IMAGE TAMPERING DETECTION

Shan Shazad
School of Applied Technology
Illinois Institute of Technology
201 East Loop Road,
Wheaton, IL 60189
sshazad@hawk.iit.edu

Fahad Wahid
School of Applied Technology
Illinois Institute of Technology
201 East Loop Road,
Wheaton, IL 60189
fwahid@hawk.iit.edu

Abstract - To find and further develop a powerful and advanced image tampering detection tool, which will able to confirm the credibility of images that have been computerized. As technology is quickly evolving, almost any image can be modified today. The detection of image manipulation is crucial because it can be used for legal evidence, forensics investigations, and in many other fields. This research will explore the ability to detect image tampered with specialized methods. Four methods will be addressed in combating against images that have been tampered. These include (ii) copy move forgery, slicing (ii), digital watermarking (iii), and format-based image forgery detection (iv).

***Keywords*: Image Tampering, Splicing, Image Authentication, Bayesian, PRNU**

I. INTRODUCTION

The vision of this paper is to present various aspects of image tampering detections, and how it can be identified and solved. The structure of this paper provides a quick review of image tampering detection have been presented in the first section. In the second section, we discuss the different types of digital image tampering techniques that exists. In the third section, we present the idea of a image tampering detection method. In fourth section, the different types of pixel-based image forgery detection, and then the conclusion of the paper.

A - Problem

The main objective of this project is to find and develop a Digital Image Forgery Detection tool which would determine whether a digital image has been tampered using passive forensic techniques. There are a lot a variety of image detection techniques that are used such as Pixel based, Format based, Camera based, Physically based, and Geometric based. Digital images typically form a key part of the forensic evidence for a forensic investigator. They can raise a host of legal and ethical questions and before answers can be obtained, the analysis must start with image source and identification. This is of critical importance to law enforcement agencies, including the FBI, who are very interested in developing Digital Image Forgery Detection tools and techniques

B - Problem Approach

To develop Digital Image Forgery Detection tool and generate PRNU fingerprints that act as a fingerprint for the digital devices, allowing us to determine if there are regions of the image that do not conform to this fingerprint, indicating that tampering has occurred. The tool will throw off some sort of "noise" that will fluctuate based on the image being used. In order to create a tool to detect image tampering, we would first need to use the image tampering techniques to change around the pictures. The techniques are as followed: Copy-Move Forgery Detection, Image Tampering with Splicing, Image Resampling, and Image Retouching.

C – Bayesian (Bayes) Algorithm Approach

When it comes to image tampering, using the Bayesian approach can be useful in being able to detect large forgeries, including in unfavorable circumstances. [10] For example, dark and textured regions, therefore the goal of the approach is to produce believing accuracy of tampering statistics. The approach produces trusted and better balance of the analyzed image statistics and the prior knowledge of the current images. The Bayes theorem example below explains that P that is the probability given hypothesis H and evidence E, states the relationship between the probability and hypothesis P(H) before getting the evidence and the probability P(H | E) of the hypothesis after getting the evidence [12].

$$P(H \mid E) = \frac{P(E \mid H)}{P(E)}\, P(H).$$

II. IMAGE TAMPERING TECHNIQUES

Whenever an image has been slightly modified or deleted some of its important features, that is characterized as the image being "tampered". Throughout the past few decades, there have been many different techniques for tampering with an image, such as the copy-move forgery, image splicing, and image resampling. Below, we will discuss the types of image tampering techniques still used today.

A - Copy-Move Forgery Detection

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. [4] Maliciously manipulated, and tampered digital images without leaving any obvious clues became very easy with the widely available, easy to use and extremely powerful digital image processing tools such as Photoshop and Freehand [4]. As a result, there is a rapid increase of the digitally manipulated forgeries in mainstream media and on the Internet.

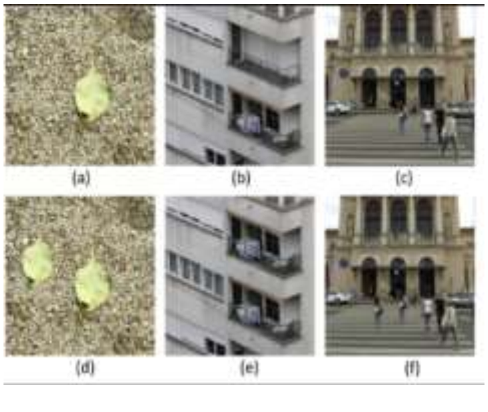

Fig. 1. This figure portrays copy image forgery.

