Effective CCTV Image Tampering Introspection Using Forensic Approaches

Abila Elizabeth.C[1] and Dr.Nancy Jasmine Goldena[2]
[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli,*
[2]Assistant Professor, Department of Computer Applications, Sarah Tucker College, Tirunelveli.

Abstract
Closed Circuit Tele Vision monitoring plays a vital role in the safety measures for residential, offices and public organization nowadays. It is not easy to monitor with manual implementation of human being for entity monitoring system whereas the machine based system reduces the complexity and increase the availability and persistence for ensuring the safety with its compactness and protection. The monitoring technology grows in a linear fashion whereas the illegal operations and actions against safety improve in an exponential way. The art of ensuring safety includes lot of Hardware, software, methodologies ad procedural measures. Image tampering includes two types of operations such as removal of contents or manipulation of actual contents which mislead others to think in a misconception manner. The entire dependency on tampered images will affect any organization future with falsified information's This paper deals with the Forensic image processing which is a scientific methodology that can analyze the image and process it in certain standards to check for its genuinely. In near future we will implement the advanced neural network based web data integrity for optimal productive data integration in web data mining.

Keywords: *CCTV, tampering, introspection, forensics, image mining.*

I.INTRODUCTION

a. Forensic Science:
Forensic science, also known as criminalistics [1], is the application of science to criminal and civil laws, mainly—on the criminal side—during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure. Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation. While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals.

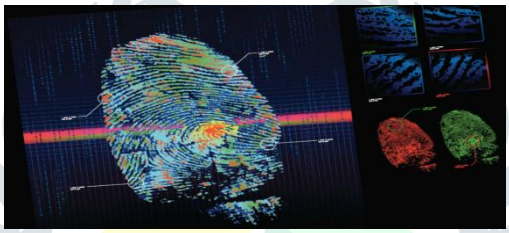

Fig-1: Digital image forensics

b.CCTV
Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point-to-point (P2P), point-to-multipoint (P2MP), or mesh wired or wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, stores, and other areas where security is needed.

Fig-2: CCTV footage for chain snatching

c. Image Tampering:
Image tampering represents the removal of all the contents in an image or manipulation of images with addition or removal of particular component in an image; sometimes the entire modifications except few background details are also possible to mislead the viewers. The depth analysis over the image details only reveal the tampering level for it's genuinely.

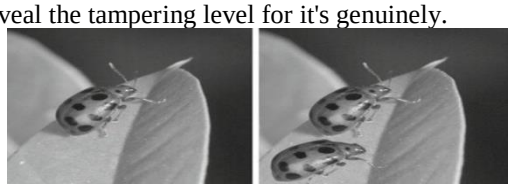

Fig-3: Original Vs Tampered image

In Fig-3, the second one is tampered which can be easily identified through its shadow property of the insects.

II.PROPOSED METHODOLOGY

The proposed methodology initially taking the input image and then perform preprocessing techniques by converting it into proper format and type. Then the forensic processing of interpretation and examination will be applied with various image component

introspection aspect which results with the final output as original and tampered pair if any manipulations applied or original image alone if its genuine .

