International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

IMAGE FORENSICS TOOL WITH STEGANOGRAPHY DETECTION

[1]Mr More Praveen, [2]Ms. K Apurva,

[1,2] Assistant Professor,Dept. of CSE,

Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

Abstract : It is this issue background that has inspired and driven the development of this project concept. After all, as the old saying goes, "A picture is worth a thousand words." When it comes to forensically rich media, images contain a plethora of metadata that can be extracted for use in any Digital Forensics investigation. Images can also answer the three w's: what (what device was used to capture the picture or image), where (the location where the picture or image was captured), and when (when the picture or image was captured) (the exact time and date when the image was capture). Some of the present challenges include the fact that most of the existing picture forensics tools' output is too complicated to interpret, making it difficult for students just starting out in their studies in digital forensics to comprehend some of the subtleties of their output. Whether steganography is used to conceal messages or goods, the programme will also determine if the picture has been manipulated or if any concealed messages or items have been put inside it. An Picture Forensics Tool with Steganography Detection is being developed as part of this project. It may be used to assist in digital forensics investigations in which the investigator is needed to extract information from any digital image.

INTRODUCTION

Our present state of digital photography is characterised by a revolution; several advancements have been achieved in the field, including the use of artificial intelligence (AI) and computational imaging. In the same way that everything else in our world may be utilised for good or ill, digital image developments can be used for good or harm. The development of digital image processing software and editing tools has made it possible to modify and transform images in many ways. Visually, these alterations are quite difficult to distinguish from one another by the human eye. In recent years, there has been a significant rise in the number of digital picture forgeries that have been published online and in the media. In addition to being a potentially harmful trend, it also undermines the trust of digital photos. As a result, developing techniques to verify its ethnicity is extremely important because images are presented as evidence in court of law in a variety of scenarios, including financial documents, medical documents, and news articles.

The acquisition, saving, and editing stages of a digital picture life cycle may all be represented as three phases in a digital image life cycle diagram. While the camera is in the acquisition phase, the diaphragm controls the amount of light from the scene that falls on the image sensors, while the shutter speed controls the length of time the camera is exposed for and the lens forms a coherent image on the sensors, all while the camera is in the exposure phase. Photographic image sensors in digital cameras are typically comprised of CMOS (Complementary Metal Oxide Semiconductor) or CCD (Charge-coupled device) technology. These sensors are constructed from photosensitive diodes, which are also known as photosites. When a sensor captures data for each individual pixel or picture element in an image, it generates grayscale images. This is because the sensor is unable to distinguish between colours, and colours are typically depicted as a mixture of various percentages of the primary colours, which are Red, Green, and Blue (RGB). The information about the colours is obtained by using a mosaic of the Color Filter Array (CFA).

MATERIALS AND METHODS

The survey, which was done through questionnaire, had 54 responses, which was somewhat more than the 50 responses that had been targeted for the survey. Participants in the questionnaire represented a diverse range of ages, with the majority ranging from 18 to 25 years old, and the majority of them were university students. Which of the following is the intended user for this project? For starters, the poll revealed two frightening facts: First, a large percentage of those who took part in the survey voluntarily downloaded digital photographs from unidentified sources. It's also important to note that they are either unaware of or have not been trained about the many forms of digital crimes, such as picture forgery and Steganography. People that are knowledgeable about steganography prefer the Least Significant Bit encoding, which is the sort of steganography encoding that will be applied in this project, which is a great development. Data acquired via observation and data mining indicates that digital photographs have been a frequent attack vector for hackers over the last several years. In particular, through posting harmful digital pictures packed with viruses and backdoors on social networking platforms, sending emails, and using other internet-based messaging services, malware spreads. The significance and relevance of this initiative are shown in this way.

Image Forgery detection Methods

Image fraud detection techniques are many, and they are divided into two categories: passive image forgery detection and active image forgery detection approaches. The active technique necessitates that the digital picture be pre-processed in order to incorporate a watermark or generate a signature, and it also restricts their applicability in digital forensics inquiry and investigation. The passive approach approaches, on the other hand, do not need the use of watermarks or signature-based methods. The passive approach techniques may be split into five groups (Format based, Pixel based, Camera based, Geometry based, Physical environment based).

