International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 04, 2019
ISSN: 1475-7192

Image Forensics Tool with Steganography Detection

Ed Keneth Joel Melanie, Maryam Var Naseri and
Nor Afifah Binti Sabri

Abstract--- *The problem context that inspired and motivated this project idea is that as the quote says a picture or image speaks a thousand words. An Image is forensically rich media it contains a lot of metadata you can extract for any Digital Forensics investigation and it can answer the 3 w's. which is what (what device is used to capture the picture or Image), where (The location where the picture or image was capture) and when (the exact time and date when the image was capture). The current issues are that most of the current image forensics tools is their output is too complex to understand, for students starting out their studies into digital forensics its quite difficult for them to comprehend some details of their output. The tool will also detect if the image has been tempered with if any hidden messages or items is stored inside using steganography. The project is an Image Forensics Tool with Steganography Detection, which can aid in a digital forensics' investigation where by the investigator is required to get metadata out of any Digital image.*

Keywords--- *Image Forensics, Image Forgery Detection, Image Steganography, Image Steganalysis, Image Processing.*

I. INTRODUCTION

We are currently in a revolution in Digital images, many developments have been made in Digital images such as the implementation of artificial intelligence (AI) and computational imaging. As like everything in this world Digital images advancements can be used for good and bad things. Due to advancement of digital image processing software and editing tools, an image can be modified and manipulated. These modifications are very difficult to be identified visually by a human eye. In the recent years there has been massive increase in digital image forgeries online and as well by the media. Which is a very dangerous trend, which diminishes the credibility of digital images. Therefore, developing techniques to verify its ethnicity, this is very crucial because images are presented as evidences in court of law as various scenarios such as part of financial documents, Medical documents, and news items.

A Digital image life cycle has three phases where it can be represented, which is acquisition, Saving and Editing. While it is in acquisition phase the diaphragm manages the amount of light from the scene that falls onto the image sensors, whilst the shutter speed controls the time of the exposure and the lens forms a coherent image onto the sensors. In general, digital cameras utilizes CMOS (Complementary Metal Oxide Semiconductor) or CCD (Charge-coupled device) as image sensors. These sensors are made from light sensitive diodes which are called photosites. The sensor captures data for each single pixel or picture element in an image thus generating grayscale images

Ed Keneth Joel Melanie, Student at Asia Pacific University. E-mail: tp043358@mail.apu.edu.my
MaryamVar Naseri, Lecturer at Asia Pacific University. E-mail: maryam.var@staffemail.apu.edu.my
Nor Afifah Binti Sabri, Lecturer at Asia Pacific University. E-mail: afifah@staffemail.apu.edu.my

Received: 18 Sept 2019 | Revised: 20 Oct 2019 | Accepted: 20 Nov 2019

because the sensors isn't able to differentiate between colours and the colours of an image is usually depicted as mixture of various percentages of the primary colours which is Red, Green and Blue (RGB). The information of the colours is gained by using a mosaic of the Colour Filter Array (CFA).

II. MATERIALS AND METHODS

The research conducted via questionnaire received a little over the target amount of engagements, which was 50, with 54 engagements. The questionnaire participants came from different age groups with the majority from the 18 to 25, and they were mostly student at university level. Which is the target user for this project. The two alarming facts gathered through the questionnaire firstly was that the majority of the participants download digital images from unknown sources willingly. Secondly is that they are not aware or have been educated about the types of digital crimes, image forgeries and Steganography. The positive fact is that those who knows about steganography prefers the Least significant Bit encoding, which is the steganography encoding type that will be implemented in this project. Through the observation the data gathered shows that digital images are common attack vectors by hackers over the past few years. Especially by sending malicious digital images embedded with viruses and backdoors on social media platforms, emails and other internet-based messaging services. Which shows the importance and the relevance of this project.

