Huge set of researches have been performed over coding artifacts. The presence of inconsistencies becomes the trace factor of evidence of tampering. One of the

commonly used technique in many research works is DCT block based JPEG compression analysis. It is a popular technique for forgery detection in coding phase.

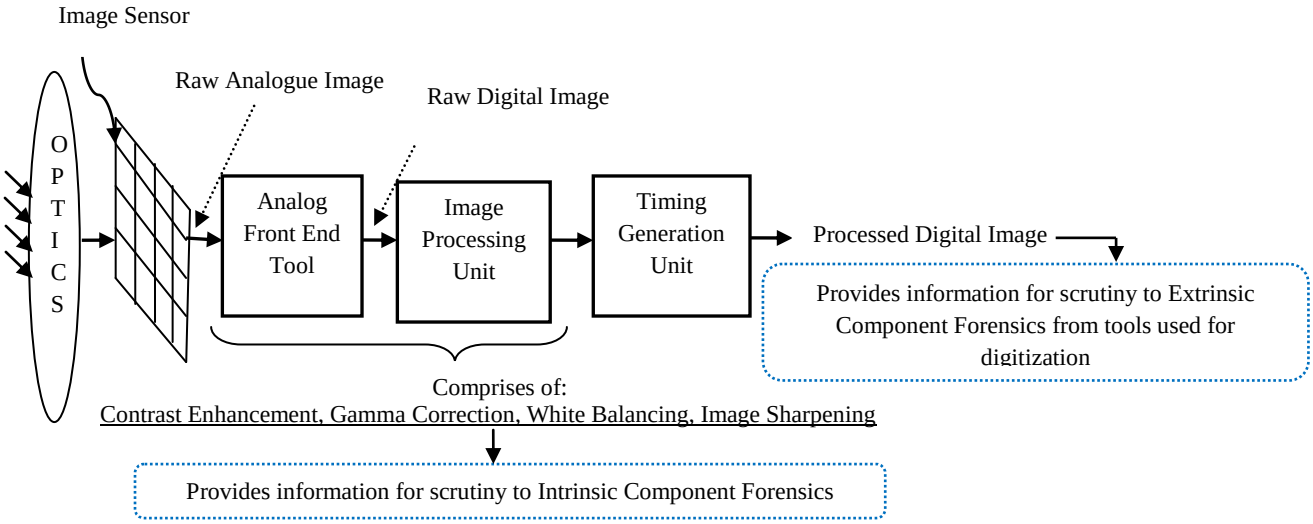

Figure 1: Block Diagram emphasizing Imaging Process as a Root for Component Forensics

Techniques such as the one discussed, forms the part of intrinsic component forensics which can be judged from the figure (1).

The next phase includes processing the generated image to enhance its features by using special editing software and tool. The processing employed over the obtained image leave typical traces which define fingerprint editing. This comes under the part of extrinsic component forensics of which passive image tampering detection is a sub-branch. The branch aims at inspection of tampering detection of images. Active image tampering detection uses previous traces for source identification.

6. Analogue versus Digital Images

In a broad sense, the images recorded on film, till recent, are grouped as analogue images. These can be characterized by color levels and brightness though low in comparison to digital images. Figure (2) represents analogue image versus digital images. Analogue images are of continuous form. Digital images use electronic charge to record impulses of light. They are formed from several number of picture elements called pixels which are the intersection of rows and columns of image matrix used to carry information such brightness and color. Digital images are discontinuous in nature but the resolution factor being very large, this quality becomes rarely noticeable.

In past, digital photography was only supposed to scan analogue prints and negatives into pixel files for image enhancements. But, the recent stories exhibit complete dependency of some fields like medical imaging, space research areas and wild life research on digitization. The dependency factor led to fast development in processing tools, software and digitization hardware as a way hindering security issues. Human subjects suffer from difficulty in distinguishing photographic images over photorealistic images generated by computer graphics.

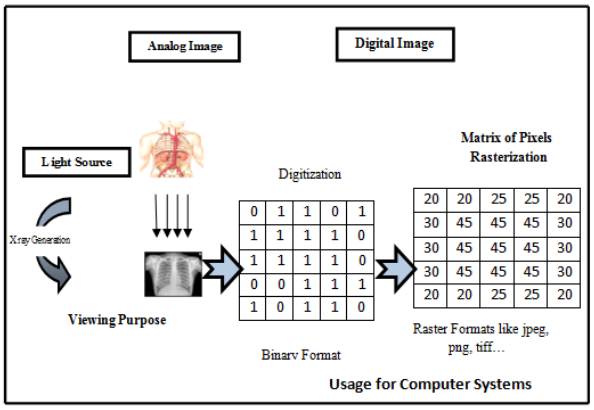

Figure 2: Diagram showing digitization of Analogue Image

7. State-of-the-Art: Part-II

In this section, we discuss various methods for implementing security attributes over source image. Studying the same, we propose a schema emphasizing total protection. Many types of security structures presented recently have been assessed and clustered. A model highlighting total protection has been framed. Here, we present the key attributes as levels of the security. We discuss the proposed State-of-the Art in the section below.

7.1 Generic Schema for Diverse Security Techniques

The schema of figure (3) below focuses on total security issue when the image is subjected for digitization. We treat security attributes as phases of employing protection at various levels of image creation to preliminary and infinitesimal components of image. Researches till date have shown about the interest for security only over certain attributes like integrity wherein watermarking scheme, authentication proving hash based key exchange has been individually implemented. We propose a scheme to provide all the key attributes of security namely the confidentiality, integrity and authentication jointly in our construct.

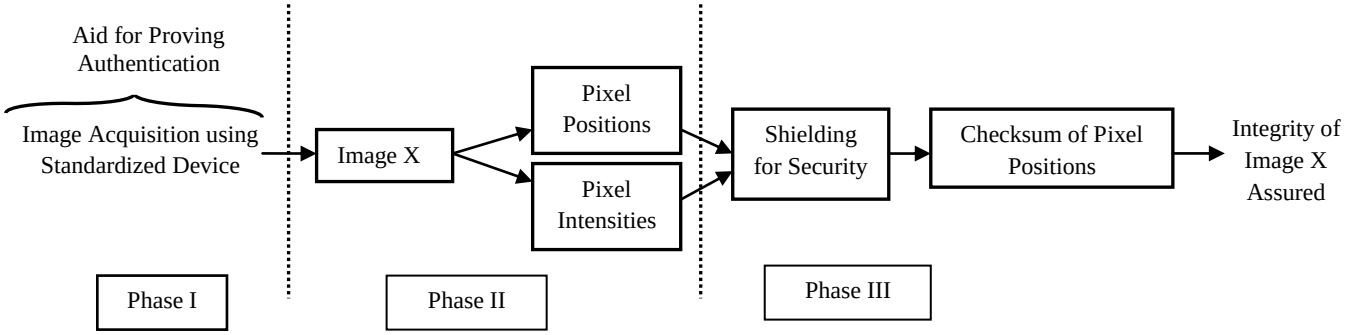

Figure 3: Generic Schema for Diverse Techniques of Information Security over an Image

Figure (3) illustrates the proposed schema which emphasizes implementation of security to be employed at each level in the process of digitization. The position and intensity are the infinitesimals of a digital image. The security attributes have been implemented in stages for shielding the image. The proposed schema supports intrinsic component forensics (ICF) under the fact that the former legally depends on extrinsic component forensics (ECF). The integrity factor decides correct identification of source. As can be analyzed from figure (1), constructive implementation of integrity is shown right from acquisition stage. Source identification is bestowed to ICF which if proven correctly will assure integrity component from the proposed system.

