Developing of Image Detection System with JPG Format using Error Level Analysis Technique

Andriani Silviana Primastuti
Department of Informatics
UniversitasAhmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Digital image manipulation is increasingly difficult to detect. Software for image processing is easily available, making it easier for someone to manipulate a photo. Image manipulation techniques produce fake photos that are difficult to detect. Crime cases that use photo manipulation are increasingly rampant in fake news (hoax). Detection of manipulated images in crime cases using digital forensics.The object of this research is the attack on the jpg image. The data collection method used in this research is the observation technique and literatul study (library). The method used in this research is Error Level Analysis (Ela). ELA is a forensic method for identifying parts of an image with different levels of compression. This research is concerned with detecting errors that occur due to a decrease in image quality. If a JPEG image is attached to another JPEG image, then saved as a JPEG, there will be a difference in the level of compression that occurs.

Keywords

Image, Jpeg, Image Manipulation, Image Forensics, Error Level Analysis

1. INTRODUCTION

Photo media is one of the communication media, namely media that can be used to convey messages/ideas to other people[1]. Photo media or the term photography is a medium that can be used to document an important moment or event.[2] As a medium that can record images, with all forms of life stopping in a photo such as pressing the pause button on the nature of life, photography captures and eternal use[3].

Regarding photography as a medium, in this subchapter, as a carrier of information, it has something to do with photography as a supporting medium in the world of journalism.[4] In general, photojournalism is produced through the photographic process to convey a message, information, an event that is interested to the public and disseminated through mass media[5].

The news that is spread is not certain of the truth, because in the current era of globalization it is very easy to manipulate data and change photos as evidence so that it allows many people to fake news and produce a lot of hoax news[6]. Digital image is one type of digital goods that has a very high level of risk and evidence of information loss[7].

Manipulated images and videos can be used for a variety of purposes, such as advertising, entertainment, crime and tricking investigators[8]. While from the reader's point of view, as in criminal cases, it is investigators, manipulated images and videos can mislead investigations and arrest the wrong perpetrators[9]. In the case of pornography, manipulated images and videos can damage the name and reputation of a person to the company[10]. Those who are negatively affected by the manipulation of images and videos are victims in large numbers because anyone can become a victim[11].

The field of digital image forensics, will assist law enforcement, intelligence, private investigations, and the media[12]. The increasingly advanced image technology at this time raises new issues and challenges in determining the authenticity of images in digital images[13]. Digital image forensics is one of the scientific methods in the field of research that aims to obtain evidentiary facts in determining the authenticity of images in digital images[14].

Disturbances are often found in image formats such as the Joint Photographic Experts Group (JPEG). JPEG is the most common format supported by devices and applications[15]. Therefore, the researcher will analyze the forensic image using the Error Level Analysis (ELA) technique[16]

Based on this description, to be able to overcome the problems that occur can be handled using one of the forensic field methods, namely the Error Level Analysis technique. To find out the original image that is widely circulated on social media by building tools that can be used to detect the authenticity of the image.

2. STUDY LITERATURE

2.1. Image Forensic

Forensic technique to check the authenticity of photo files is one part of forensic photography techniques, which are used to examine the evidence, in the form of image files which are one of the evidence that can be submitted to the court, if the photo files are in accordance with the standards set by law, but it can also be used for the function of documentation, intelligence analysis[17].

In checking the authenticity of photo files, several forensic techniques are used to prove and examine the photo, either by using software that is used to examine sensitive data contained in the photo with the help of photographic tools and techniques[18].

2.2.Digital Evidence

Digital evidence is information stored or transmitted in binary form that can be relied upon in court. It can be found on computer hard drives, cell phones, personal digital assistants (PDAs), CDs, and flash cards in digital cameras, among other places. Digital evidence is generally related to digital or electronic crimes, such as pornography, porting, identity, theft, phishing, or fraud in the form of credit cards or

ATMs[19].However, digital evidence is now being used to prosecute all kinds of crimes, not just digital crimes[20].

