International Journal of Pure and Applied Mathematics
Volume 116 No. 8 2017, 229-233
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DIGITAL FORENSICS AND IMAGE FORGERY TO PREVENT CYBER ATTACK

Ms. Mary Linda.I[1], Mrs. K. Shanmugapriya[2]
[1,2] Assistant Professor, Department of CSE, BIST,BIHER,Bharath University, Chennai-73
[1]marylinda.cse@bharathuniv.ac.in

Abstract: Numerous digital tools and techniques square measure getting used to realize this. Our paper explains forensics analysis steps within the storage media, hidden knowledge analysis within the classification system, network rhetorical ways and cyber-crime data processing. This paper proposes a brand new tool that is that the combination of digital rhetorical investigation and crime data processing. The projected system is meant for locating motive, pattern of cyber-attacks and counts of attacks varieties happened throughout an amount. Thus the projected tools permit the system directors to alternate the system vulnerability.

Keyword: Digital Forensics, Cyber-attacks

1. Introduction

Computer forensics is that the method that applies engineering science and technology to gather and analyse proof that is crucial and admissible to cyber investigations. Network forensics is employed to seek out attacker's behaviour and trace them by assembling analysing log and standing data. A digital thetorical investigation is associate degree inquiry into the unacquainted or questionable activities within the cyber house or digital world. The investigation method is as follows[1-3]:

Collection: The primary step within the rhetorical method is to spot potential sources knowledge of information and acquire forensic data from them. Major sources of knowledge area unit desktops, storage media, routers, cell phones; cameraetc. a thought is developed to accumulate information in keeping with their importance, volatile and quantity of effort to gather[4].

Examination: Once information has been collected, consequent section is to look at it, which involves assessing and extracting the relevant items from the collected data[5-7].

Analysis: Extracted and relevant information has been analysed to draw conclusions. If further information is hunted for detail investigation can concern through information assortment.

Reporting: This can be the method of getting ready and presenting the results of the analysis section. Digital rhetorical science covers PC forensics, disk forensics, network forensics, firewall forensics, device forensics, information forensics, mobile device forensics, computer code forensics, live systems forensics etc.

A forgery detection methodology that exploits refined inconsistencies within the color of the illumination of images to realize this, we tend to incorporate information from physics and statistical based fuel estimators on image regions. We tend to try and extract texture and edge based options from the fuel estimates. These options area unit provided to a machine learning approach for creating call mechanically. The classification performance exploitation AN SVM meta-fusion classifier is promising. A SVM classifier is trained for using applied math options of pattern noise for classifying small blocks of a picture. SVM classifier is employed which have similar purposeful type to neural networks. Image, texture and pal price based mostly options area unit extracted and analysed from the pictures. Then has values area unit calculated for these options[8].

2. Digital Image Authentication

There are two approaches of digital image authentication:

1) Active approach
2) Passive approach

Active Approach: The active approach includes ways like water marking and digital signature. These are called non-blind ways. The key downside of watermark approach is that watermarks have to be compelled to be embedded within the image before distribution within the market[9-10].

Passive Approach: In passive approach of digital image authentication technique, no data has to be embedded in picture for distribution. These strategies are called blind because the presence of original image not needed to verify the authenticity. So, these strategies even have the appliance within the field of image rhetorical. Digital image rhetorical may be a PC technique for up a digital image like police investigation, circuit TV, infrared image etc. These techniques involve digital "filters" which will suppress noise within the digital image, extract the details from

shadow and supply image sharpening. The distribution of image pixels i.e., histograms may be optimized for data extraction and since of this it become straight forward to verify credibleness and integrity of details images in an exceedingly field wherever the geniuses of image features a prime vital. Since the matter of image forensics is extremely broad, this paper focuses on forgery detection in digital pictures. There are three lead directions for image forensics analysis. The supply of picture is known. Makes an attempt to classify PC generated pictures from natural pictures. Tackles the matter of forgery detection for digital pictures. This paper offers the economical and reliable techniques for detective work globally and regionally applied distinction sweetening, cut-and –paste forgery, bar chart deed, noise and image scaling within the digital image[11].