The other two attributes namely, authentication and confidentiality have been implanted after post-acquisition stage which comprises of out-camera processing using various images editing software. Extrinsic component forensics depends on stages succeeding post-acquisition. The schema is designed to help extrinsic component forensic. Furthermore the schema also emphasizes implementing the security structures at various levels in the image development stage wherein position and intensity being the basis infinitesimals of the image.

7.2 Image Editing versus Manipulation

The key motive for image editing includes image enhancements and compression for storage purpose. Digital software provides various functions like histogram, sharpening, color changing, and many more for the purpose of enhancement. Image manipulation is the application of few of these techniques for creating fantasy, glamour or delusion. A typical example of image manipulation can be photo retouching as shown in the picture (a). Such manipulations are not considered as forgery. These can be better grouped as fake image. Forged images are the attempts of malicious image editing process. The Intruder, here, aims at changing the semantic contents to alter the meaning of the attacked portion of the image. Hence, we justify that forgery can be created only from attack. The images in picture (a) thus can be termed as manipulated images.

7.3 Categorization of Attacks

7.3.1 Photomontage

Digital image forensics aim at detection of photomontage based attacks, the task of which is governed by passive image forensics. Image composition has been used as a construct for forgery creation by using features of composition like cutting and joining in a way such that the action remains imperceptible to the spectator, the resultant of which is called duplicated or cloned image. Image Splicing is a construct for dividing the multiple image file into individual component image file. Due to the ease of this technique, intruders have been exploiting this concept widely for changing the contents of the image. Healing is a construct is used to perform copy-by-replace action on pixels. By using this construct, pixels belonging to uneven textural regions of an image are replaced by cloned pixels of even textural regions. On a large scale, composition, splicing and healing have been used for creating forged images.

7.3.2 Semantic Alterations

Sometimes, depending on the type of the image, it may have key information may be present not objects as components but on other features. More precisely, some images show features to be interdependent rather than objects. Image Forensic Science depends on Statistical reasoning, Fuzzy logic Science and texture analysis to interpret the interdependency of semantic contents of the image. Also many researches exhibit autocorrelation as a better construct in detection of such attacks based on embedding semantic contents. Here, we show two pictures showing manipulations generated from image editing constructs. Picture (a) shows normal manipulations done to enhance the image for objective of glamour whereas picture (b) shows an example of copy-move forgery using composition as an editing construct.

(a) (b)

Picture (a) shows an example of Image Manipulation by Photo Editing.

Picture (b) shows an example of Copy-move forgery. The two photographs are combined. Sharp-eyed journalists at another paper spotted Iraqis at left who were repeated in the picture. These photos appeared in "The Washington Post: Manipulating Truth, losing Credibility" by Frank Van Riper, November 2013. [69]

7.4 IMAGE SECURITY TECHNIQUES

The image may have active or passive approaches of providing security. In an active image security process statistical information using various constructs is embedded/stuffed/associated to the image by techniques like hashing, watermarking and signature based approaches. These approaches ease the task of forensics by providing sensitivity to image characteristics. The image can be linked to its origin which becomes the preliminary stage for forgery identification. We discuss various constructs under the active approaches used so far in this section.

7.4.1 Types of Security Methods

Various techniques have been used for image security over the past decades. A lot many new approaches have gained success over those used in the past. All of these methods are discussed as this section.

7.4.1.1 Cryptographic Security

Cryptographic measure like challenge-response models, message authentication code (MAC) schemes, cryptographic hashes are commonly used approaches but they hardly proved for security. These constructs fail to provide integrity, the examples of which show intrusions that inject and incorporate unintended data to the image under transmission which itself proves image tampering. Any image transmitted over the channel has been proved to be used as a means of secret communication which symbolizes a drawback of cryptographic ways of authentication.

7.4.1.2 Watermarking

Watermarking was the default way to provide protection which legally provided integrity and authentication. Researches so far judge watermarking as part of protection more over analogue images rather on digital ones. In [1] Min-Jen Tsai emphasized visible watermarking for content authentication is presented. In [2] Lihua Tian et al. implemented watermarking for synchronous image authentication. M.P. Queluz in [3], emphasized schemes for evaluation of integrity of images and video using watermark and labeled approaches have been discussed. Gwo-Jong Yua, Chun-Shien Lub, Hong-Yuan Mark Liao in [4] presented a cocktail watermarking system. Three categories of digital watermarks like robust, fragile and semi-fragile have been implemented using vivid algorithms and constructs. Due to advancements of technologies, it has been proved that the said construct is prone to intrusion easily spoiling its popularity now over digital platforms.

7.4.1.3 Robust Watermarking

Most images and documents need to protect for ownership, copyrights and patents. Researchers have proven watermarking type called robust watermarks especially for such aspects. The robustness makes them imperceptible to various modifications like filtering and cropping.

7.4.1.4 Fragile Watermarking

Middle ages of digitization use watermarking by implanting fragility feature. It provided sensitivity to the image for certain post-processing operations. It is prone to wrecking easily. A set of minute changes can inadvertently modify it. The key objective of providing sensitivity is established by using stipulated procedures like the ones used in [5-11]. Authors in ref. [5, 9] highlight chaotic maps which themselves by property are sensitive to certain initial values manipulated on them, thereby providing fragility. Wei-Che Chen, Ming-Shi Wang in [6], describe a fuzzy c-means clustering, wherein fuzzy constraints defined over certain range of pixel bound to unique clusters initiating sensitivity factor. Chunlei Li et al in [7] emphasized a dual redundant ring structure making watermark of one block be hidden in the 1-LSB of another and copy of the watermark in 2-LSB of another block whose position is determined by the previous block is implemented. Luis Rosales-Roldan et al, in [8], half toning is used for association of sensitivity. Dariusz Bogumi in [10] presented asymmetric public-key watermarking scheme for static images was implemented wherein cryptographic method of private & public key for embedding and decoding the watermark has been used. Here the watermark is used as a synchronization template. Shan Suthaharan in [11] emphasized fragile watermarking algorithm for image authentication and tamper detection over gradient image. It provided more security to certain attacks like vector quantization attack.

7.4.1.5 Semi-Fragile Watermarking

Potential of semi-fragility bears inadvertent alterations but is fragile against deliberate modifications. Many researches under semi-fragile watermarking like the one in [12], as proposed by Xunzhan Zhua, Anthony T.S. Hob, Pina Marziliano exhibit Irregular sampling based restoration over semi-fragile scheme. The method provides restoration of tampered portions. Xiaojun Qi, Xing Xin in [13], states usage of non-traditional quantization method for robustness against incidental attacks and sustains fragility against malicious attacks.