2.3. Error Level Analysis

If an image is saved in JPEG format, there will be a loss of quality[21]. ELA detects errors that occur as a result of the degradation.

a. In Error Level Analysis several things need to be considered in analyzing
b. Edges are pixels or call it small colorful dots that form a line following the original image area (forming a pattern).
c. Pattern is a collection of pixels that form the same image as the original image with detailed edge features and the same color. In the modified area, the pattern will form a distinct edge (less detail) with a lighter color.
d. Surface is an area or area that has the same color. For example, photos that have a wall or sky background. In the modified photo, this surface will form a rainbow[22].

2.4. Image Forensic

Forensic technique to check the authenticity of photo files, is one part of forensic photography techniques, which are used to examine evidence, in the form of image files which are one of the evidences that can be submitted to court, if the photo files are in accordance with the standards set by law, but it can also be used for the function of documentation, intelligence analysis[23].

In checking the authenticity of photo files, several forensic techniques are used to prove and examine the photos, either by using software that is used to examine sensitive data contained in photos with the help of photographic tools and techniques[24].

2.5. Acquisition

Acquisition is the process of making copies of digital evidence and documenting the methodology used and the activities carried out. The officer making the acquisition must select the most appropriate method based on the situation, cost and time, and document the decision chosen to use the particular method and appropriate tool[25].

The method chosen must also be practicable, the process can be repeated with the same results, and it can be verified that the copies are exactly the same as the original evidence. In circumstances where the verification process cannot be carried out, for example when the acquisition process is running, suddenly the original copy being made has error sectors, then in such a case the investigative officer conducting the acquisition must choose the most feasible method for carrying out the acquisition process. Re-acquisition and document it, then be able to explain why the reacquisition was made and be able to defend the argument.

3. METHOD

3.1 Research Stage

This study uses several data collection methods including a literature study where in this stage data collection is done by studying and reading books, literature, research journals that have to do with the problem being solved.

The next stage is observation where in this stage the observation of the existing forensic photo facilities and experimental and simulation techniques to observe and experiment the analysis process is carried out to determine the authenticity of the image.The stages of the research can be seen as shown in Figure 1 The research stage:

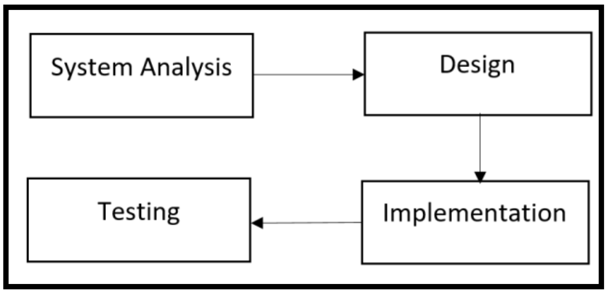


Figure 1. The Research Stage

A. System Analysis

The data that will be used for the analysis process are images or photos in jpeg format. An image saved in the JPEG format will experience a decrease in quality.In the compression analysis process that has been run, it will produce a JPEG file from the data used.

B. Design

The design process carried out in this research is as follows:

1) Data Design

The data that will be used for research is a file in JPEG format. The processed data is stored in a folder that has been determined to carry out an analysis process so that the data can be run properly.

2) Process Design

This stage is the basic stage in the system design process to be made. Here is the process design:Input photos or images to be analyzed, in this process the photos are in the form of files in .jpg format. The results of the photo or image input will be compressed using the ELA algorithm which will show the photo or image is original or has been digitally modified. Then it will issue an output in the form of an image with a .jpg format where the image displays the compressed results.

3) Interface Design

The system that will be designed to improve document security has several tools, such as:

a. Input image file or photo format *.jpg
b. Compression process for documents that have been inputted
c. Provision of a compressed photo download feature for analysis

C. Implementation

At the implementation stage, the system is made in a programming language that is understood by computers, in this study it will be implemented into a web programming language, namely HTML, and Python programming language.

D. Testing

The testing phase is carried out to ensure that the algorithm in the system that is made can be in accordance with the theory used and can display the compression results of an image.