2.1 Image Forgery Detection Methods

There are many methods to Image forgery detection methods, and it is classified into approaches passive and active image forgery detection. The active approach requires the digital image to be pre-processed for watermark embedding or signature generation, furthermore the active approach limits their application in digital forensics investigation. Whereas the passive approach techniques do not require watermark and signature-based methods, the passiveapproach can be divided into five types (Format based, Pixel based, Camera based, Geometry based, Physical environment based)

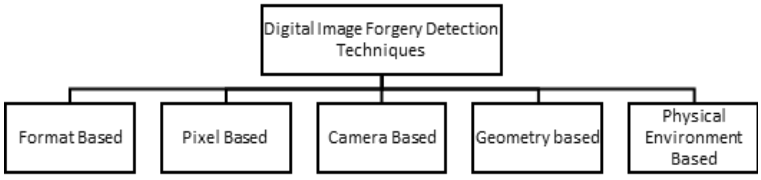

Figure 1: Digital Image Forgery Detection Techniques [1]

2.2 Steganography

Steganography is the hiding of a message within another one so that it's not detected. Its concept is based that the message to be transmitted and it's not visible. The word steganography itself comes from the Greek word that means covered writing. There are several types of steganography encoding or embedding. Steganography also occurs in technology it is does by hiding data into a digital media such as images, videos. Steganalysis is the process or art of detecting the presence of steganography. Digital Images can be represented in various ways and its pervasive application in our daily life nowadays. Hence why it makes it more appealing to hide data inside or within a digital image.

Received: 18 Sept 2019 | Revised: 20 Oct 2019 | Accepted: 20 Nov 2019

There are three common criteria or requirements for steganography that is imperceptibility, security and capacity. Steganography is vulnerable to certain attacks, these attacks can be either passive of active, hence the need of security. Capacity to be successful in hiding the secret message it is useful, if the hiding capacity should be as high as possible. Imperceptibility, Stego-Images must not have any highly visible artefacts. There are also certain criteria for steganalysis. Furthermore, Steganalysis main objective is to identify whether a suspected or unsuspected medium is embedded with any secret data. The method used to analyse a suspicious medium has four possible results, which is (TP) True positive, (FP) False positive, (TN) True negative, (FN) False negative.

(TP), means that the stego medium is classified as Stego-Image correctly.

(FP), means that the cover medium is classified as Stego-Image wrongly.

(TN), means that the cover medium is classified as Cover-Image correctly.

(FN), means that the stego medium is classified as Cover-Image wrongly.[23]

2.2.1 Image Steganography

Image Steganography has made progress in the recent years. Researchers has mainly focus on hiding data in color images and grayscale images, Grayscale images is considered to be more suitable than color images for data hiding. The reason why is that grayscale images is considered more suitable is because the correlations between the color components in color images can easily reveal the trace of embedding. Spatial steganography encoding is done by the embedding to directly change the image pixel values to hide the data, its embedding rate is most often measured by (BPP)bit per pixel. There are several types steganography encoding such as Least Significant Bit (LSB) Based Steganography, Multiple Bit-planes Based Steganography and Noise-adding Based Steganography.

Least Significant Bit (LSB) Based Steganography, is one of the most conventional techniques. It has the capacity to hide large secret message into a cover image. The embedding process works by replacing the Least Significant Bit (LSB) of randomly chosen pixels un the cover image with the bits of the secret message.

2.2.2 Image Steganqlysis

Image steganalysis is regarded as a two-class pattern classification, which aims is to identify whether the testing medium is a Stego medium or Cover medium. Image steganalys is divide into two methods universal methods and specific methods. The universal method can be utilized to detect various kind of steganography and it does not require the knowledge of the type of embedding operations that has been used, its often referred as the blind method. the specific methods

The universal steganalytic method utilizes a learning-based strategy, that involves a testing and training stage. Both of the stages are used in the feature extraction step. The function of the feature extraction step is to map a high-dimensional image to a low dimensional image. The training stage aim is to get a trained classifier. There are various types of classifiers such as support vector machine (SVM), neural network (NN), Fisher linear discriminant (FLD), etc., can be chosen. The classifier forms decision boundaries to separate the feature space into two regions positive and negative regions with the use of the feature vectors that is extracted from the training images. Testing Stage Utilizes the trained classifier to classify the image under analysis according to its feature vector. If its feature

vector identifies as positive region, it will be therefore classed as a positive class (Stego Image). Contrarily if the feature vector identifies the image as negative region, it will be classed as a Negative class (cover Image). The process is shown in the figure below