B - Image Tampering with Splicing

The fragments of one or more images are compiled together to create a tampered image. This tampering technique requires one to use the original image, then find a similar one to copy and paste certain features of one image to another [3]. This image illustrates the perfect example of image splicing, and how it can change visual message and meaning of digital images.

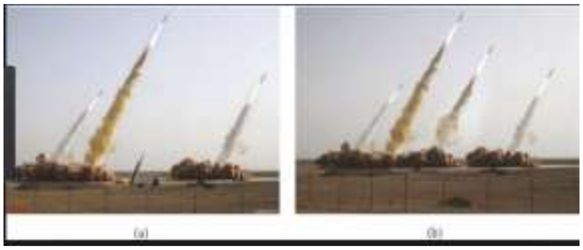

Fig. 2. This figure portrays image splicing. In the second picture, an additional rocket has been added.

C - Image Resampling

To make an astounding forged image, some selected regions must undergo geometric transformations like rotation, scaling, stretching, skewing, flipping and so forth. The interpolation step plays a important role in the resampling process and introduces non-negligible statistical changes. Resampling introduces specific periodic correlations into the image. These correlations can be utilized to recognize phony brought about by resampling. In Figure 3, the picture on the left is the original image while the one on the right is the forged image obtained by rotation and scaling it.

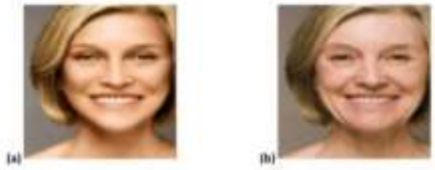

Fig. 3. (a) The real image (b)Result of image retouching

D - Image Retouching

A most commonly used image tampering technique used by many commercials and aesthetics applications to display a particular image or object. The retouching operation goal is to enhance and tamper the features of an image. It may also be carried out by trying to identify the blurring, color modifications, and other enhancements in the forged image. Being able to detect images that are retouched could be easy if the original image is found, however blind detection technique can be a challenging task. Within this tampering, two modifications are done to tamper an image, either global or local. Local changes are done in the copy-move or splicing, but contrast enhancements or actual pixel changes are completed in the global level and that detection could be difficult to see.

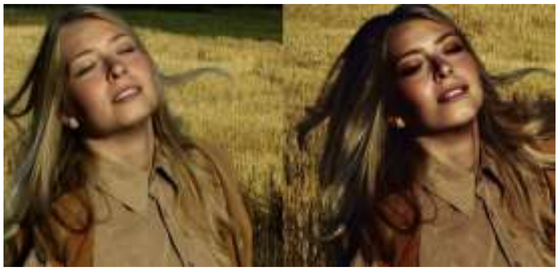

Fig. 4. This figure illustrates how image retouching was used.

III. DIGITAL IMAGE FOGERY DETECTION METHODS

Digital image forgery detection techniques are grouped into two categories; active approach and passive approach. In the active approach, certain information is embedded inside an image during the creation in form of digital watermark [5]. The downside to this approach is that a watermark must be inserted at the time of recording, which would limit to specialty cameras In the passive approach, there is no pre-embedded information inside an image during the creation. This method works purely by analyzing the binary information of an image. Our goal is to use passive image forgery detection in order detect image forgery. Passive image forgery detection techniques roughly grouped into five categories.

A. Pixel-based image forgery detection

Pixel-based techniques accentuate on the pixels of the digital image. These techniques are generally classified into four sorts such as copy-move, splicing, resampling and statistical [5]. This is most common image manipulation technique amongst the well-known phony identification techniques.

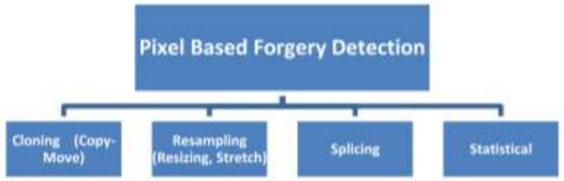

Fig. 5. This is a diagram of Pixel Based Forgery Detection [2].

B. Format-based image forgery detection

Whenever we take a picture from a digital camera, the picture moves from the camera sensor to the memory and it experiences a progression of processing steps, including quantization, color correlation, gamma correction, white adjusting, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may shift on the premise of camera model and camera antiques. These techniques work on this standard. These methods can be separated into four classes such as chromatic aberration, color filter array, camera response and sensor noise.