3.2 Research Scenario

The research scenario is a stage to describe the research that will be carried out, the stages that will be carried out as in Figure 1 using the Error Level Analysis method will be scenario, the scenario that will be made is the preparation stage that must be carried out to carry out the investigative process in handling digital evidence starting from determining the image to the analysis.

In crimes that often occur in spreading false news (hoaxes) using photos, usually by manipulating the photo and then spreading it like the simulation shown in Figure 2.

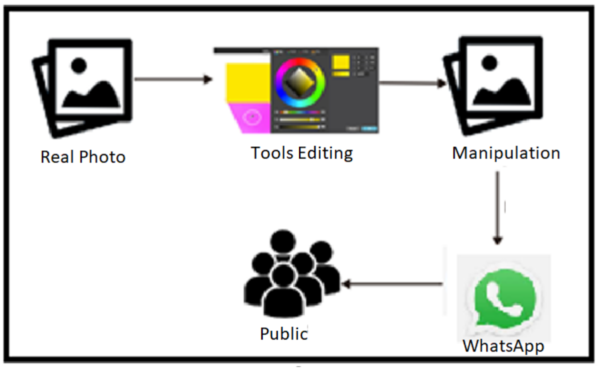


Figure 2. Photo Manipulation Spread Simulation

Figure 2 shows how the process of distributing manipulated photos to the public. In today's era, most people use WhatsApp to share information, therefore it is very easy to spread news through WhatsApp Messenger.

The perpetrator takes the original photo and then manipulates it using existing editing tools and adapts it to the news that will be disseminated, after the photo has been successfully manipulated it will then be distributed via WhatsApp and will be spread to the public in a way that people will believe the news because there are photos that support it and will be shared with other people. others in the person's WhatsApp contacts.

In the research scenario, it consists of several stages as shown in Figure 3.

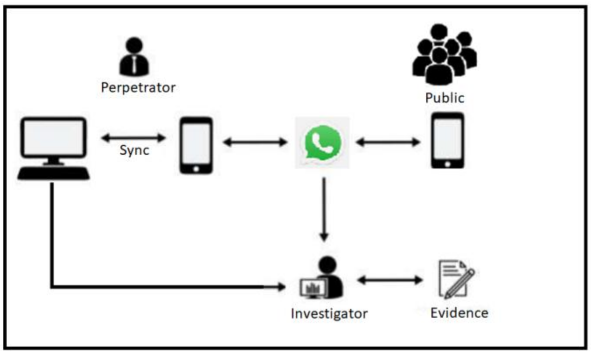


Figure 3. Research Scenario

Figure 3 is a research scenario of the forensic analysis process on photos, in this study the main focus is on analyzing the level of error in photos.

Perpetrators use smartphones and laptops to edit and spread hoax news and photos with WhatsApp messenger which will be accepted by the public via WhatsApp on their smartphone.

The investigator will analyze the evidence found on WhatsApp messenger and laptop and then an analysis will be carried out using an error level analysis technique. After obtaining the information, the next step is to analyze the information whether a photo is a real photo or an engineered one. The conclusion is to explain whether a photo is original or engineered and explain if the photo has been engineered it will show where the photo is changed or added.

4. RESULTS AND DISCUSSION

the acquisition of evidence through WhatsApp is done with 2 tools, namely FTK Imager and MobileEdit Forensic. The following is the result of the acquisition on a smartphone using mobileEdit Forensic can be seen in Figure 3.

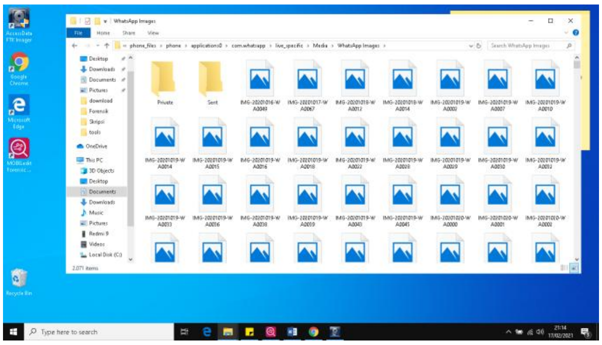


Figure 3 Acquisition with MobileEdit Forensic

Figure 3 is the result of the acquisition of the WhatsApp application on the smartphone. then the acquisition was made on WhatsApp web using FTK Imager, the results can be seen in the following figure 4.