3. Proposed Work

In this project we tend to propose the tactic to find the rhetorical within the photography. For that here we tend to use the SVM classifier for the rhetorical detection. At first we tend to establish the fuel map within the image. We discover the face from the photography. For the face find here we tend to use the violo john technique. Once face detection we tend to crop the face image and calculate the clever edge and HOG feature. The technique counts occurrences of gradient orientation in localized parts of a picture. This technique is analogous to it of edge orientation histograms. The tactic extracts in variance to geometric and measure transformations for object orientation. Then we tend to calculate the native Binary Patterns of the image. At that time we tend to establish the applied mathematics analysis of structure data (SASI). In SASI the applied mathematics data of the image like energy, entropy, correlation add of energy and add of correlation are calculated. The extracted feature can pass to the SVM classifier for the coaching. SVM is stands for Support vector machine. It's a binary classifier. It's a kernel primarily based learning classifier. The trained classifier can predict regarding the image whether or not it's original or rhetorical image[12].

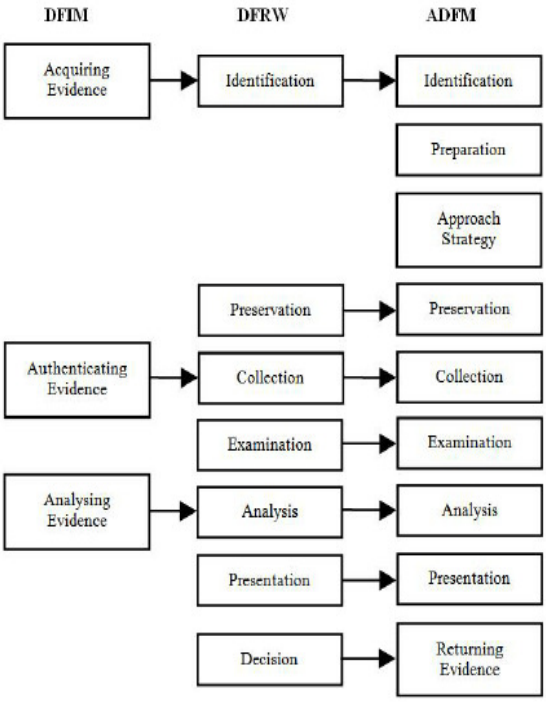

Figure 1. Classification of image analysis

4. Basic Steps In Storage Media Investigation

1) Replication of rhetorical image: Nonintrusive acquisition of a replicated image of knowledge extracted from the questioned device[13].

2) For integrity perform Hash worth calculation.

3) Conducting a file-fragment recovery procedure to recover files and folders to a replacement location.

4) Examine all files particularly deleted files.

5) Reviewing typical evidentiary objects such as:

a) Analyse free areas, slack areas and dangerous sectors.

b) Application computer code file.

c) Photographic camera, printer and appurtenant devices.

d) E-mails, Games & Graphics pictures.

e) Net chat logs & Network activity logs.

f) Recycle folders.

g) System and file date/time objects.

h) User-created directories, folders, and files.

i) Latent information extraction from page, temp, and written account space.

6) Copy the content of the evidentiary object into textfiles.

7) Sorting out key-term strings.

8) Reviewing file notations.

9) Scrutinize applications or indications of as file eradications, file encoding, file compressors or file concealment utilities.

10) Making ready proof summaries, exhibits, reports,and skilled findings supported evidentiary extracts and investigative analysis.

4. Crimedatamining Algorithm

1) Determine variables/item sets from a case report (our proposed system stores these variables as attributes of tables, filesystem table, network table)[14].

2) Item sets I = {I1,I2,I3…IM}.

3) Set of actions D = {t1,t2,t3…tn}.

4) Notice frequent item sets by exploitation Apriori algorithmic rule. Employs associate degree reiterative level to seek out set of frequent item sets[15-17].

E.g. if associate degree offender attacked information, login try results a data loss/Data meddling and case report show actions like knowledge deleted, Login try, attack sort = SQL injection, If these item sets area unit frequent then we are able to set a rule " motive of attack is knowledge theft".

5) Build Association Rules i.e. It is a rule in the form X → Y showing an association between X and Y that if X occurs then Y will occur. If the attacker accessed operating system files then we can say motive of attack is system Crash. If the attacker attacked Database login and Password steel then we can say criminal motive for data theft/data change. This maximum frequent item sets also shows attack patterns. Finding other signs of evidence Correlation, contingences (Consider these values while making rule sets[18-20]).

6) Set SQL queries according to the rules.

7) Retrieve data.