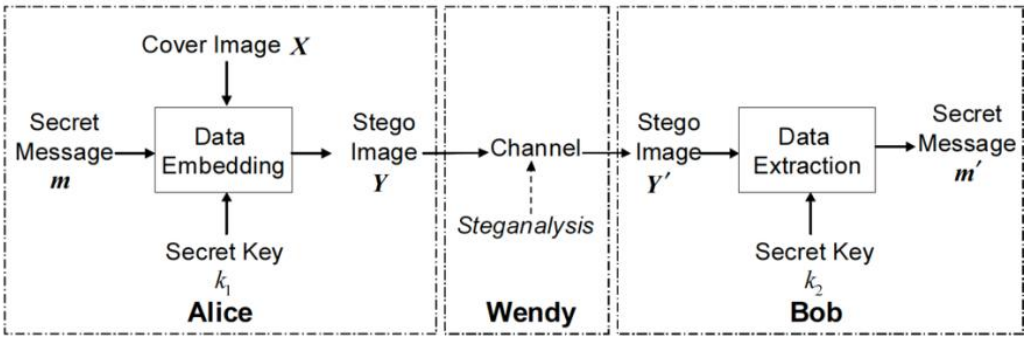

Figure 2: Steganography and Steganalysis [23]

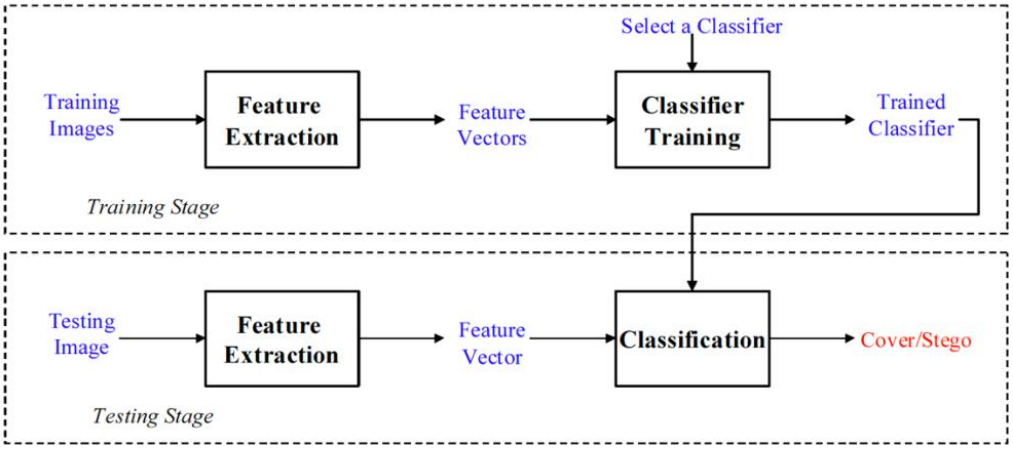

Figure 3: Universal Steganalytic Method [23]

III. Results And Discussion

3.1 Similar Systems

There is currently several Image forensics Tools in existence, all of them differing from each other but has some similar features. The Image forensics tools span from paid and free versions. They are based on different platforms some are windows system based some a web based and some are even open source. But they do have their limitations.

3.1.2 Limitations of the Similar Systems

The main limitations of these above mention tools are that they are limited to analyses JPEG format with the exceptions of JPEGsnoop and FotoForensics, when analysing other formats some features are disabled, or they are unable to render. The tools also lack cryptographic and steganographic detection. Thus, making them unable to identify if there is any hidden data embed in a digital image. Their output is quite complex and do not the access to print out the report of the analysis.

Received: 18 Sept 2019 | Revised: 20 Oct 2019 | Accepted: 20 Nov 2019

Table 1: Simliar Systems

Tool Name	Free or Paid	Features	Platform
FotoForensics	Both	• Error Level Analysis • Metadata Analysis • Last-Save Quality • Color Adjustments • Parasite Detection	Web-Based
JPEGsnoop	Free	• Decode JPEG, AVI (MJPG), PSD images • MCU analysis with detailed decode • Extract embedded JPEG images • Detect edited images through compression signature analysis • Report all image metadata (EXIF) • Batch file processing	Open Source Windows Based
Ghiro	free	• Error Level Analysis • Hash digest • Hash list matching • Strings extraction • Signature engine	Open Source Linux Based
Forensically	Free	• Clone Detection • Error Level Analysis • Noise Analysis • PCA Principal component analysis on the image.	Web-Based

In comparison to the proposed tool. It will also contain Image processing and Steganography detection components, which is not common component for these tools mentioned above. The image processing feature can make manipulated regions stand out in various ways. For example, they can be darker or brighter than similar regions which have not been manipulate. The steganography detection tool will have is the ability to detect if there's any embedded data or information in the image. Furthermore, it will have capability report all image metadata (EXIF).