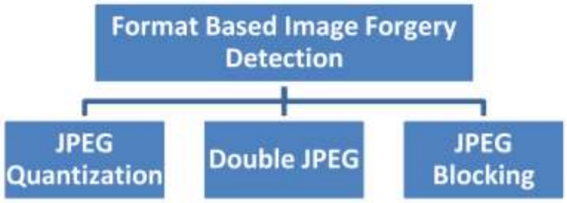

Fig. 6. This is a diagram of Format Based Forgery Detection [2].

C. Camera-based image forgery detection

Whenever we take a picture from a digital camera, the picture moves from the camera sensor to the memory and it experiences a progression of processing steps, including quantization, color correlation, gamma correction, white adjusting, filtering, and JPEG compression [10]. These processing steps from capturing to saving the image in the memory may shift on the premise of camera model and camera antiques. These techniques work on this standard. These methods can be separated into four classes such as chromatic aberration, color filter array, camera response and sensor noise [10].

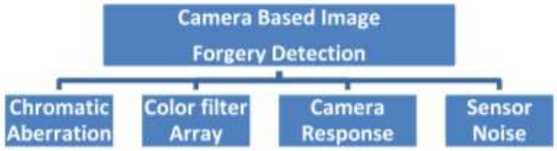

Fig. 7. This is a diagram of Camera Based Forgery Detection [2].

D. Physical environment-based image forgery detection

These techniques basically based on three dimensional interactions between physical object, light and the camera. Consider the creation of a forgery showing two movie stars, rumored to be romantically involved, strolling down a nightfall shoreline. Such a picture may be made by grafting together individual pictures of each movie star. In this manner, it is frequently hard to exactly match the lighting effects under which each individual was initially captured. Contrasts in lighting across an image can be utilized as proof of altering. These techniques work on the basis of the lighting environment under which an article or picture is caught. Lighting is very important factor for capturing an image. These techniques are isolated into three classifications such as light direction (2-D), light direction (3-D) and light environment.

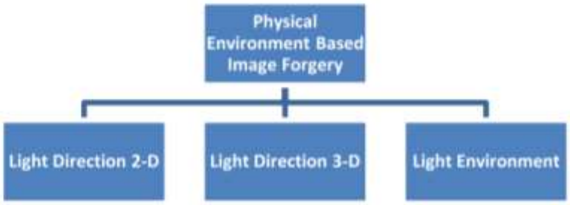

Fig. 8. This is a diagram of Physical Environment Based Forgery Detection [2].

E. Geometry-based image forgery detection

Geometry-based image forgery detection methods are separated into two classes such as principle point and metric measurement [11].

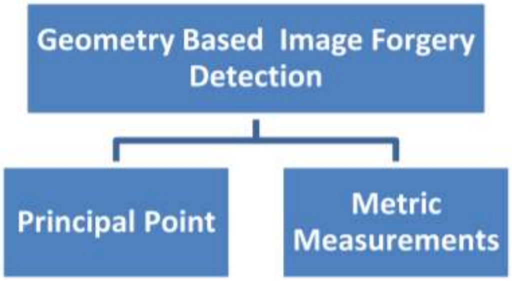

Fig. 9. This is a diagram of Geometry Based Forgery Detection [2].

IV. RESULTS AND DISCUSSION

In the last decades, many forgery detection techniques have been proposed. An attempt is made to bring in various potential algorithms that signify improvement in image authentication techniques. From knowledge of the image authentication techniques, it is inferred that Passive or blind techniques which need no prior information of the image under consideration have a significant advantage of no requirement of special equipment's embed the code into the image at the time of generation, when compared to active techniques [9]. We have discussed various methods that are proposed by various authors, to detect image forgery. The thought process of the considerable number of strategies, is to recognize the imitation in the picture yet the procedures are diverse. There are a number of drawbacks with the presently available technologies. Firstly, all systems require human interpretation and thus cannot be automated. Secondly, being the problem of localizing the forgery, and also the problem is of robustness to common image processing operations like blurring, JPEG compression, scaling, and rotation [9]. There is also a setback of no established benchmarks which makes performance analysis and comparison of results of current algorithms difficult. As such there is need to develop common benchmark for image data set and image forgery detection techniques that could detect any type of forgery with lesser computational complexity and high robustness. Our results indicated that Cloning had the least F-measure (FM) at 43.87% followed by Splicing at 68.25%, and Resampling at 90.65%.