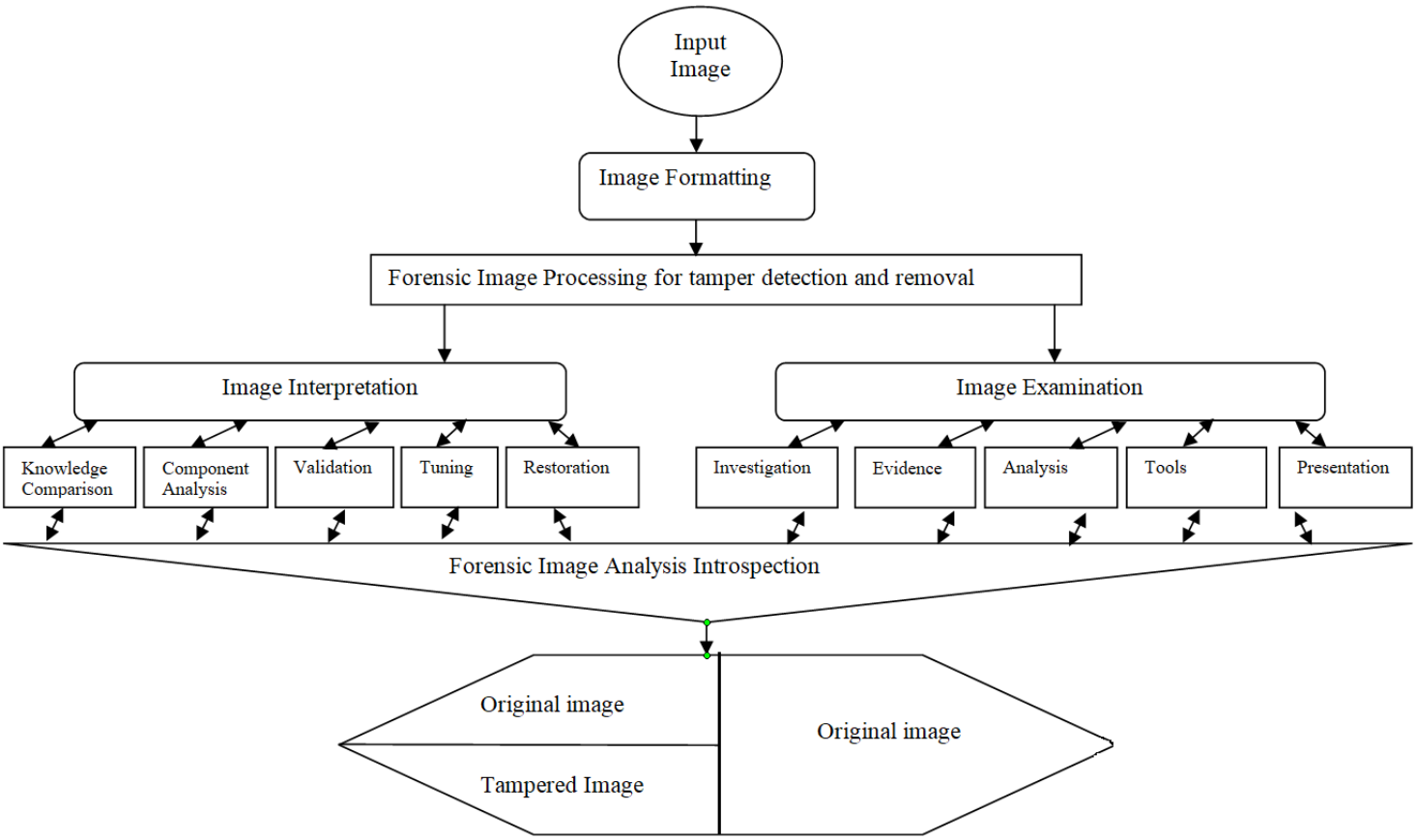

Fig-4: Proposed effective image tampering introspection using forensic approach

The final output image is highly valid because of its effective introspection which includes interpretation and examination components with maintaining the standards for image analysis processing order which saves time and space.

III. IMPLEMENTATION

The implementation of our proposed methodology consists of two phases with two different images, phase 1 uses a genuine image and phase 2 will be implemented by a tampered image.

Phase-1: Consider the image of Sarah Tucker College, Tirunelveli, and Tamilnadu, India.

Fig-5: Sample image-1 for tampering checking

Step1: Image interpretation

Collecting the EXIF data of the image using Philhervey or Jefrey Exif data extraction tool, we obtain the following,

Make	Canon
Model	Canon EOS 5D Mark III
Orientation	top-left
XResolution	72
YResolution	72
Resolution Unit	2
Software	Adobe Photoshop CS2 Windows
Date Time	2018:10:05 16:47:00