IV. DESIGN

The programing language chosen to develop the tool is C# programming language was chosen because its characteristics such as it easy coding in the syntax is less complex like for example java. Its object oriented which will make implementing the Graphical User Interface (GUI) simpler. The nature of the programming language will make work well with the proposed software development methodology, which is the scrum method. The developer can develop several aspects of the tool and then in the final stages link them together by using C#. Furthermore, the tools such as GDI+, which has the proper classes in-built that will make

The Image forensic tool with Steganography detection has three main core features which is the Image File Metadata Extraction, Image Processing, and Steganography detection. The tool itself has the ability to read any digital image format available to date. Each of these three core features has sub features included some of the sub features are optional for example the save file feature and some are mandatory for example the hashing of report feature.

Image File Metadata Extraction, this feature will require the user to upload or open an image file unto the tool and the system will attempt to extract the metadata or exif data of the image file, Then list the data down so the user can view it and the user will have the option to save the Metadata gathered by the system into a text file. While saving the file the tool will perform hashing using SHA256 hash, so that the data integrity is preserved.

Received: 18 Sept 2019 | Revised: 20 Oct 2019 | Accepted: 20 Nov 2019

Image processing this feature will also require the user to upload or open an image file unto the tool. This includes the conversion of the digital image file by using five different image filters and perform thresholding. The filters will be utilised so that the user can examine the digital image file. The filters include red filter, green filter, yellow filter, grayscale filter and a negative filter. Furthermore, the user has the option to save the processed image file in any digital image format.

Steganography detection, this feature will require the user to upload or open an image file unto the tool as well. When the user upload or open the image file unto the system, it will check and analyse the image file to see if there's a file embedded within the image file. If the tool detects a file or text embedded in the digital image. The user has the option to extract and save the file or text embedded within the digital image file.

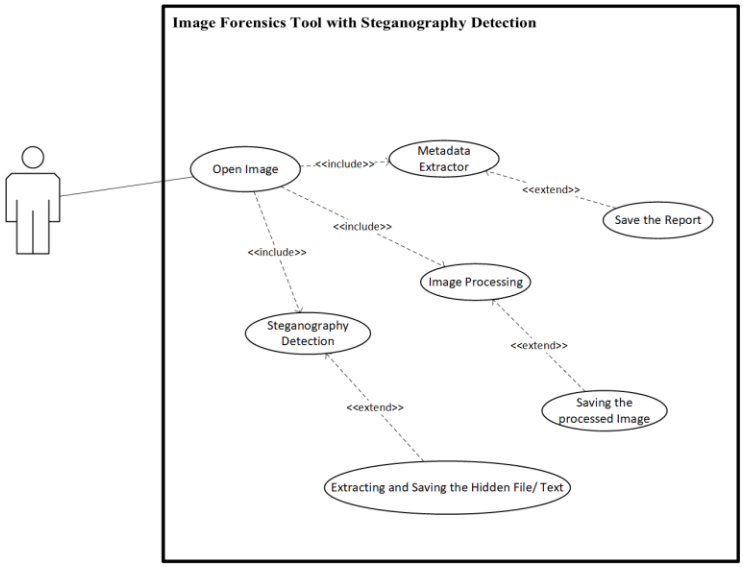

Figure 4: Use Case Diagram for the Image Forensics Tool with Steganography Detection

V. CONCLUSION

The Image forensics tool with steganography detection has a lot of merits, as many researchers from previous studies has stated. The lack of awareness about digital crimes and digital image forgery was very alarming with people sharing and downloading images from unknown sources online.

This project was able to achieve all its set targets and the tool was successfully implemented.

The tools three main features image metadata extractor and steganography detection of the tool works without any glitches. The other features such as reports saving and hashing also works tremendously well.

The researcher was able to make thorough investigation. The questionnaire gave the researcher great insight about the target users audience, about their online activities. The people who participated in the questionnaire doesn't know how to detect if a digital image has been tempered with or aware that digital image forgery is a crime.

For further future enhancements to the tool will be to add error level analysis and add more steganography encoding to the tool. The error level analysis will permit the user to identify area with different compression areas

with a digital image. Reason for suggesting adding more steganography encoding is that hackers most often don't use the most popular encoding to embed malicious file into a digital image file.