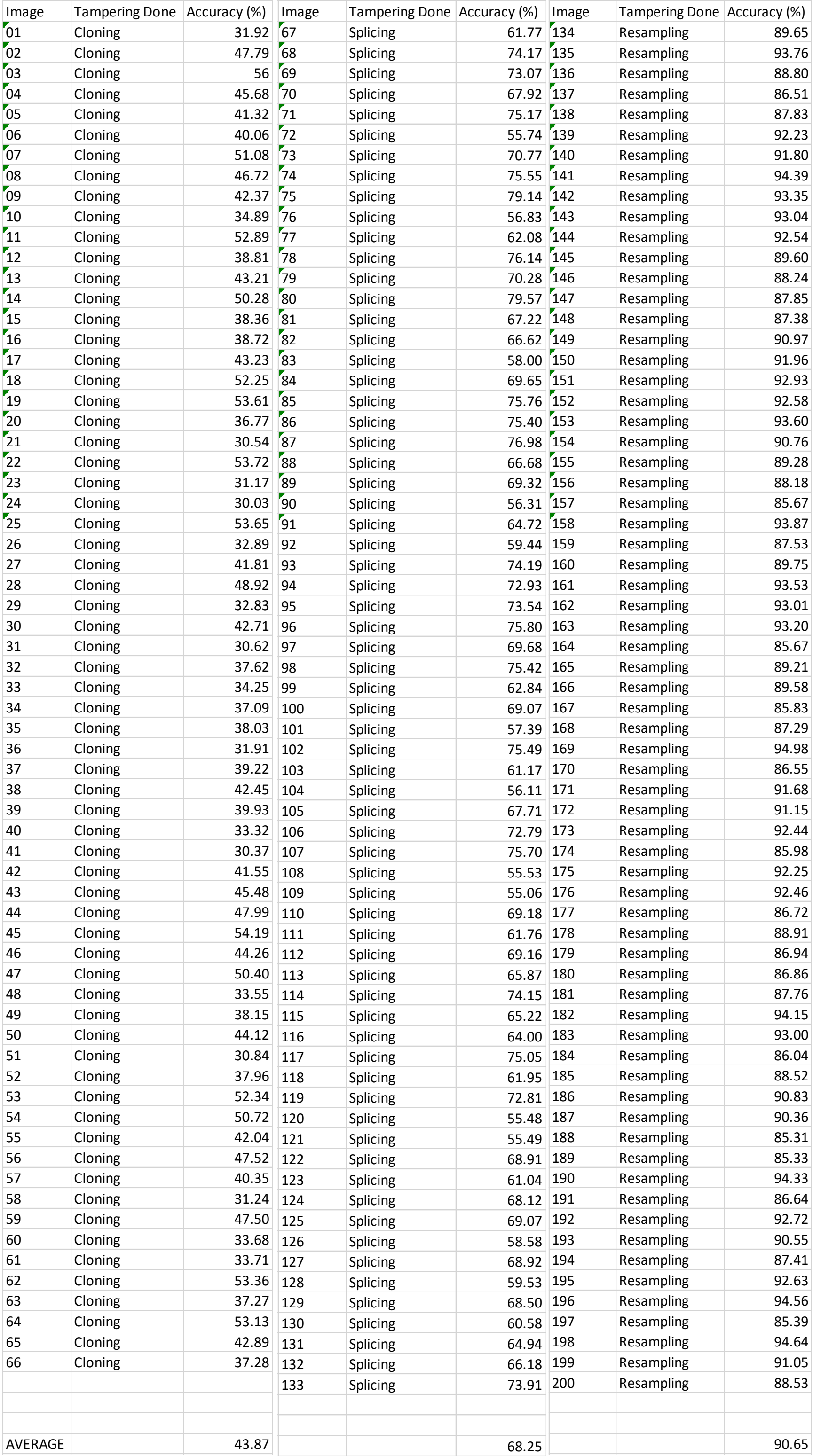

Image	Tampering Done	Accuracy (%)
01	Cloning	31.92
02	Cloning	47.79
03	Cloning	56
04	Cloning	45.68
05	Cloning	41.32
06	Cloning	40.06
07	Cloning	51.08
08	Cloning	46.72
09	Cloning	42.37
10	Cloning	34.89
11	Cloning	52.89
12	Cloning	38.81
13	Cloning	43.21
14	Cloning	50.28
15	Cloning	38.36
16	Cloning	38.72
17	Cloning	43.23
18	Cloning	52.25
19	Cloning	53.61
20	Cloning	36.77
21	Cloning	30.54
22	Cloning	53.72
23	Cloning	31.17
24	Cloning	30.03
25	Cloning	53.65
26	Cloning	32.89
27	Cloning	41.81
28	Cloning	48.92
29	Cloning	32.83
30	Cloning	42.71
31	Cloning	30.62
32	Cloning	37.62
33	Cloning	34.25
34	Cloning	37.09
35	Cloning	38.03
36	Cloning	31.91
37	Cloning	39.22
38	Cloning	42.45
39	Cloning	39.93
40	Cloning	33.32
41	Cloning	30.37
42	Cloning	41.55
43	Cloning	45.48
44	Cloning	47.99
45	Cloning	54.19
46	Cloning	44.26
47	Cloning	50.40
48	Cloning	33.55
49	Cloning	38.15
50	Cloning	44.12
51	Cloning	30.84
52	Cloning	37.96
53	Cloning	52.34
54	Cloning	50.72
55	Cloning	42.04
56	Cloning	47.52
57	Cloning	40.35
58	Cloning	31.24
59	Cloning	47.50
60	Cloning	33.68
61	Cloning	33.71
62	Cloning	53.36
63	Cloning	37.27
64	Cloning	53.13
65	Cloning	42.89
66	Cloning	37.28
AVERAGE		43.87

Image	Tampering Done	Accuracy (%)
67	Splicing	61.77
68	Splicing	74.17
69	Splicing	73.07
70	Splicing	67.92
71	Splicing	75.17
72	Splicing	55.74
73	Splicing	70.77
74	Splicing	75.55
75	Splicing	79.14
76	Splicing	56.83
77	Splicing	62.08
78	Splicing	76.14
79	Splicing	70.28
80	Splicing	79.57
81	Splicing	67.22
82	Splicing	66.62
83	Splicing	58.00
84	Splicing	69.65
85	Splicing	75.76
86	Splicing	75.40
87	Splicing	76.98
88	Splicing	66.68
89	Splicing	69.32
90	Splicing	56.31
91	Splicing	64.72
92	Splicing	59.44
93	Splicing	74.19
94	Splicing	72.93
95	Splicing	73.54
96	Splicing	75.80
97	Splicing	69.68
98	Splicing	75.42
99	Splicing	62.84
100	Splicing	69.07
101	Splicing	57.39
102	Splicing	75.49
103	Splicing	61.17
104	Splicing	56.11
105	Splicing	67.71
106	Splicing	72.79