7.4.1.6 Hybrid Watermarking

F. Deguillaume, S. Voloshynovskiy, T. Pun in [14] proposed a scheme which combined both the approaches of fragile and semi-fragile. The scheme provides both copyright protection and tamper proofing to give robust and superior performance.

7.4.1.7 Watermark Chaining

Huiping Guo, Yingjiu Li, Sushil Jajodia in [15], the authors implemented chaining of watermarks wherein the data were divided to form groups of synchronization points which insisted modifications made to one group affected other two groups. Watermarks are embedded unique to each group to save communications bandwidth henceforth making flexible the process of detection and location of modifications if any made to the data stream.

7.4.1.8 Hierarchical Watermark

Phen Lan Lina, Chung-Kai Hsiehb, Po-Whei Huangin [16], highlight inspection of tampering using a hierarchical structure. It uses mechanisms of parity check and comparison between average intensities for detection of tampering at various levels.

7.4.1.9 Dual Watermarking

Sometimes watermarking can be implemented as a combination of both visible and invisible watermark depending on regions of where integrity needs to be maintained. Qingtang Sua in [17, used dual watermarking using optimized compensation based on singular value decomposition specifically for color images. Yanjiao Shia et al, [18] highlight dual watermark for video authentication. Fre´de´ ric Lusson et al, in [19] implemented digital watermark by technique of exploiting the color spaces.

7.4.1.10 Content Based Authentication

Xiaofeng Wanga et al, in [20], used forensic signature for content authentication on basis of adaptive Harris corner detection algorithm for extraction of feature points. The statistics of feature point is formulated into forensic signature.

7.4.1.11 Hash Based Image Authentication

In [21], Jillian Cannons and Pierre Moulin emphasized hash based scheme for authentication, robust against content-preserving manipulations. The basis is bestowed upon observations against rotation invariant image pixels of each ring. Marco Tagliasacchi, Giuseppe Valenzise, and Stefano Tubaro in [22], highlighted the hash method for detection of sparse tampering especially in the context of generating first

the random projections. This kind of authentication schema has also been proposed for human detection methods.

7.4.1.12 Hamming Code Based Authentication

Chi-Shiang Chan in [23], emphasized authentication scheme using hamming code generation algorithm. The method generates hamming code from parity of pixels and stuffs them in other pixels. Authentication is proved by correct predicted of bit and parity check bits before recovery.

7.4.1.13 Fusion based Authentication

Learning the hurdles of older approaches as the ones discussed above, researches have laid platform for fusion based authentication. Usually this construct gained a rapid strength for biometric based systems wherein multiple images need to be authenticated under the major one. In [24]-[33], many approaches implemented fusion as authentication. Fusion of images is formed by collecting useful information from various regions of all images under the scene. The resultant image is the fused image pertaining to those information sets which can jointly be applied suitable authentication approach. Image fusion is the feature basically used for merging the gray-level high-resolution panchromatic image along with multispectral low-resolution color image. In [25], Chin-Chuan Han implemented a coarse-to-fine strategy for hand-based personal authentication as a basis of extracted ROI from palm-print features along with hand geometry. Also in [34], K.Somasundaram and N.Palaniappa have implemented cryptographic fusion based authentication by using fusion of personal ID along with blind and zero watermarking. Yi Zheng Goh, Andrew Beng Jin Teoh, Michael Kah Ong Goh in [35], presented wavelet based fusion scheme for face verification. Jun-ying Gan, Yu Liang in [36], implemented Face and Iris authentication for multimodal biometrics. It uses 2DFLD analysis for implementation. Dakshina Ranjan Kisku et al, in [37] presented an in-depth working over score-level fusion algorithms used specially in biometric authentication systems. The procedure gives a deep idea of implementing fusion in biometric and personal ID authentications.

7.4.1.14 Visual Cryptography

Recently, many researchers have placed visual cryptography as an authentication scheme. It is a secret sharing scheme by which secret image can be scrambled to form multiple shares, each having no independent disclosure. It has always been proved to provide an extra layer of security. P.S.Revenkar, Anisa Anjum, W .Z.Gandhare in [38] implemented method for Human identity verification. The authors used the concept of visual shares for authentication. Biometric image templates within a database were utilized as shares to provide authentication based on visual cryptography.

7.4.1.15 Neural Network

The tool for intrusion detection has always been proven by neural networks because of the properties such as random similarity, parameter sensitivity, diffusion property, confusion property, one-way property. Shiguo Lian in [39], proposed a method for multimedia content authentication. A secret parameter is produced from neural network when subjected with authentication code and a unique key. Authentication is proven when the said network produces the computed authentication code over secret parameter and the key fed to it. The system overall is a low-cost architecture. Chih-Hung Lin, Tzung-Her Chen, in [40], emphasized BCH based image block coding as an authentication scheme. The Bayer Pattern technique is applied as a tamper therapy. Piyu Tsaia ,Yu-Chen Hub, Chin-Chen Changa in [41] implemented set partitioning technique for authentication.

7.4.1.16 Steganography

Steganography from past decades have been implemented as a means of information hiding. But fast researches over the subject of steganography have been recently implementing it as a tool for integrity & protection. S.M.Elshoura, D.B.Megherbi in [42], used the Tchebichef moments of the carrier image to hide the watermarked image along with other hidden information. The scheme implements authentication as well as integrity. Authors in [43-50], presented vivid techniques of image information hiding. Hiding in edges, LSBs, by Pixel value differencing (PVDs) have been popular techniques and gaining platform as a means of secret communication to prove a tool for authentication and integrity. LSB based approaches lower the image quality. A research in [48] presented by Cheng-Hsing Yang shows technique using inverted pattern to hide in LSBs to improve quality of stego-gramme. Suresh N. Mali, Pradeep M. Patil, Rajesh M. Jalnekar in [50], present a robust hiding technique using image adaptive energy thresholding to provide potency against intentional and unintentional attacks.

7.4.1.17 Other Security Constructs

Guangjie Liu et al in [51] presented a passive authentication scheme based on Hu moment which makes usage of circular blocks. Using of the blocks of circular shape stimulates detection in terms of rotational variations here in this scheme. The authors proposed this scheme as passive authentication which is also termed to be known digital forensic into the context that no information can be externally associated or may be utilized for authentication of the image. The authentication attribute is proven passively. Jun-Chou Chuang, Yu-Chen Hu in [52], presented an approach for authentication by detecting illicit alterations using index table for non-overlapping index blocks on compressed images.

7.5 Active Approaches for Image Tampering Detection

Detection of image tampering on architectures using active approaches for protection provides a step for investigating about the image origin. Accordingly, a construct for tampering detection over the one used for security method is used to build the approach. But though providing robustness to attack, these may exhibit clues for intruders and therefore, various types of tampering detection schemes over possible and known attacks have been discussed in the table I. Figure (4) below, illustrates generic schema for detection of tampering when active approaches were used for image security. The major problem in the development of this platform lies on the fact that a generalized tampering detection algorithm to work on all possible constructs of active methods of protection (like watermarking, hashing association, signature-based) cannot be used for correct identification, localization, recovery of tampered regions of image.