ACKNOWLEDGMENTS

This paper would not have been possible without, firstly for the amount of effort and commitment of the authors put to make this project successful. I would like to thank my colleagues for their insight and help they provided to me during this project and the people who participated in my survey and the unit testing of the tool. Lastly, I would like to thank the people who research about Image Forensics tool and Steganography by providing insights via articles and papers. which I have sited their work accordingly. I am extremely grateful for the individuals I have mentioned above, because they were vital for the success of this final year project.

REFERENCES

[1] M.D. Ansari, S.P. Ghrera and V. Tyagi, "Pixel-Based Image Forgery Detection: A Review," *IETE Journal of Education,* 2014.

[2] B. Li, J. He, J. Huang and Y. Q. Shi, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 2, no. 11, p. 2, 2011.

[3] N. Schonning, N. Potapenko, t. pratt, M. Hoffman, M. Jones, L. Latham and M. Wenzel, "How to: Read Image Metadata," 2017. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/framework/winforms/advanced/how-to-read-image-metadata. [Accessed 30 1 2019].

[4] Merriam Webster, "meme," 2019. [Online]. Available: https://www.merriam-webster.com/ dictionary/meme. [Accessed 21 1 2019].

[5] M. Kan, "Hacker Uses Internet Meme to Send Hidden Commands to Malware," 2018. [Online]. Available: https://sea.pcmag.com/news/30767/hacker-uses-internet-meme-to-send-hidden-commands-to-malware. [Accessed 20 1 2019].

[6] T. Marques, "PNG Embedded – Malicious payload hidden in a PNG file," 2016. [Online]. Available: https://securelist.com/png-embedded-malicious-payload-hidden-in-a-png-file/74297/. [Accessed 20 1 2019].

[7] D. Cid, "Malware Hidden Inside JPG EXIF Headers," 2013. [Online]. Available: https://blog.sucuri.net/2013/07/malware-hidden-inside-jpg-exif-headers.html. [Accessed 20 1 2019].

[8] Microsoft Doc, "Image.PropertyItems Property," [Online]. Available: https://docs.microsoft.com/en-us/dotnet/api/system.drawing.image.propertyitems?redirectedfrom=MSDN&view=netframework-4.7.2#System_Drawing_Image_PropertyItems. [Accessed 5 2 2019].

[9] Microsoft, "PropertyItem.Id Property," [Online]. Available: https://docs.microsoft.com/en-us/dotnet/api/system.drawing.imaging.propertyitem.id?redirectedfrom=MSDN&view=netframework-4.7.2#System_Drawing_Imaging_PropertyItem_Id. [Accessed 15 2 2019].

[10] Layola Marymount University, "webapps," [Online]. Available: http://cs.lmu.edu/~ray/notes/webapps/. [Accessed 29 January 2019].

[11] Microsoft, "Steganography - LSB," 2014. [Online]. Available: https://social.msdn.microsoft.com/Forums/vstudio/en-US/ae4c9a97-286b-467f-ae58-0774c9c0d7c6/steganography-lsb?forum=vbgeneral. [Accessed 16 2 2019].

[12] Microsoft, "PropertyItem Class," 2015. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/api/system.drawing.imaging.propertyitem?redirectedfrom=MSDN&view=netframework-4.7.2. [Accessed 15 2 2019].

[13] Cyberdiligence.com, "Email Forensics," 2014. [Online]. Available: http://www.cyberdiligence.com/email_forensics.html. [Accessed 24 November 2018].

[14] Paraben, "Paraben Email Examiner," 2018. [Online]. Available: https://www.paraben.com/products/e3-emx. [Accessed 24 November 2018].

[15] Veracode, "Common Malware Types: Cybersecurity 101," 2012. [Online]. Available: ahttps://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101. [Accessed 29 January 2019].