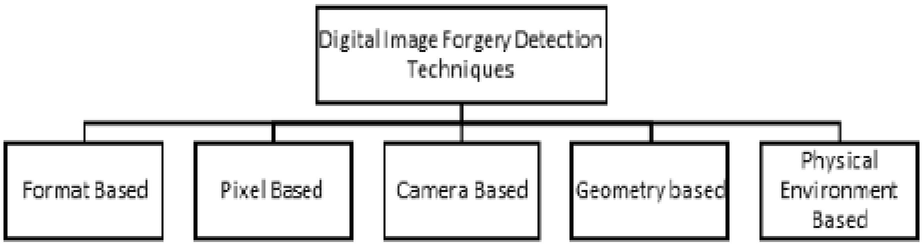

Digital Image Forgery Detection Techniques
Format Based
Pixel Based
Camera Based
Geometry based
Physical Environment Based

Figure 1: Digital Image Forgery Detection Techniques [1]

Steganography

Steganography is the process of concealing a message inside another message in order to avoid detection. Its notion is based on the fact that the message to be conveyed is not visible to the recipient. The name steganography itself derives from a Greek term that literally translates as "covered writing." There are several methods of steganography encoding or embedding that may be used. Steganography is also used in technology, and it is accomplished by embedding data into digital material such as photographs or movies, for example. In steganography, the technique or skill of identifying the existence of steganography is referred to as "steganalysis." Digital images may be portrayed in a variety of ways, and their widespread use in our everyday lives is becoming more common. As a result, it becomes more desirable to conceal data inside or within a digital picture as time passes.

Stegography may be classified into three categories, each with its own set of criteria or requirements: imperceptibility, security, and capacity. Steganography is subject to a variety of assaults, which may be either passive or aggressive in nature, necessitating the use of security measures. Because of the importance of being effective in concealing the secret message, it is important that the hiding capacity be as large as feasible. Stego-Images must be imperceptible, and they must not include any highly noticeable artefacts. In addition, there are several requirements for steganalysis. Furthermore, the primary goal of Steganalysis is to determine if a suspected or unsuspected medium contains any classified information. There are four potential outcomes from the approach employed to analyse a suspicious medium: (TP) True positive, (FP) False positive, (TN) True negative, and (FN) False negative.

(TP) indicates that the stego medium has been appropriately categorised as a Stego-Image.

(FP) indicates that the cover media has been incorrectly classed as Stego-Image.

(TN) indicates that the cover media has been appropriately categorised as a Cover-Image.

(FN) indicates that the stego media has been incorrectly classed as a Cover-Image. [23]

Image Steganography is a kind of image steganography in which one image is hidden inside another image.

Steganography of images has made significant strides in recent years. Researchers have concentrated their efforts mostly on concealing data in colour and grayscale photos. Grayscale images are believed to be more suited for data concealment than colour ones. Why grayscale photos are preferred over colour images is because the correlations between the colour components of a colour image may readily expose the trail of embedding, however with grayscale images this cannot be done. Space-based steganography encoding is accomplished by the embedding of data to directly modify the picture pixel values in order to conceal the data; the embedding rate is most often measured in bits per pixel (BPP). It is possible to encode information using steganography in a variety of ways, including using the Least Significant Bit (LSB), multiple bit-planes, and noise-adding.

Steganography based on the Least Significant Bit (LSB) is one of the most widely used methods in the world. It has the capability of concealing a significant hidden message under a cover picture. The embedding technique works by swapping out the Least Significant Bit (LSB) of randomly picked pixels in the cover picture with the bits of the secret message, which is stored in the cover image.

Steganqlysis of an image

Image steganalysis is considered as a two-class pattern classification technique whose goal is to determine if the testing media is a Stego medium or a Cover medium, according to the literature. There are two types of image steganalys approaches, universal methods and particular methods, which are divided into two categories. This approach, also known as the blind method, may be used to detect many types of steganography since it does not need the user to be aware of the sort of embedding operations that have been employed. Because of this, it is frequently referred to as the universal method. the exact strategies that are used

The global steganalytic technique is based on a learning-based strategy, which includes a testing and training step before it is implemented. The feature extraction process makes use of both of the steps described above. An picture with high spatial resolution is transformed into an image with low spatial resolution via the feature extraction stage. The goal of the training step is to produce a classifier that has been trained. There are several different kinds of classifiers that may be used, including support vector machines (SVM), neural networks (NN), Fisher linear discriminant (FLD), and others. With the help of the feature vectors that were extracted from the training pictures, the classifier creates decision boundaries to divide the feature space into two regions: positive and negative. The decision boundaries are used to divide the feature space into two regions: positive and negative. Testing Stage makes use of the trained classifier to categorise the picture under study according to its feature vector, as defined by the feature vector. If its feature vector detects a positive area, it will be classified as a positive class as a result of this identification (Stego Image). If, on the other hand, the feature vector identifies the picture as a negative area, the image will be classified as a Negative class, and vice versa (cover Image). The procedure is shown in the diagram below.