107	Splicing	75.70
108	Splicing	55.53
109	Splicing	55.06
110	Splicing	69.18
111	Splicing	61.76
112	Splicing	69.16
113	Splicing	65.87
114	Splicing	74.15
115	Splicing	65.22
116	Splicing	64.00
117	Splicing	75.05
118	Splicing	61.95
119	Splicing	72.81
120	Splicing	55.48
121	Splicing	55.49
122	Splicing	68.91
123	Splicing	61.04
124	Splicing	68.12
125	Splicing	69.07
126	Splicing	58.58
127	Splicing	68.92
128	Splicing	59.53
129	Splicing	68.50
130	Splicing	60.58
131	Splicing	64.94
132	Splicing	66.18
133	Splicing	73.91
		68.25

Image	Tampering Done	Accuracy (%)
134	Resampling	89.65
135	Resampling	93.76
136	Resampling	88.80
137	Resampling	86.51
138	Resampling	87.83
139	Resampling	92.23
140	Resampling	91.80
141	Resampling	94.39
142	Resampling	93.35
143	Resampling	93.04
144	Resampling	92.54
145	Resampling	89.60
146	Resampling	88.24
147	Resampling	87.85
148	Resampling	87.38
149	Resampling	90.97
150	Resampling	91.96
151	Resampling	92.93
152	Resampling	92.58
153	Resampling	93.60
154	Resampling	90.76
155	Resampling	89.28
156	Resampling	88.18
157	Resampling	85.67
158	Resampling	93.87
159	Resampling	87.53
160	Resampling	89.75
161	Resampling	93.53
162	Resampling	93.01
163	Resampling	93.20
164	Resampling	85.67
165	Resampling	89.21
166	Resampling	89.58
167	Resampling	85.83
168	Resampling	87.29
169	Resampling	94.98
170	Resampling	86.55
171	Resampling	91.68
172	Resampling	91.15
173	Resampling	92.44
174	Resampling	85.98
175	Resampling	92.25
176	Resampling	92.46
177	Resampling	86.72
178	Resampling	88.91
179	Resampling	86.94
180	Resampling	86.86
181	Resampling	87.76
182	Resampling	94.15
183	Resampling	93.00
184	Resampling	86.04
185	Resampling	88.52
186	Resampling	90.83
187	Resampling	90.36
188	Resampling	85.31
189	Resampling	85.33
190	Resampling	94.33
191	Resampling	86.64
192	Resampling	92.72
193	Resampling	90.55
194	Resampling	87.41
195	Resampling	92.63
196	Resampling	94.56
197	Resampling	85.39
198	Resampling	94.64
199	Resampling	91.05
200	Resampling	88.53
		90.65