[16] Penn State Extension, "Standard Operating Procedures: A Writing Guide," 2019. [Online]. Available: https://extension.psu.edu/standard-operating-procedures-a-writing-guide. [Accessed 29 January 2019].
[17] J. Kennedy and M. Satran, "Property Item Descriptions," [Online]. Available: https://docs.microsoft.com/en-us/windows/desktop/gdiplus/-gdiplus-constant-property-item-descriptions. [Accessed 12 2 2019].
[18] Paweł Korus, "Digital image integrity – a survey of protection and verification techniques," Elsevier, 2017.
[19] D. Schweitzer, Incident Response: Computer Forensics Toolkit, 1 ed., *Wiley Publishing Inc.*
[20] B.S. Felix C. Freiling, "A Common Process Model for Incident Response and Computer Forensics," 2011.
[21] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. Volume 90, no. Issue 3, pp. 727-752, 2010.
[22] J. Kamenicky, M. Bartos, J. Flusser, BabakMahdiana, J. Koteraa, A. Novozamskya, S. Saic, F. Sroubek, M. Sorel, A. Zita, B. Zitova, Z. Sima, P. Svarc and J. Horinek, "PIZZARO: Forensic analysis and restoration of image and video data," *Forensic Science International*, vol. 264, pp. 153-166, 2016.
[23] X. Qiu, H. Li, W. Luo and J. Huang, "A universal image forensic strategy based on steganalytic model," ACM, pp. 1-1, 2016.
[24] N. Afshin, F. Razzazi and M.-S. Moin, "A dictionary based approach to JPEG anti-forensics," 2016 *IEEE 8th International Conference on Intelligent Systems* (IS), 2016.
[25] G. Fahmy and R. Wurtz, "Phase based forgery detection of JPEG anti forensics," 2016 *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2016.
[26] F. Wei, W. Kai, C. François and X. Zhang, "JPEG Anti-Forensics with Improved Tradeoff between Forensic Undetectability and Image Quality," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1211 - 1226, 2014.
[27] H.T. Sencar and N. Memon, Digital Image Forensics: There is more to a Picture than Meets the Eye, *New York: Springer*, 2013.
[28] H. Farid, Fake photo, The MIT Press Publication, 2019.
[29] H. Farid, Photo Forensics, MIT press, 2016.
[30] D. Cabrera, "Get image file metadata in C# using .NET," 2018. [Online]. Available: https://medium.com/@dannyc/get-image-file-metadata-in-c-using-net-88603e6da63f. [Accessed 4 2 2019].
[31] D. Noakes, "C# Exif code - sample usage," 2011. [Online]. Available: http://www.holmessoft.co.uk/homepage/Software/ExifUsage.htm. [Accessed 11 2 2019].
[32] S. Ambli, "Getting Started with Image Processing," 2014. [Online]. Available: https://code.msdn.microsoft.com/Getting-Started-with-Image-74a37d8b/sourcecode?fileId=113114&pathId=208812097. [Accessed 15 2 2019].
[33] R. Stephens, "compare images to find differences in c," 2015. [Online]. Available: http://csharphelper.com/blog/2015/07/compare-images-to-find-differences-in-c/. [Accessed 17 2 2019].
[34] R. Stephens, "use image subtraction to compare images in c," 2015. [Online]. Available: http://csharphelper.com/blog/2015/07/use-image-subtraction-to-compare-images-in-c/. [Accessed 15 2 2019].
[35] H. soboh, "Steganography: Simple Implementation in C#," 2014. [Online]. Available: https://www.codeproject.com/Tips/635715/Steganography-Simple-Implementation-in-Csharp. [Accessed 17 2 2019].
[36] A. Tanasi and M. Buoncristiano, "Ghiro," 2018. [Online]. Available: http://www.getghiro.org/. [Accessed 29 12 2018].
[37] A. Tanasi and M. Buoncristiano, "Image Forensic," 2019. [Online]. Available: http://www.imageforensic.org/. [Accessed 12 1 2019].
[38] N. Krawetz, "Foto Forensics," 2019. [Online]. Available: http://fotoforensics.com/. [Accessed 10 1 2019].
[39] B. Turnbull and S. Randhawa, "Automated event and social network extraction from digital evidence sources with ontological mapping," *Digital Investigation*, vol. 13, pp. 94-106, 2015.
[40] D. Quick and K.K. R. Choo, "Big forensic data reduction: digital forensic images and electronic evidence," *The Journal of Networks, Software Tools and Applications*, vol. 22, 2016.
[41] N. Singh and S. Joshi, "Digital Image Forensics: Progress and Challenges," *National convention of Electronics and Telecommunication Engineers*, vol. 31, 2015.
[42] B.V. Prasanthi, "Cyber Forensic Tools: A Review," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 41, no. 5, 2016.
[43] M. Cicconet, H. Elliott, D. Richmond, D. Wainstock and M. Walsh, "Image Forensics: Detecting duplication of scientific images with manipulation-invariant image similarity," arXiv., 2018.