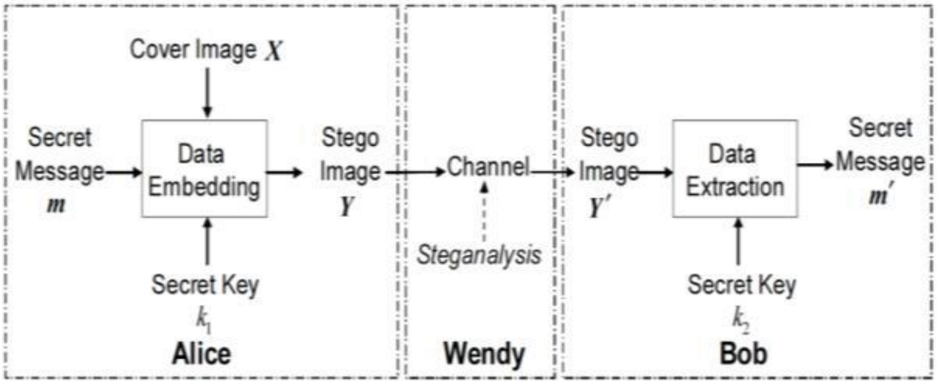


Figure 2: Steganography and Steganalysis [23]

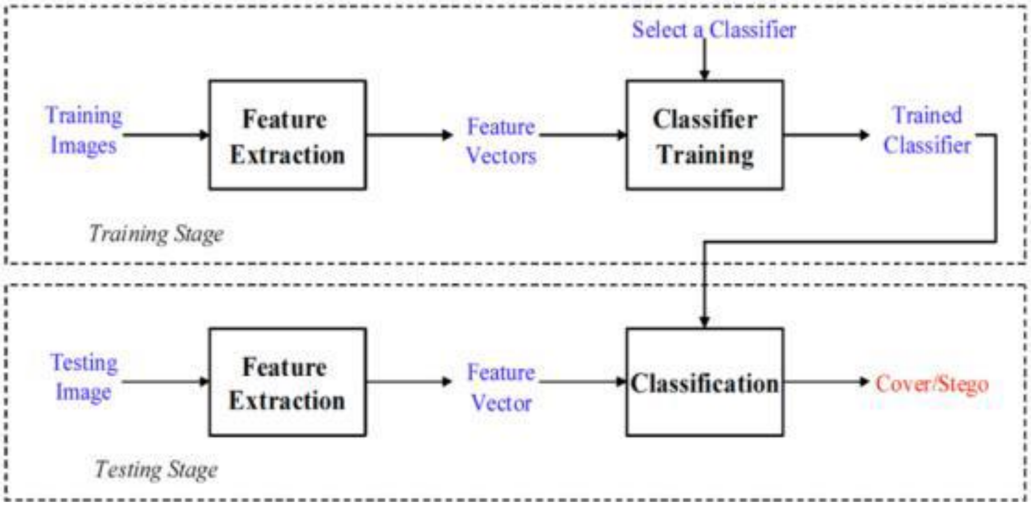


Figure 3: Universal Steganalytic Method [23]