The working of the generic schema for active tampering detection is described below. Figure (4) shows the operational model for it.

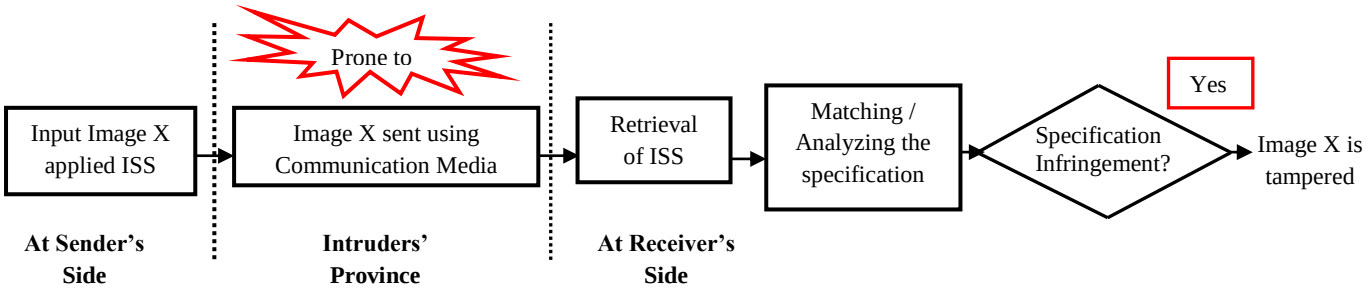

Figure 4: Generic Schema for Active Image Tampering Detection

Methodology

1. The Input image X is shielded with a certain ISS.

2. It is sent to the receiver of the image over the channel. The Channel here can be any electronic media.

3. To check whether the security is breached or the image is infringed, the receiver will cross verify with the information associated with the image X.

4. The receiver retrieves the associated information from the ISS applied since the semantics of applied ISS is known to the receiver.

5. An analysis for the match is performed, any violation in which justifies tampering of the image X.

6. A proof of tampering is assured from the information of standardized tools which were used in the generation process of Image X.

The commonality of retrieving the associated information for matching the parameters caused this branch to be known as active tampering detection. Dependency of generation of Tamper Detection algorithm lies on the technique used for security. Henceforth, the field is gaining more importance for new researches.

7.6 Passive Image Tampering Detection Techniques

Passive tampering detection is a contradictory approach to active approach wherein no information either about the source or the image metadata is associated to the image. The investigation process remains blind. Also, the image under investigation does not have any actively embedded construct for security to it. Henceforth, only measures for scrutiny are i) Identification of Source and ii) Localization of Tampered regions. Passive Detection of tampering is purely based on investigating the features or characteristics of the image and analyzing the fingerprints, footprints in identification of source. The method used for passive tampering detection is dependent on the image under scrutiny; due to this fact many researches under this field have shown various schemata.

Table I in the appendix, gives a brief analysis on attacks and corresponding passive tampering detection schemes. Figure (5) provides a detail outline of techniques used for aforementioned approaches. As can be judged from the schema stated, vivid constructs can be generated for analysis of the image under subjection from listed features that bind it to give a certain semantic meaning through it.

Passive Detection of tampering is purely based on investigating the features or characteristics of the image. As in active approaches discussed above, no information in any kind is associated or linked the image under analysis. Such analysis is also known as blind forensics. Therefore, forensic investigations are bestowed upon source identification and forgery detection. Passive Forensics is dependent on image acquiring, image statistics and traces of forgery creation as the key objectives from image under analysis, which becomes the reason for burgeoning platform for research. Figure (5) introduces a generic schema for passive detection of image tampering. As shown in the illustration, no approach for security construct is known at the time of passive forensics.

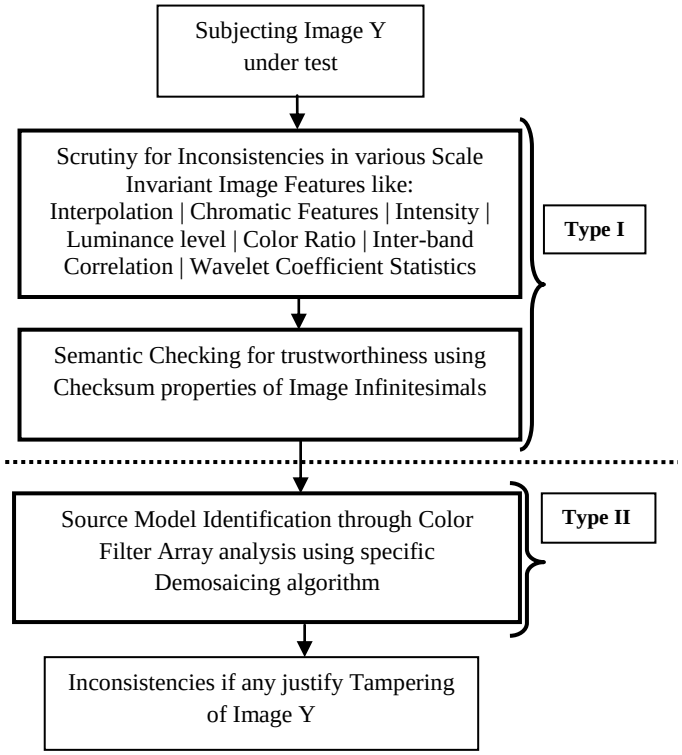

Figure 5: Generic Schema for Passive Image Tampering Detection

The image when subjected under scrutiny undergoes blind analysis. An appropriate schema for a certain type of scrutiny techniques have been discussed in table I and table II in the appendix. Mostly the forgery detection is based on two types of techniques.

7.6.1 Deviations in Image Features

Most techniques are based on analyzing variations in set of selected features. Usually if an image had underwent manipulations, it is ought to have deviations and dissimilarities. All methods which rely on analyzing such deviations are categorized as type I.

These methods aim to find out whether the image had underwent certain type of processing such as image resizing, compression and many other operations. Also, there are some properties which remain invariant to certain operations hence

can be used to detect alterations done to the image. Various methods have been used to detect a certain type of forgery. Such as inconsistencies between correlations of pixels is a technique to detect image resizing. Copy-paste forgeries have been traced by exhaustive search and analysis of correlation parameters. But the method is proven to exhibit unsatisfactory results. Another method which uses sampling of DCT coefficients from overlapping blocks has been proven to detect copy-paste forgeries precisely. Figure (5) provides an elaborative description of type I and type II methods.