5. Applications of Image Forensics

FIP technology is primarily used for sweetening of police investigation video. This police investigation imagination will be created by video cameras or cameras that manufacture individual image frames. The police investigation video will be from a good type of locations like bank lobbies and ATMs, hospitals, universities, retail locations, looking malls, traffic signals, toll booths, outside venues, and far a lot of. Whereas the term "photograph" describes the output of a camera, a picture refers to associate degree kind of graphical illustration for depiction of an object, together with a photograph. So, a photograph is a picture but a picture isn't essentially a photograph. During this context, rhetorical image process is additionally applicable for the enhancement of pictures, like pictures of fingerprints[21-24], retinal scans, shoe impressions, and so on. Typically, within the event of a criminal offense, a criminal offense scene investigator can recover the police investigation video for analysis by a criminologist, or rhetorical image analyst[25-28]. The goal of the analyst is to see the image sweetening method which will allow most data extraction from the police investigation video. Zhao Jun Hong targets copy-move forgery detection in digital image. This technique uses a brand new approach supported one improved LLE, as a result of a way supported PCA to observe copy-move forgery can't observe the amalgamated edge, that's why this paper gift LLE technique, that not solely observe copy-move areas however additionally amalgamated edges[28-30].

6. Conclusion

In this approach, new technique for detective work cast pictures of individuals' mistreatment the fuel color has been mentioned.The illuminate colours a physics-based technique and employing a applied mathematics grey edge technique that exploits the inverse intensity chromaticity color area has been calculable. This fuel map is treated as texture maps.AN data on the distribution of edges on fuel maps square measure extracted. In order to outline the sting data, a brand new algorithmic rule supported the HOG descriptor and edge-points, referred to as Hog edgeis planned. Respectable results are achieved over net pictures andbeneath cross-database training/testing. The proposed technique needs solely a least of human interaction and provides a crisp statement on the credibleness of the image. In addition, it's a serious progress within the exploitation of fuel color as a rhetorical cue.

7. References

[1] Tiago Jose de Carvalho,Christian Riess,Elli Angelopoulou and Helio Pedrini "Exposing Digital Image Forgeries By Illumination Color Classification" IEEE Trans. Inf. Forensics Security ,Vol. 8, no. 7, pp. 1182 - 1194, July 2013. ISSN: 2231-5381.

[2] A. Rocha, W. Scheirer, T. E. Boult, and S. Goldenstein, "Vision of the unseen: Current trends and challenges in digital image and video forensics," ACM Comput. Surveys, vol. 43, pp. 1–42, 2011.

[3] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," Inf. Hiding, vol. 6387, pp. 66–80, 2010.

[4] H. Farid and M. J. Bravo,"Image forensic analyses that elude the human visual system," in Proc. Symp. Electron. Imaging (SPIE), 2010, pp. 1–10.

[5] Y. Ostrovsky, P. Cavanagh, and P. Sinha, "Perceiving illumination inconsistencies in scenes," Perception, vol. 34, no. 11, pp. 1301–1314, 2005.

[6] R. Kawakami, K. Ikeuchi, and R. T. Tan, "Consistent surface color for texturing large objects in outdoor scenes," in Proc. IEEE Int. Conf. Comput. Vision, 2005, pp. 1200–1207.

[7] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in Proc. IEEE Region 10 Conf., 2008, pp. 1–5.
[8] J. F. O'Brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," ACM Trans. Graphics, vol. 31, no. 1, pp. 1–11, Jan. 2012.
[9] J. Lukas, J. Fridrich, andM.Goljan, "Digital camera identification from sensor pattern noise," IEEE Trans. Inf. Forensics Security, vol. 1, no.2, pp. 205–214, Jun. 2006.
[10] H. Farid, A 3-D lighting and shadow analysis of the JFK Zapruder film (Frame 317), Dartmouth College, Tech. Rep. TR2010–677, 2010.
[11] M. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, 2005, pp. 1–10.
[12] M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inf. Forensics Security, vol. 3, no. 2, pp. 450–461, Jun. 2007.
[13] M. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in Proc. Int.Workshop on Inform. Hiding, 2007, pp. 311–325.
[14] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Dec. 2010, pp. 1–6.
[15] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.
[16]Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[17]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[18] Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[19]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[20] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[21]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[22]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[23] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[24] Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[25]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
[26]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[27]R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[28]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[29]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[30]Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.