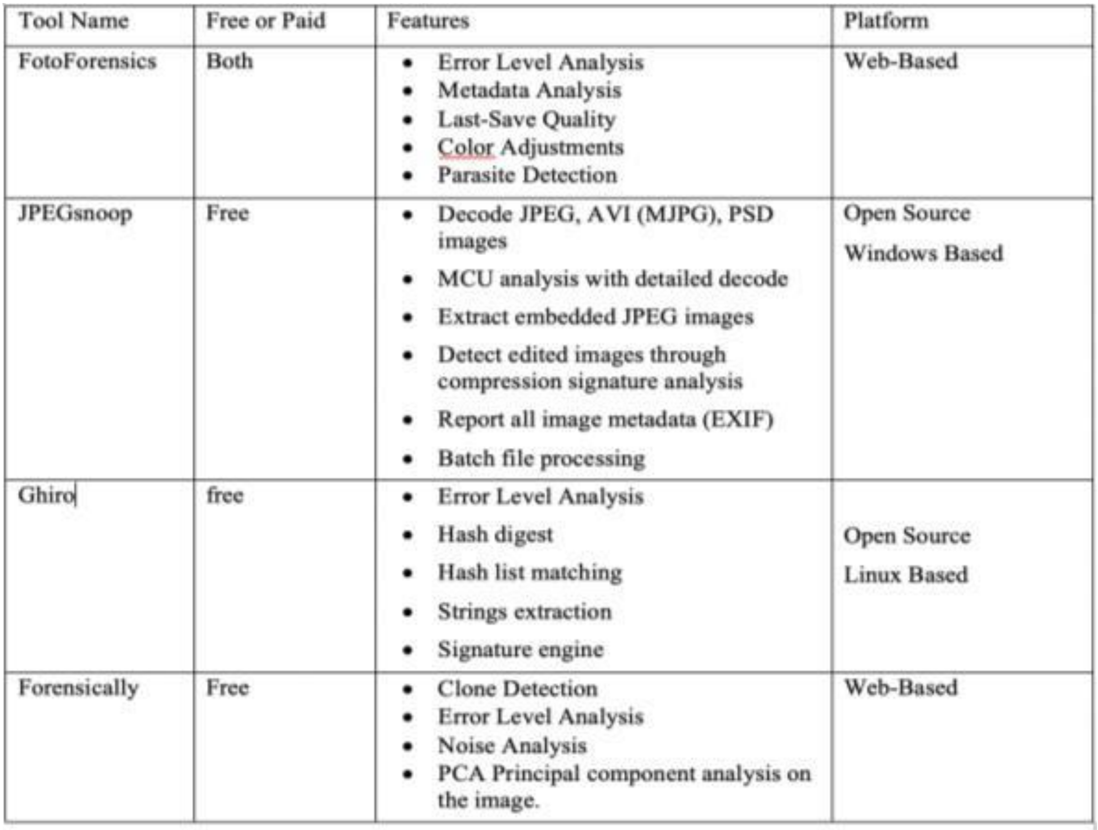
RESULTS AND DISCUSSION

Systems that are similar

Existing image forensics tools vary from one another, but they all have certain common aspects that make them useful in a variety of situations. Image forensics software is available in both commercial and free versions. Their platforms vary; some are based on the Windows operating system, while others are web-based and others even use open source software. They do, however, have their limits.

There are certain limitations to such systems.

The primary drawbacks of these programmes, with the exception of JPEGsnoop and FotoForensics, are that they are only capable of analysing the JPEG format; when analysing other formats, certain capabilities are disabled or they are impossible to display properly. In addition, there is no cryptographic or steganographic detection in the tools. As a result, they are unable to determine whether or not there is any concealed data included in a digital picture. Their output is rather sophisticated, and they do not provide an option to print a report of the analysis results.



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

CONCLUSION

As many academics from prior studies have noted, the image forensics tool with steganography detection offers a great deal of potential benefits. Individuals were sharing and downloading photographs from unknown sources online, indicating a general lack of knowledge about digital crimes and digital image fraud, which was very concerning.

It was possible for this project to meet all of its objectives, and the tool was effectively implemented.

The three primary aspects of the programme, which are picture metadata extraction, steganography detection, and steganography detection, all perform flawlessly. The other functions, such as the storing of reports and hashing, are likewise very well-designed.

The researcher was successful in conducting a comprehensive inquiry. The questionnaire provided valuable information to the researcher about the target users' audience and their online activity. The respondents who took part in the survey had no idea how to tell whether a digital icture has been manipulated, nor were they aware that digital image forgery is a criminal offence.

Future updates to the programme will include the addition of error level analysis as well as the addition of further steganography encoding to the tool. It will be possible for the user to detect regions with varying compression levels by doing an error level analysis on a digital picture. The reason for requesting that additional steganography encoding be added is because hackers do not always employ the most common encoding to insert dangerous files inside digital picture files, as is the case with most malware.

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].