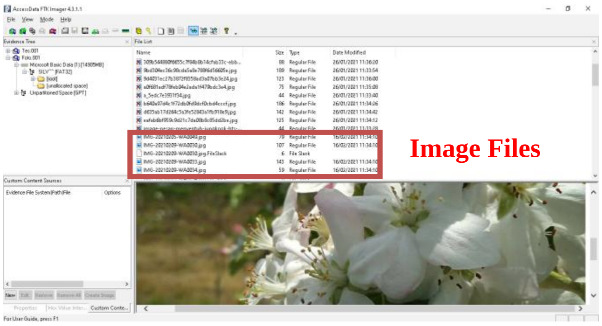


Figure 4. Acquisition with FTK Imager

After the results obtained from Figure 3 and Figure 4 above, it will then be focused on the image file on WhatsApp for further analysis using the system that has been built.

4.1. Requirements Analysis

4.1.1 Data Requirements Analysis

Data analysis is used to determine what data will be processed in system development. The data to be used is a file in the form of an image or photo with the extension *.jpeg. If the document used for processing in the system that was built uses other than documents with the extension *.jpeg, the system will not run properly or a notification will appear that only types of documents with the extension *.jpeg can be processed.

4.1.2 System Requirements Analysis

a. User Requirements

1) User can upload files in the form of images or photos

2) User can upload the result of the compression view

b. System Requirements

1) The system is able to validate the file format to be processed
2) The system is able to display the compression results of an image
3) The system is able to save photos to the database
4) The system is able to upload the results of the compression view

4.2 System Design

4.2.1 Use Case Diagram

Use case diagrams are used to describe what processes can be carried out by the system to be made, which can be seen in Figure 5.

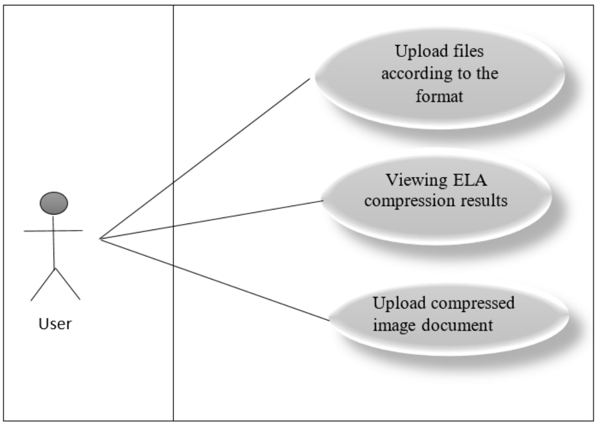

Upload files according to the format
Viewing ELA compression results
Upload compressed image document
User

Figure 5. Use Case Diagram

Figure 5 is a use case diagram display of users who will use the system. The use case has several flows that will be run by the user, namely the user can upload a document in the form of an image according to the specified format, the user can also upload an image document from the compression display.

4.2.2 Diagram Activity

Activity diagram is a diagram that can model the processes that occur in a system. The process sequence of a system is depicted vertically. Activity diagram is a development of Use Case which has activity flow. The activity diagram can be seen in Table 1.