Fig. 9. Results based on a test bed of 200 images.

V. CONCLUSION

Image Tampering is one of those techniques that brings an issue to image confidentiality and authentication. Once it has been tampered, it can be difficult to detect the authenticity of the images. The research for the project is further being addressed at, however we have gathered compelling information on active and as well as passive tamper detection techniques. It may sound easy to not only just replicate and transmit image contents without damaging its actual quality, but also to manipulate them. In the paper, we have carefully compiled over passive detection techniques such as splicing, cloning, retouching, and being able to detect the forged images. Interestingly, there are many ways to detect based on analyzing the lighting environment, camera feature, and understanding the statistical and geometric properties it has. [5] In our abstract section, our goal is to be successfully find and further on develop a powerful image tampering detection tool, that can potential help us detect tampered images throughout the project. The four tampering methods we will look at is copy move, slicing, digital watermarking, and format-based image detection. The problem that needs to be resolved is to find a working image tampering program, and further develop it so It can work the way we want it to. Our goal is to have the program able to detect through pixels changes, format, camera, physically, and geometric.

REFERENCES

[1] Deepika Sharma and Pawanesh Abrol, "Digital Image Tampering – A Threat to

Security Management", Version 1.0, October 10, 2013, fromhttps://www.ijarcce.com/upload/2013/october/74-h-deepika_sharma-digital.pdf

[2] Minati Mishra and Munesh Chandra Adhikary, "Digital Image Tamper Detection Techniques – A Comprehensive Study", June 2013, fromhttps://www.researchgate.net/publication/243458359_Digital_Image_Tamper_Detection_Techniques_-_A_Comprehensive_Study

[3] ChitwanBhalla Surbhi Gupta, "A Review on Splicing Image Forgery Detection Techniques", Vol 6, April 2016, from https://ijcsits.org/papers/vol6no22016/49vol6no2.pdf

[4] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," Aug 2003, from http://www.ws.binghamton.edu/fridrich/Research/copymove.pdd

[5] Hai Tao, Li Chongmin, Jasni Mohamad Zain, and Ahmed N. Abdalla "Robust Image Watermarking Theories and Techniques: A Review", February 2014, from http://www.sciencedirect.com/science/article/pii/S1665642314716128

[6] Mohd D. Ansari, S.P. Ghrera, and Vipin Tyagi "Pixel-Based Image Forgery Detection: A Review" Aug 07, 2014, fromhttp://www.tandfonline.com/doi/pdf/10.1080/09747338.2014.921415

[7] Jiri Fridrich, "Method for Tamper Detection in Digital Images" from http://ws.binghamton.edu/fridrich/Research/acm99ps.ps

[8] Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom Gupta, "An Evaluation of Digital Image Forgery Detection Approaches" March 2017, from https://arxiv.org/pdf/1703.09968.pdf

[9] Massimo Luliani, "An Introduction to Geometric Based Image Forensics" Retrived on October 2nd, 2017, from http://lesc.dinfo.unifi.it/sites/default/files/Documenti/Demo/2014-10-23-Seminario-Iuliani.pdf

[10] Kruttika Pillary, and Shubhangi Moon, "Source Camera Detection Techniques to Remove Dust Particles – A Review, from http://www.ijsr.net/archive/v6i3/ART20171205.pdf

[11] Hanson K. M., "Introduction to Bayesian image analysis" Retrieved on November 1st, 2017, from http://kmh-lanl.hansonhub.com/publications/medim93.pdf

[12] Ellinor Andrew, Williams Christopher, Strandberg Adam,…"Bayes' Theorem and Conditional Probability" Retrieved on November 1st, 2017, from https://brilliant.org/wiki/bayes-theorem/