7.6.2 Variations in Scrutiny of Acquisition Process

The image acquisition process introduces certain characteristics in the acquired image which can be used for detection of image tampering. These characteristics remain uniform over the acquired image. A consistent distribution of such characteristics across the image could be used for precise identification of the source. Inconsistency in the examination of these characteristics determines tampering and can thus be localized. A lot many methods which belong to this category have proven these facts one of which is color filter array interpolation. In this method, the pattern of CFA and interpolation filter is first estimated. A demosaiced image is then constructed which is compared with the image itself. The coefficients of the linear part are obtained by modeling it using deconvolution. A classifier is designed for tampering detection. It then compares filter coefficients with reference pattern obtained from direct output of camera. Other methods include analyzing inconsistencies in sensor pattern noise extracted from the image and inconsistencies in lateral chromatic aberrations. More methods like analyzing fingerprint image matching to detect inconsistency and examination of components of digital camera pipeline have also been proven successful.

7.7 Brief Mathematical Assessment for Passive Image Tampering Detection

The detection of image tampering passively restricts to image quality feature analysis as described in figure (5). A digital image is an array of M X N pixels, the process of scrutiny rely on analysis of various image quality factors like moments, cross-correlation, structural content, local mean and standard deviation etc. Let 'Q' denote a set of these features.

When on examination a certain set of image quality feature can be taken from the group of image features. The inspection of forgery relies on matching this set of features with the features of suspected regions. But since some kinds of forgeries are invisible to human visual system so a decision rule for semantic analysis can be formulated which proves the forgery attempts. There are certain statistical changes which cannot be termed as forgeries so all factors based on statistics cannot be formulated into forgery decision. We therefore formulate a decision rule for image tampering.

Decision Rule: The Claimant externally declares a set of features that justify genuineness of the semantic contents of the image. Let 'F' denote the set of these features.

An infringement in the analysis of elements of the set 'F' proves forgery of the image under test. We present an Algorithm to work for the same.

Segmentation Principle: Let 'T' be the image under test so 'T_f' denotes regions segmented on basis of the decision rule.

1. The test image is segmented into suspected regions which form a set of 'Rs' using the segmentation rule.

2. For all regions in the set R_s, each region is divided into blocks to form a set of all blocks of R_s. Let 'B_{rs}' denote these blocks.

3. For each block in the set B_{rs}, performing inspection on image quality feature chosen from 'Q' as per step 4.

4. Computing 'Q_i' for each block in B_{rs}. Appling suitable transformation to obtain numeric values.

5. Formulating feature vector of size p*q wherein 'p' denotes total number of pixels in each block and 'q' denotes corresponding quality feature computed in step 4, collecting them into "Bag-of- B_{rs}".

6. Repeating steps 2-5, now for all blocks in the set

'T - Tf' that is,

6.1: Let '$R_{\hat{s}}$' denotes regions not in the set 'R_s'.

6.2: Dividing each region in the set '$R_{\hat{s}}$' to form blocks. Let 'B`' denote these set of blocks.

6.3: Computing 'Q_i' for each block in B` by same procedure as in step 4 and obtaining numeric values of each.

6.4: Formulating feature vectors by the same procedure as of step 5. Collecting them into "Bag-of-B`".

7. Let 'B+' denotes all blocks from "Bag-of- Brs" and "Bag-of-B`".

8. Formulate training data set $\{a_i, b_i\}$ for i = 1, 2....n where $a_i \in$ B+ and bi $\in \{-1, 1\}$ such that

$$f(a_i) = \begin{cases} \geq 0 & b_i = +1 \\ < 0 & b_i = -1 \end{cases}$$

This differentiates the forged blocks from non-tampered blocks.

9. Correct Classification will produce $b_i f(a_i) > 0$.

8. DISCUSSION AND CONCLUSION

Detection and recovery are the two major domains under image forensics. Chuan Qin et al, in [59], proposed the method for tamper recovery based on VQ indexing. Pradyumna Deshpande, Prashasti Kanikar in [62], considering pixel as the key feature, various techniques under the same have been discussed. Ashwin Swaminathan, Min Wu and K. J. Ray Liu in [63], present blind deconvolution as a technique for tampering identification. M. Barni and A.Costanzo in [64] show implementation of fuzzy approach as a measure of inconsistency in detection of tampering.

After in depth assessment of image forensics and study of digital image from creation to protection, we now derive the conclusion. Digital photography has seen to be successful in replacing analogue photography. Advancements in image editing softwares have made the task of forgery creation straightforward. The issues under image forgery detection have acquired importance. Despite implanting active constructs for image security, advancement in technology, have always made a provision for intrusions which breach these constructs leading to forgery. Recently, several passive forgery detection methods have been proposed. But as per our assessment in previous sections, we learn that a common method cannot be used for passive image forensics. The root

of forgery creation has to be inspected to detect tampering passively. Henceforth, source identification has become a topic of research. Various techniques for localizing tampered regions passively have been recently proposed which are discussed in the table I and II. Many approaches for localizing tampered blocks based on study of features like moments, pixel value differencing, geometric features have been proposed. Tamper recovery is a very difficult issue in context of digital forensics and acquiring scope for research now a day. Domains like machine learning, computer graphics, data mining algorithms like clustering and classification algorithms signal processing tools have proven to be effective solutions for passive detection of image tampering.

9. ACKNOWLEDGMENT

We would like to sincerely thank Prof. Hany Farid for his worthwhile work in Image Analysis and Human perception.

10. REFERENCES

[1] Min-Jen Tsai, "A visible watermarking algorithm based on the content and contrast aware (COCOA) technique ", J. Vis. Commun. Image R. 20 (2009) 323–338 http://dx.doi.org/10.1016/j.jvcir.2009.03.011

[2] Lihua Tian , Nanning Zheng, Jianru Xue, Ce Li, Xiaofeng

Wang, "An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection", Signal Processing: Image Communication 26 (2011)427–437 http://dx.doi.org/10.1016/j.image.2011.06.001

[3] M.P. Queluz, "Authentication of digital images and video: Generic models and a new contribution", Signal Processing: Image Communication 16 (2001) 461-475

[4] Gwo-Jong Yua, Chun-Shien Lub, Hong-Yuan Mark Liao, "A message-based cocktail watermarking system", Pattern Recognition 36 (2003) 957 – 968 http://dx.doi.org/10.1016/S0923-5965(00)00010-2

[5] Sanjay Rawat, Balasubramanian Raman, "A chaotic system based fragile watermarking scheme for image tamper detection", Int. J. Electron. Commun. (AEÜ) 65 (2011) 840–847 http://dx.doi.org/10.1016/S0031-3203(02)00106-1

[6] Wei-Che Chen, Ming-Shi Wang, "A fuzzy c-means clustering-based fragile watermarking scheme for image authentication", Expert Systems with Applications 36 (2009) 1300–1307 http://dx.doi.org/10.1016/j.aeue.2011.01.016 http://dx.doi.org/10.1016/j.aeue.2011.02.001

[7] Chunlei Li, Yunhong Wanga, Bin Maa, Zhaoxiang Zhang, "A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure", Computers and Electrical Engineering 37 (2011) 927–940 http://dx.doi.org/10.1016/j.eswa.2007.11.018