Table1. Diagram Activity

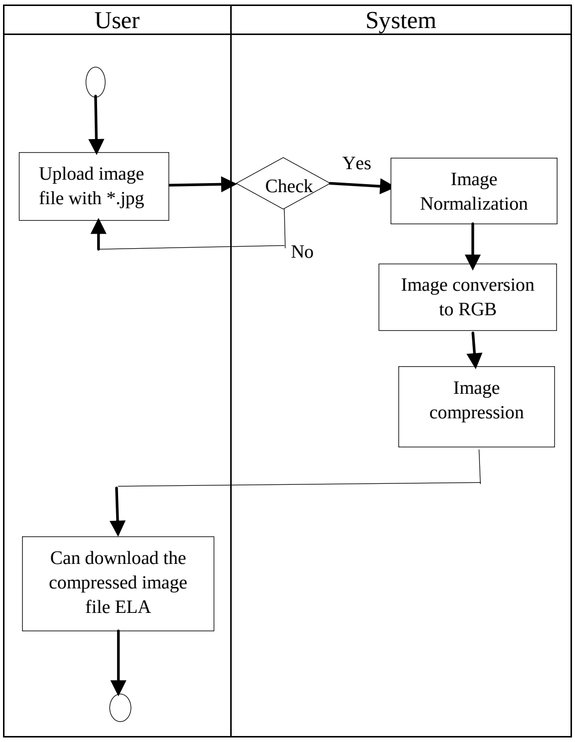
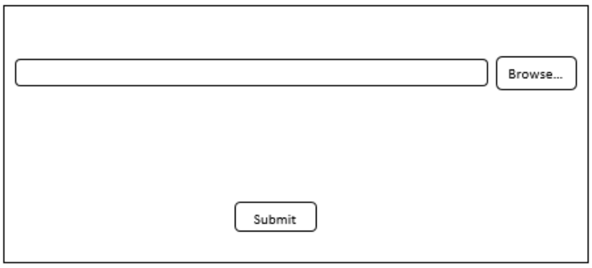


Table 1 explains that the user uploads an image then there is a condition that is run by the system to check the image format. If the image does not match the specified format, it will return to the image upload process until it matches the format, but if the conditions are met, it will continue to the next process.The next process is that the system divides the image into 8 x 8 blocks and recompresses it at an error rate of up to 90%.

Each square should provide approximately the same level of quality if the image is completely unmodified. Error rate of information lost while the image is saved in JPG format. The error rate will increase will increase on the save operation again. Subsequent save-back operations can reduce potential error rates and show through dark ELA results. After a number of save operations, the square grid can reach its minimum error rate. Frequency and details can be lost by each save operation.

4.2.3 Interface Design

Interface design is the design of the appearance of the system to be built. The process of drawing is carried out to show the relationship between the user and the designed system. The results of the representation of the scheme are made in a simple manner and aim to make it easier for the user to read the information provided.The interface will be a medium of interaction between the user and the system. The following is a display of the system interface design that has been built, which can be seen in Figure 6.



Figurer 6. Interface Design 1

Figure 6 is an interface design for the initial display when the user opens the system. Then the display when the user has used the system and the system displays the results of the ELA extraction can be seen in Figure 7.

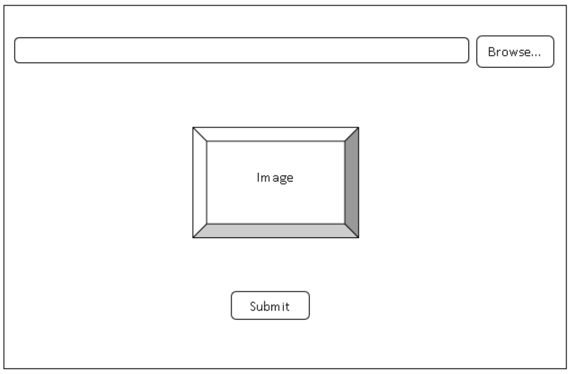


Figure 7. Interface Design 2

Figure 7 is a display design when the user successfully performs an ELA extraction of the uploaded image.

4.3 Implementation

4.3.1 System Workflow

The image detection system created is an implementation of the analysis and design that has been discussed previously by using the PHP and Python programming languages. The Python programming language is used to run the ELA algorithm process in detecting the authenticity of the image, while the PHP programming language is used to create a web-based system. In addition, it provides a coding standard that makes it easier to study the application system that is built and has a very small file size and is not too much in the configuration process.