[44] A. Singh and J. Malik, "A Comprehensive Study of Passive Digital Image Forensics Techniques based on Intrinsic Fingerprints," International Journal of Computer Applications, vol. 116, no. 19, 2015.

[45] S. Wickramasinghe and S. Hettiarachchi, "Use of Computer Forensics and Its Implications," *Research Gate*, 2016.

[46] F.Y.L. Chow, "Computer Forensics – An Essential Element of Modern IT Security," *Journal of Harbin Institute of Technology*, vol. 6, no. 2014, 2014.

[47] T.S. Amor Lazzez, "Forensics Investigation of Web Application Security Attacks," I. *J. Computer Network and Information Security*, 2015.

[48] L.R.J. III, Computer Incident Response and Forensics Team Management Conducting a Successful Incident Response, elsevier, 2014.

[49] N.M.N. Sundresan Perumal, "New Improvement in Digital Forensic Standard Operating Procedure (SOP)," *Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI*, vol.3, no. 104, 2011.

[50] I.L. L. A.C. Yun-Sheng Yen, "A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime," *International Journal of Computer Engineering Science (IJCES)*, vol. 2, no. 3, 2012.

[51] R.H.A. Baláž, "Forensic Analysis of Compromised Systems," *IEEE International Conference on Emerging eLearning Technologies and Applications*, vol. 10, 2012.

[52] M.T. Banday, "Techniques and Tools for Forensic Investigation of E-Mail," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, no. 6, 2011.

[53] Microsoft, "System. Drawing. Imaging Namespace," 2015. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/api/system.drawing.imaging?view=netframework-4.8. [Accessed 22 1 2019].

[54] P. Mary Jeyanthi, Santosh Shrivastava Kumar "The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region", *Theoretical Economics Letters*, 2019, 9, 752-760, ISSN Online: 2162-2086.

[55] P. Mary Jeyanthi, "An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors", *The Empirical Economics Letters*, Vol.18; No. 3, March 2019, ISSN: 1681-8997, which is in C category of ABDC List. http://www.eel.my100megs.com/volume-18-number-3.htm

[56] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Hybrid Metaheuristic techniques", *International Journal of Business Intelligence Research*, - Volume 5, Issue 1, April-2014.

[57] P. Mary Jeyanthi, "Industry 4.O: The combination of the Internet of Things (IoT)and the Internet of People (IoP)", *Journal of Contemporary Research in Management*, Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.

[58] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS)*, issue 3, volume 5, ISSN Online: 2350-1111 (Online).

[59] P. Mary Jeyanthi," An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions", *Vivekananda Journal of Research.* Vol. 7, Special Issue 1, May 2018, ISSN 2319-8702(Print), ISSN 2456-7574(Online).

[60] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Artificial bear Optimization Approach", *International Journal of Scientific & Engineering Research*, Volume 4, Issue 8, August-2013. URL: https://www.ijser.org/onlineResearchPaperViewer.aspx?Business-Intelligence-Artificial-Bear-Optimization-Ap-proach.pdf

[61] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Optimization techniques for Decision Making", *International Journal of Engineering Research and Technology*, Volume 2, Issue 8, August-2013. URL: https://www.ijert.org/browse/volume-2-2013/august-2013-edition?start=140

[62] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering*, Volume 3, Issue 3, March-2014. URL: https://ijarcce.com/wp-content/uploads/2012/03/IJARCCE7F-a-mary-prem-A-NEW-IMPLEMENTATION.pdf

[63] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", *International Journal of Web Technology* (ISSN: 2278-2389) – Volume-4, Issue-2. URL: http://www.hindex.org/2015/p1258.pdf

[64] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)

[65] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).

[66] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy" (*ICSMS2018).

[67] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).

[68] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[69] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management (ICMEB 2012).*

[70] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making", 2011 *IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[71] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", 2011 IEEE *International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[72] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", State level seminar on Computing and Communication Technologies. (SCCT-2015)

[73] Dr.P. Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, Bonfring Publication. Issue Date: 01-Apr-2019

[74] Dr.P. Mary Jeyanthi, "Customer Value Management (CVM) – Thinking Inside the box" – ISBN: 978-93-87862-94-4, *Bonfring Publication,* Issue Date: 16-Oct-2019.

[75] Jeyanthi, P.M., & Shrivastava, S.K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. *Theoretical Economics Letters*, 9(4), 752-760