[8] Luis Rosales-Roldan , Manuel Cedillo-Hernandez , Mariko Nakano- Miyatake , Hector Perez-Meana , BrianKurkoski, "Watermarking-based image authentication with recovery capability using halftoning technique", Signal Processing: Image Communication 28 (2013)69–83 http://dx.doi.org/10.1016/j.image.2012.11.006

[9] Xiaojun Tong ,YangLiu, MiaoZhang, YueChen, "A novel chaos-based fragile watermarking for image tampering detection and self-recovery", Signal Processing: Image Communication 28 (2013)301–308 http://dx.doi.org/10.1016/j.image.2012.12.003

[10] Dariusz Bogumi, "An asymmetric image watermarking scheme resistant against geometrical distortions" Signal Processing: Image Communication 21 (2006) 59–66 http://dx.doi.org/10.1016/j.image.2005.06.005

[11] Shan Suthaharan, "Fragile image watermarking using a gradient image for improved localization and security", Pattern Recognition Letters 25 (2004) 1893–1903http://dx.doi.org/10.1016/j.patrec.2004.08.017

[12] Xunzhan Zhua, Anthony T.S. Hob, Pina Marziliano, "A new semi-fragile image watermarking with robust tampering restoration using irregular sampling", Signal Processing: Image Communication 22 (2007) 515–528

[13] Xiaojun Qi, Xing Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication", J. Vis. Commun. Image R. 22 (2011) 187–200 http://dx.doi.org/10.1016/j.jvcir.2010.12.005

[14] F. Deguillaume, S. Voloshynovskiy, T. Pun , "Secure hybrid robust watermarking resistant against tampering and copy attack", Signal Processing 83 (2003) 2133 – 2170 http://dx.doi.org/10.1016/j.jvcir.2010.12.005

[15] Huiping Guo, Yingjiu Li, Sushil Jajodia, "Chaining watermarks for detecting malicious modifications to streaming data", Information Sciences 177 (2007) 281–298 http://dx.doi.org/10.1016/j.ins.2007.02.020 http://dx.doi.org/10.1016/j.ins.2007.02.043 http://dx.doi.org/10.1016/j.ins.2006.03.014

[16] Phen Lan Lina, Chung-Kai Hsiehb, Po-Whei Huang, "A hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition 38 (2005) 2519 – 2529 http://dx.doi.org/10.1016/j.patcog.2005.02.007

[17] Qingtang Sua, Yugang Niu, Yongsheng Zhao, Shan Panga, Xianxi Liuc, "A dual color images watermarking scheme based on the optimized compensation", Int. J. Electron. Commun. (AEÜ) 67 (2013) 652– 664 http://dx.doi.org/10.1016/j.aeue.2013.01.009

[18] Yanjiao Shia, Miao Qia, Yugen Yia, Ming Zhanga, Jun Konga, "Object based dual watermarking for video authentication", Optik 124 (2013) 3827– 3834 http://dx.doi.org/10.1016/j.ijleo.2012.11.078

[19] Fre´de´ ric Lusson, KarenBailey, MarkLeeney, KevinCurran, "A novel approach to digital watermarking exploiting color spaces", Signal Processing 93 (2013) 1268–1294 http://dx.doi.org/10.1016/j.sigpro.2012.10.018

[20] Xiaofeng Wanga, Jianru Xue, Zhenqiang Zheng , Zhenli Liu , Ning Li, "Image forensic signature for content authenticity analysis", J. Vis. Commun. Image R. 23 (2012) 782–797 http://dx.doi.org/10.1016/j.jvcir.2012.03.005

[21] Jillian Cannons, and Pierre Moulin, "Design and Statistical Analysis of a Hash-Aided Image Watermarking System", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 10, OCTOBER 2004 1393

[22] Marco Tagliasacchi, Giuseppe Valenzise, and Stefano Tubaro, "Hash-Based Identification of Sparse Image Tampering" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 18, NO. 11, NOVEMBER 2009 2491

[23] Chi-Shiang Chan, "An image authentication method by applying Hamming code on rearranged bits", Pattern Recognition Letters 32 (2011) 1679–1690 http://dx.doi.org/10.1016/j.patrec.2011.07.023

[24] Gemma Piella, “A general framework for multiresolution image fusion: from pixels to regions”, Information Fusion 4 (2003) 259–280 http://dx.doi.org/10.1016/S1566-2535(03)00046-0

[25] Chin-Chuan Han , “A hand-based personal authentication using a coarse-to-fine strategy”, Image and Vision Computing 22 (2004) 909–918 http://dx.doi.org/10.1016/j.imavis.2004.05.008

[26] Maycel-Isaac Faraj , Josef Bigun, “Audio–visual person authentication using lip-motion from orientation maps”, Pattern Recognition Letters 28 (2007) 1368–1382 http://dx.doi.org/10.1016/j.patrec.2007.02.017

[27] Andrew Teoh Beng Jina, David Ngo Chek Linga, Alwyn Goh, “Biohashing: two factor authentication featuring fingerprint data and tokenized random number”, Pattern Recognition 37 (2004) 2245 – 2255 http://dx.doi.org/10.1016/j.patcog.2004.04.011

[28] Loris Nanni, Alessandra Lumini, “Fusion of color spaces for ear authentication”, Pattern Recognition 42 (2009) 1906 – 1913 http://dx.doi.org/10.1016/j.patcog.2008.10.016

[29] Hyun-Ae Park, Kang R young Park, “Iris recognition based on score level fusion by using SVM”, Pattern Recognition Letters 28 (2007) 2019–2028 http://dx.doi.org/10.1016/j.patrec.2007.05.017

[30] Jiansheng Chen, Yiu-Sang Moon , Ming-Fai Wong , Guangda Su, “Palmprint authentication using a symbolic representation of images”, Image and Vision Computing 28 (2010) 343–351 http://dx.doi.org/10.1016/j.imavis.2010.03.003 http://dx.doi.org/10.1016/j.imavis.2009.04.012

[31] Ajay Kumar, David C.M. Wong, Helen C. Shen, Anil K. Jain, “Personal authentication using hand images”, Pattern Recognition Letters 27 (2006) 1478–1486 http://dx.doi.org/10.1016/j.patrec.2006.02.021

[32] Girija Chetty, Michael Wagner, “Robust face-voice based speaker identity verification using multilevel fusion”, Image and Vision Computing 26 (2008) 1249–1260 http://dx.doi.org/10.1016/j.imavis.2008.02.009

[33] Rongrong Nia, Qiuqi Ruana, H.D. Cheng, “Secure semi-blind watermarking based on iteration mapping and image features” Pattern Recognition 38 (2005) 357 – 368 http://dx.doi.org/10.1016/j.patcog.2004.08.006

[34] K.Somasundaram, N.Palaniappan, “Cryptographic Image Fusion for Personal ID Image Authentication”., available on http://www.ruraluniv.ac.in/papers/89.pdf