4.3.2 System Implementation

This is the implementation of the design results into an application. Image detection system using error level analysis technique. The display of the system when it is run can be seen in Figure 8.

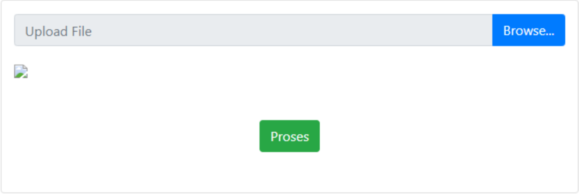


Figure 8. System Implementation

Figure 8 is the display of the system when it is first run,here you can directly upload images on the device via the browser menu. This system can only accept input with the extension .jpg only and will reject files with extensions other than .jpg. The following validation form can be seen in Figure 9.

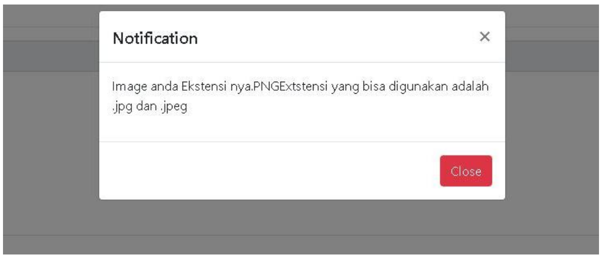


Image anda Ekstensi nya.PNGExtstensi yang bisa digunakan adalah .jpg dan .jpeg

Figure 9. Form Validation

Picture 9 is the display when the uploaded image does not match the specified format, namely .jpg. If the image is in accordance with the format then extracted, a display of the results of the ELA extraction will appear on the uploaded image. The results of the ELA extraction can be seen in Figure 10.

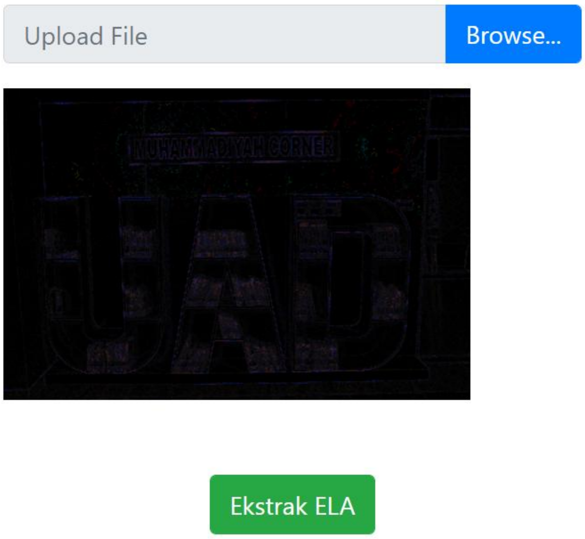


Figure 10. ELA Compression

Figure 10 shows the results of the ELA compression, the image can be downloaded by clicking on the image and it will automatically download. After the image is successfully downloaded, it can be analyzed and then it can be used as digital evidence

4.4 Testing

The process of detecting object matches in digital images begins with creating a scenario in the form of preparing two image files consisting of an original image and an edited/altered image. Then input the two images into forensic tools, in this study using Forensicallybeta, after that the images will be processed by the tools so that they get results that can be analyzed. The final stage is to analyze the two image detection results so that conclusions can be obtained.The following is a photo of the results of image manipulation and the original photo from a cellphone camera can be seen in Table 2.

Table 2. Edited and Original Photos

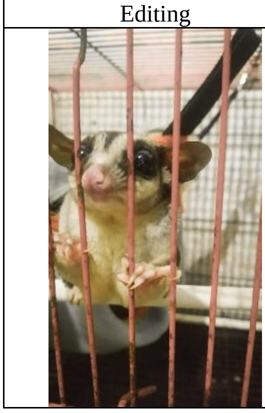
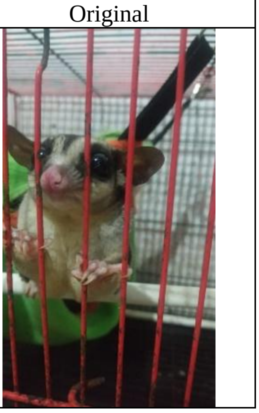
Editing	Original
	

Table 1 above is the original photo and the photo that has been manipulated which will then be used as a sample for detection using the system that has been built. The results of ELA using the system that has been built can be seen in table 3.