YCbCrPositioning	2
Exposure Time	0.00625
F-number	11
ExifIFDPointer	312
Exposure Program	Manual
Photographic Sensitivity	200
Sensitivity Type	2
RecommendedExposureIndex	200
ExifVersion	0230
DateTimeOriginal	2018:08:17 11:23:47
DateTimeDigitized	2018:08:17 11:23:47
Components Configuration	YCbCr
ShutterSpeedValue	7.375
Aperture Value	7
Exposure Bias	0
Metering Mode	Pattern
Flash	Flash did not fire, compulsory flash mode
Focal Length	70
Subjective	00
SubSecTimeOriginal	00
SubSecTimeDigitized	00
FlashpixVersion	0100
Color Space	1
PixelXDimension	900
PixelYDimension	600
InteroperabilityIFDPointer	1212
FocalPlaneXResolution	2628.3367556468174
FocalPlaneYResolution	2633.7448559670784
FocalPlaneResolutionUnit	2
Custom Rendered	Normal process
Exposure Mode	1
White Balance	Manual white balance
SceneCaptureType	Standard
CameraOwnerName	
BodySerialNumber	368023003365
Lens Specification	24,70,0,0
Lens Model	EF24-70mm f/2.8L II USM
LensSerialNumber	2725001584

a. Knowledge comparison:
The image Exif data reveals the Original timestamp and digitized times stamp are same with custom rendered as normal and color space=1 reveals no added colors.
b. Component Analysis:
The wall, trees and gate colors are normal no purposefully added objects are there.
c. Validation:
The image compared with web images for clarity and brightness modifications from different resources.

Fig-6: Validation from different resources-sample-1

d. Tuning:
The brightness and contrast variations are gradually applied with no extraordinary pixel value variations.

Fig-7: Tuning strategy for image tampering-sample-1

e. Restoration:
Mixture of filters and effects applications with its restoration does not affect the original image.

Step-2: Image Examination
a. Investigation:
The object pixilation and clarity in max gain is not altered.

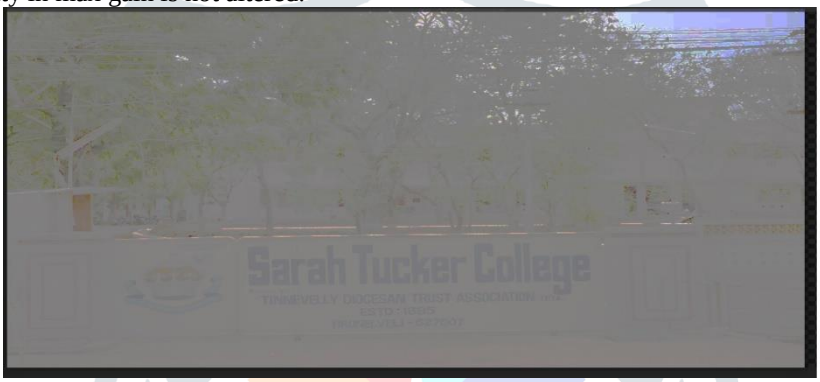

Fig-8: Investigation strategy for image tampering-sample-1

b. Evidence:
All the shadow effects, pixel variations are verified with proper care,

c. Analysis:
Using the Mat lab tool the Matrix conversion of the given STC college image is as follows

00000000000000000000001111100000101111110
00000000000000000000000000100011011011100
00000000000000000000000000000000110000000
00000000000000000000000000000001111110100
00000000000111011000100000000011111111111
00000000000110000000000000000000000000000
11000000000100000000000000000000000000000
11000000001111111000000000000000010000000
11000000000110000000000000000000101000000
00000111111111111111111111111111000101111
00011111111101111011011110010111111111111
00110110011100000100000100000111111111111
00110110011100100110001100000111110000011
00110100010111111111111111101111100000000
00110110111111111111111111111111100000000
00010111111111111111111111111111000000000
00000111111111111111111111111110000111000
00001111111111111111111111111111111111111
11111111111111111111111111111111111111111

d. Tools:
Using Mat Lab and Exif Photo analyzer the STC college image pixel values are gradually distributed based on the region wise computations.

e. Presentation Reports:
The given STC College image is a genuine one.