[35] Yi Zheng Goh , Andrew Beng Jin Teoh , Michael Kah Ong Goh, “Wavelet local binary patterns fusion as illuminated facial image preprocessing for face verification”, Expert Systems with Applications 38 (2011) 3959–3972 http://dx.doi.org/10.1016/j.eswa.2010.09.057

[36] Jun-ying Gan , Yu Liang, “A Method for Face and Iris Feature Fusion in Identity Authentication”, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006 135

[37] Dakshina Ranjan Kisku, Ajita Rattani, Phalguni Gupta, Jamuna Kanta Sing, C. Jinshong Hwang, “Human Identity Verification Using Multispectral Palmprint Fusion”, Journal of Signal and Information Processing, 2012, 3, 263-273 http://dx.doi.org/10.4236/jsip.2012.32036

[38] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, “Secure Iris Authentication Using Visual Cryptography”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010

[39] Shiguo Lian, “Image Authentication Based on Neural Networks” available on arxiv.org/ftp/arxiv/papers/0707/0707.4524.pdf

[40] Chih-Hung Lin, Tzung-Her Chen , Chun-Wei Chiu, “Color image authentication with tamper detection and remedy based on BCH and Bayer Pattern”, Displays 34 (2013) 59–68 http://dx.doi.org/10.1016/j.displa.2012.11.004

[41] Piyu Tsaia ,Yu-Chen Hub, Chin-Chen Changa, “Using set partitioning in hierarchical trees to authenticate digital images”, Signal Processing: Image Communication 18 (2003) 813–822 http://dx.doi.org/10.1016/j.image.2003.06.001

[42] S.M.Elshoura, D.B.Megherbi, “A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments”, Signal Processing: Image Communication 28 (2013)531–552 http://dx.doi.org/10.1016/j.image.2012.12.005

[43] Wien Hong, “Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique”, Information Sciences 221 (2013) 473–489 http://dx.doi.org/10.1016/j.ins.2012.09.013

[44] Cheng-Hsing Yang, “Inverted pattern approach to improve image quality of information hiding by LSB substitution”, Pattern Recognition 41 (2008) 2674 – 2683 http://dx.doi.org/10.1016/j.patcog.2008.01.019

[45] Chang-Lung Tsai, Huei-Fen Chiang, Kuo-Chin Fan, Char-Dir Chung, “Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism”, Pattern Recognition 38 (2005) 1993 – 2006 http://dx.doi.org/10.1016/j.patcog.2005.03.001

[46] Suresh N. Mali, Pradeep M. Patil, Rajesh M. Jalnekar, “Robust and secured image-adaptive data hiding”, Digital Signal Processing 22 (2012) 314–323 http://dx.doi.org/10.1016/j.dsp.2011.09.003

[47] Da-Chun Wu, Wen-Hsiang Tsai, “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters 24 (2003) 1613–1626 http://dx.doi.org/10.1016/S0167-8655(02)00402-6

[48] Cheng-HsingYang, “Inverted pattern approach to improve image quality of information hiding by LSB substitution”, Pattern Recognition 41 (2008) 2674 – 2683 http://dx.doi.org/10.1016/j.patcog.2008.01.019

[49] Norman Poh, Samy Bengio, “Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication”, Pattern Recognition 39 (2006) 223 – 233 http://dx.doi.org/10.1016/j.patcog.2005.06.011

[50] Suresh N. Mali, Pradeep M. Patil, Rajesh M. Jalnekar, “Robust and secured image-adaptive data hiding”, Digital Signal Processing 22 (2012) 314–323 http://dx.doi.org/10.1016/j.dsp.2011.09.003

[51] Guangjie Liu, Junwen Wanga, Shiguo Lian, Zhiquan Wanga, “A passive image authentication scheme for detecting region-duplication forgery with rotation”, Journal of Network and Computer Applications 34 (2011) 1557–1565http://dx.doi.org/10.1016/j.jnca.2011.01.012 ; http://dx.doi.org/10.1016/j.jnca.2010.12.004

[52] Jun-Chou Chuang, Yu-Chen Hu, "An adaptive image authentication scheme for vector quantization compressed image", J. Vis. Commun. Image R. 22 (2011) 440–449 http://dx.doi.org/10.1016/j.jvcir.2011.03.011

[53] Hong-Jie He, Jia-Shu Zhang , Fan Chen , "Adjacent-block based statistical detection method for self-embedding watermarking techniques", Signal Processing 89 (2009) 1557–1566 http://dx.doi.org/10.1016/j.sigpro.2009.02.009

[54] Sergio Bravo- Solorio, Asoke K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localization and self- recovery capabilities", Signal Processing 91 (2011) 728–739 http://dx.doi.org/10.1016/j.sigpro.2011.01.022; http://dx.doi.org/10.1016/j.sigpro.2010.07.019

[55] Radu O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain", Measurement 46 (2013) 367–373 http://dx.doi.org/10.1016/j.measurement.2012.07.010

[56] Zhongwei He, WeiLu , WeiSun , JiwuHuang, "Digital image splicing detection based on Markov features in DCT and DWT domain", Pattern Recognition 45 (2012) 4292–4299 http://dx.doi.org/10.1016/j.patcog.2012.05.014; http://dx.doi.org/10.1016/j.patcog.2012.03.009

[57] Sergio Bravo-Solorio, Asoke K. Nandi, "Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics", Signal Processing 91 (2011) 1759–1770 http://dx.doi.org/10.1016/j.sigpro.2011.01.022; http://dx.doi.org/10.1016/j.sigpro.2010.07.019

[58] Guangjie Liu, Junwen Wang, Shiguo Lian, Yuewei Dai, "Detect image splicing with artificial blurred boundary", Mathematical and Computer Modelling 57 (2013) 2647–2659 http://dx.doi.org/10.1016/j.mcm.2012.09.012 http://dx.doi.org/10.1016/j.mcm.2012.09.019 http://dx.doi.org/10.1016/j.mcm.2012.12.006

[59] Yu Qian Zhaoa, Miao Liaoa, Frank Y. Shihb, Yun Q. Shic, "Tampered region detection of in painting JPEG images", Optik 124 (2013) 2487– 2492 http://dx.doi.org/10.1016/j.ijleo.2012.08.018

[60] Chuan Qin, Chin-Chen Chang , Kuo-Nan Chen, "Adaptive self-recovery for tampered images based on VQ indexing and inpainting", Signal Processing 93 (2013) 933–946 http://dx.doi.org/10.1016/j.sigpro.2013.03.036 http://dx.doi.org/10.1016/j.sigpro.2012.11.013

[61] Kyung-Su Kim, Min-Jeong Lee, Ji-Won Lee, Tae-Woo Oh, Hae-Yeoun Lee, "Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging", Computer Vision and Image Understanding 115 (2011) 1308–1323 http://dx.doi.org/10.1016/j.cviu.2011.05.001

[62] Xunyu Pan, Siwei Lyu, "Region Duplication Detection Using Image Feature Matching", IEEE Transactions on Information Forensics and Security, VOL. X, NO. X, XX 2010

[63] Pradyumna Deshpande , Prashasti Kanikar, "Pixel Based Digital Image Forgery Detection Techniques", Pradyumna Deshpande , Prashasti Kanikar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 539-543 539

[64] Ashwin Swaminathan, Min Wu and K. J. Ray Liu, "Image Tampering Identification using Blind Deconvolution", 1-4244-0481-9/06/C2006 IEEE

[65] M. Barni, A.Costanzo, "A fuzzy approach to deal with uncertainty in image forensics", Signal Processing: Image Communication 27 (2012)998–1010 http://dx.doi.org/10.1016/j.image.2012.07.006

[66] Amit Phadikar, Santi P. Maity, Mrinal Mandal, "Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images", J. Vis. Commun. Image R. 23 (2012) 454–466 http://dx.doi.org/10.1016/j.jvcir.2012.01.005

[67] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security.