Phase-2: Consider the image of Park with or without Rooster Image as follows,

Fig-9: Sample image-2 for tampering checking

Step-1: Image Interpretation

No proper Exif data available for this image due to its purposeful deletion of metadata by the creators.

a. Knowledge comparison:

The image non existence of Exif data reveals that the image is not a double photographed one (without and with Rooster).

b. Component Analysis:

The rooster brightness and the leg positions are not properly fixed with the floor with careful observations which also resembles that it is not a double photographed one.

Fig-10: Component strategy for image tampering identification -sample image-2

c. Validation:

The image compared with first and second parts resembles the modifications from different resources.

Fig-11: Validation strategy for image tampering identification -sample image-2

d. Tuning:

The brightness and contrast variations are gradually applied with extraordinary pixel value variations are observed.

Fig-12: Tuning brightness strategy for image tampering identification -sample image-2

While applying the contrast effect with minimal brightness the rooster borders are easily observable such that no other borders for any other objects present in the given image.

Fig-13: Tuning contrast strategy for image tampering identification -sample image-2

e. Restoration:
Mixture of filters and effects applications with its restoration affect the original image.

Step-2: Image Examination
a. Investigation:
The object brightness and clarity in max gain is altered.

Fig-14: Investigation strategy for image tampering identification -sample image-2

b. Evidence:
All the shadow effects, pixel variations are verified with proper care,

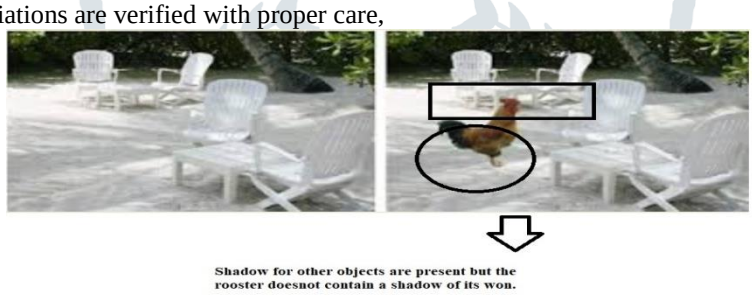

Fig-15: Evidence strategy for image tampering identification -sample image-2

c. Analysis:
Using the Mat lab tool the Matrix conversion of the given Rooster image is as follows
0000000000000000000010000000000000000000
0000000000000000000010000000000000000000
0000110000100000000000001100001000000000
0001110011101000000010001110111011000000
1111111111111110001111111111111111100011
1111111111111111111111111110111111111111
1111111111111111111111111101111111111111
1111111111111111111111110001111111111111
1111111111111111111111110001111111111111
1111111111111111111111111111111111111111
1111111111111111111111111111111111111111
1111111111110011111111111111111010111111
1111111111111111001111111111111111110011
Even in a similar component image ,the abnormal distribution of 1's in rows 1 to 6 and 8 to 13 brightness of the pixels are different due to object insertion.
d. Tools:
Using Mat Lab and Exif Photo analyzer the Rooster image pixel values are not gradually distributed based on the region wise computations.
e. Presentation Reports:
The given Rooster image second part is not a genuine one but first part is a genuine one.

IV.RESULTS AND DISCUSSION:

The proposed methodology is applied to a large sample of 100 images in which 50 are genuine and remaining 50 are suspect images with phase-1 and phase-2, the following results yield the betterment of results after proper output of image processing introspections illustrated in table-1.

Table-1: Proposed Forensic Image Introspection results

Forensic Image Tamper Introspection	Genuine	Tampered
After Phase-1 Completion stage	39	23
After Phase-2 Completion stage	11	27

The following graph shows the proposed efficient forensic image tamper introspection results as follows,

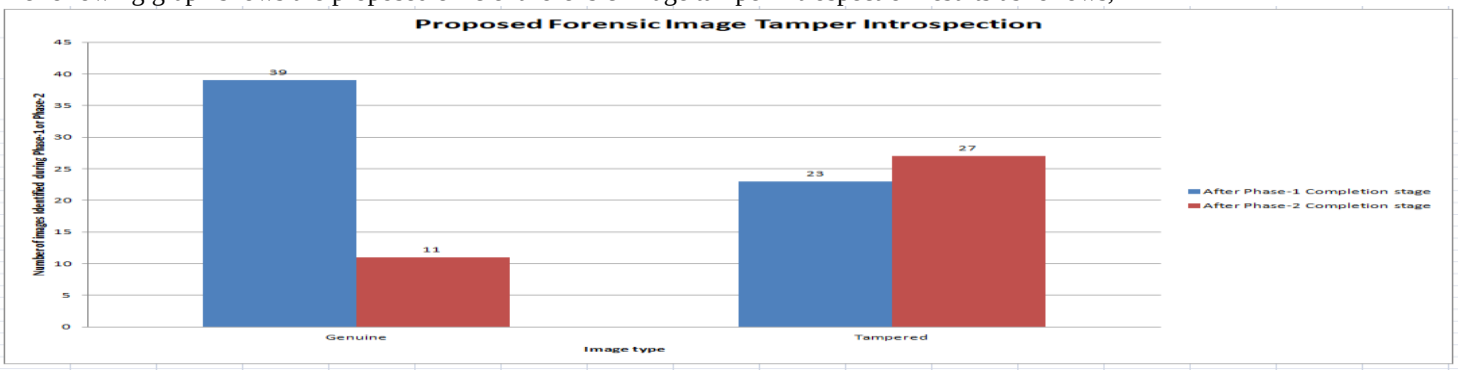

Fig-16: Proposed Forensic Image Introspection Results

V.CONCLUSION:

The proposed forensic approach for CCTV tampered image detection consists of two phases in which the first phase technically identify the image components with its level of impact on the image and the phase 2 focuses on the logical introspection of image examination towards component natural or artificial allocation based on the various image analyzing tools, Our proposed methodology yields good results with 78% success in phase-1 for genuine images and remaining 22% success obtained through phase 2 whereas the Tampered images. During the image processing functionality some images are failed to restore to its originality due to its quality and content applicability, we omitted the images in our examination for its rare support for qualitative and quantitative analysis through their copyright nature.. In near future we will implement the neural network based Forensic Image tamper detection analysis using image mining techniques.

References

[1]T. Vidas, B. Kaplan, M. Geiger, “OpenLV: Empowering investigators and first-responders in the digital forensics process”. *Digital Investigation*, vol. 11, pp. S45-S53, 2014.
[2] A. Lazzez, T. Slimani,"Forensics Investigation of Web Application Security Attacks", *International Journal of Computer Network and Information Security*, vol.7, no.3, pp.10-17, 2015.DOI: 10.5815/ijcnis.2015.03.02.
[3] Y. Prayudi, A. Ashari, T. K. Priyambodo, “A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia”. *International Journal of Computer Network and Information Security*, vol. 7 no. 11, 1, 2015.
[4] J. Sharma, M. Singh, "CUDA based Rabin-Karp Pattern Matching for Deep Packet Inspection on a Multicore GPU", *International Journal of Computer Network and Information Security*, vol.7, no.10, pp. 70-77, 2015.DOI: 10.5815/ijcnis.2015.10.08.
[5] S. Jaiswal, S. Dhavale, “Video Forensics in Temporal Domain using Machine Learning Techniques”. *International Journal of Computer Network and Information Security*, vol. 5 no. 9, 58, 2013.
[6] Y. Vural, Ş. Sağıroğlu, “A Review on Enterprise Information Security and Standards”. Journal of the Faculty of Engineering and Architecture of Gazi University, vol. 23 no. 2, 2008.
[7] M. Geddes, P. B. Zadeh, “Forensic analysis of private browsing. In Cyber Security and Protection of Digital Services (Cyber Security)”, *2016 International Conference On*, pp. 1-2. IEEE, 2016.
[8] K. Conlan, L. Baggili, F. Breitinger, “Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy”. *Digital Investigation*, vol. 18, pp. 66-75, 2016.
[9] B. Carrier, “File system forensic analysis”. Addison-Wesley Professional, 2005.
[10] U. Akalın, Ç. Uluyol, “Mobile Devices, Mobile Forensic Informatics and Proposed Process Model”, *XVIII. Akademik Bilişim Konferansı*, 2016.
[11] https://sarahtuckercollege.edu.in/.