[68] Likai Chen, Wei Lu, Jiangqun Ni, Wei Sun, Jiwu Huang, "Region duplication detection based on Harris corner points and step sector statistics", J. Vis. Commun. Image R. 24 (2013) 244–254 http://dx.doi.org/10.1016/j.jvcir.2013.01.008 http://dx.doi.org/10.1016/j.jvcir.2013.09.006 http://dx.doi.org/10.1016/j.jvcir.2013.10.003 http://dx.doi.org/10.1016/j.jvcir.2013.05.010

[69] Frank Van Riper, "Manipulating Truth Losing Credibility @ The Washington Post"; http://www.washingtonpost.com/wpsrv/photo/essays/vanRiper/030409.htm

Authors' Detail

Deepali Pande is pursuing M. Tech in Computer Science and Engineering from GHRIETW Nagpur, affiliated to RTMNU, India. She has received the B.E degree in Computer Technology in 2010 from Yeshwantrao Chavan College of Engineering, RTMNU. She is an Assistant Professor in the department of Information Technology at KDKCOE, Nagpur.

Her research area includes electronic security and image processing.
Contact Details:
zivyi.77@gmail.com,
+919595488948

Antara Bhattacharya has received the M Tech degree in Computer Science and Engineering and B.E degree in Information Technology. She is currently working as a faculty for academics in M Tech computer science department at GHRIETW affiliated to RTMNU, Nagpur, MH, and India.

Her area of research includes Data Mining, Cryptography and Network Security.
Contact Details: antara.bhattacharya@raisoni.net
+919822713698

A.R .Bhagat Patil is an Associate Professor and Head of the Department of Computer Technology at YCCE, Nagpur, MH. India.
He is pursuing PhD and has received M.Tech degree in Computer Science and Engineering. His additional qualifications includes B.A. (Add.), Sociology, B.A.(Add) Political Science, D.I.A.M.S. His area of expertise includes Computer Networks and Security.

He has performed various R&D activities in multidisciplinary/Industry based Projects Industry Aligned Professional Electives (Infosys, Global logic), Research in thrust area, Computer and Network Security. He has published in 7 international journals, 9 international conference and 6 national conferences.
Contact Details:
arbhagatpatil@gmail.com
+919422827345

APPENDIX

Table I
Comparison of Methods for Forgery Detection on Active Image Information Security Schemata

	ISS employed	Type of Attack	Method for Forgery Detection	+/-
1	For Chaotic Map based fragile watermarking	Integrity Violation	Localization of tampering by finding absolute difference of position relation of pixels between Chaotic map embedded image and obtained watermark by thwarting pixel wise independency. [5]	+ Superior to a tamper detection and localization. + High security. − No structure for Recovery possible.
2	For chaos-based fragile watermarking	Integrity Violation	Flagging along with combinations of MSB and LSB is applied over a cross chaotic map based security. [9]	+ Sister block embedding scheme used helps to improve recovery effect. + Optimization schemes give visual effects to recovered image.
3	For Fragile image watermarking	Vector Quantization, copy-paste, random alterations	Tamper localization by unmatched hash parameters. Hash generated from shift-permutation over gradient image. [9-11]	+ improved localization and security
4	For self-embedded watermarking	Collage attack and Content-tampering attack	Adjacent-block based Statistical detection method: Taking into account all adjacent blocks of the test blocks and its mapping block into account, utilized a statistic-based rule to verify the validity of image blocks. [53]	+ Reduces the probability of false rejection while detecting the altered blocks with a high probability. + outperforms conventional self-embedding fragile water- marking algorithms
5	For Fragile watermarking	Content-based tampering attack	Tamper detection by unmatched pixel based iteration to form tampered blocks. [54]	+ Very high tamper localization capability. + Capable of partially reconstructing a cover image.
6	Semi-fragile watermarking	Malicious attacks	Wavelet-based QIM data hiding technique which uses binary signature and half toning based generated message digest for embedding. The decoder is used to extract Signature non -match of which detects tamper. Extracted Message digest is used to correct tamper regions. [55]	+ Distinguishes malicious changes from common image processing operations. + provides a superior performance in terms of probability of miss and false alarm

Note " +" denotes Strength; "-" denotes Shortcoming

Table II
Comparison of Passive Image Tampering Detection Methods

	Forgery Type	Method for Tampering Detection	+/-
1	Image Splicing	Markov features are generated from transition probability matrices in DCT domain which capture intra and inter block correlation between DCT coefficients. Features constructed in DWT domain characterize position, scales and orientation dependencies. Authentic and Spliced images are classified. [56]	+ Outperforms other State-of-the-Art methods.
2	For detecting region-duplication forgery. Attack by rotation before pasting.	Circular blocks along with Hu moments were used to detect and locate the duplicate regions with rotation.	+ Robustness against noise contamination, blurring, rotation and JPEG compression
3	Image Splicing, Duplication	Detection by artificial blurred boundary technique using image edges grouped based on non-sub sampled contourlet transform to obtain a 6D feature of each edge-point composed of non-sampled contourlet coefficients& four statistics based on phase congruency to be trained and classified by SVM. [58]	+ Also capable of Detecting Image blur.
4	Image Inpainting	The tampered regions are detected by computing and segmenting the averaged sum of absolute difference images between the tampered image and a resaved JPEG image at different quality factors.[59]	+ Better detection performance.
5	Region based Duplication	Homogeneity analysis in quality-sensitive imaging for detection and restoration scheme using lossless data hiding. [61]; Image feature matching approach [62]	+ Visual of the restored images is better than conventional fixed-size block-based approach.
6	Copy-Move forgery attack	A SIFT-based method using hierarchical clustering and geometric transformations estimation.[67]	+ Also detects multiple cloning.
7	Region Duplication by Interpolation	Detection scheme using mapping of overlapping blocks of pixels to log-polar co-ordinates summing which a1-D descriptor is obtained invariant to interpolations. Harris corner interest points method based on step sector statistics representing circular region around each Harris- corner point followed by Matching algorithm. [68]	+ Better detection even for sensitive geometric changes.
8	Duplicated Region	Detection by measuring spatial regularity of local keypoint patterns along with RANSAC algorithm.	+ Effective to find duplicated regions.

Note " +" denotes Strength; "-" denotes Shortcoming