Table 3. ELA Result

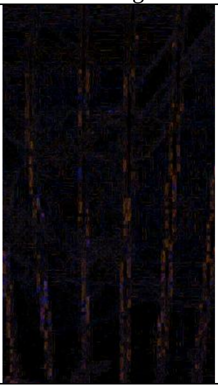
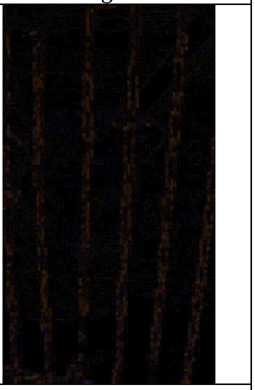
Editing	Original
	
MSE:25.4972 PSNR : 34.0999	MSE :25.3736 PSNR : 34.121

Table 3 is the result of compression from ELA which shows that photos that have been manipulated using editing tools appear to have a lot of blue dots and a few red dots. That is rainbowing. This rainbowing often appears when a photo is edited using products from Adobe such as Photoshop, etc. GIMP itself doesn't really produce this rainbowing effect. This proves that the photo has been edited using software made by Adobe.Using MSE and PSNR values for comparison.The lower the MSE value, the better, and the greater the PSNR value, the better the image quality, and conversely, the higher the MSE value, the more visible editing is in the image and the smaller the PSNR value, the more visible editing is in the image, so based on the MSE and PSNR values of the two photos, it can be ascertained that the photo on the left is undergoing the editing process

The following is an example of an analysis of the results of the ela on an image that has been pasted with other images, which can be seen in Figure 4.11

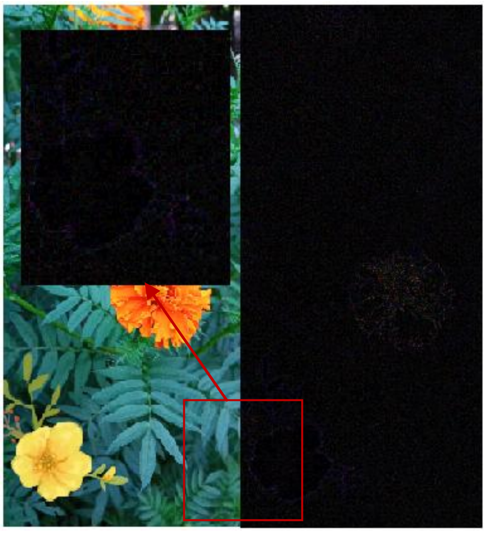


Figure 11. ELA Detection

Figure 4.11is the result of compression from ELA which shows that photos that have been manipulated using editing tools appear to have different dot colors, the part that is pasted with other images shows a darker color than the color of the surrounding dots, then on the image the color of the flowers in the red box has more blue dots and a little red, while other parts that are not edited will appear to have surfaces and patterns of the same color.

5. CONCLUSIONS

Based on the results of the research entitled Development of Image Detection System with JPG Format Using Error Level Analysis Technique, based on the digital evidence obtained in the images, it produces information on the crime of counterfeiting the news. In conducting the investigation, they succeeded in obtaining information in the form of the location of the photo that had undergone changes or had been engineered as evidence.By doing photo analysis, we can add insight to all of us in addition to increasing awareness of fake news. Before believing a news story, it's a good idea to first find out the source of the news and the authenticity of the evidence in the news.The method used in this forensic investigation uses the Error Level Analysis technique to obtain digital evidence in the form of rainbowing on the ELA compression results.The results of the calculation of the system that has been built. The System Usability Scale scores 89% so that the system is in the acceptable category.Hopefully in the future we can develop a system that can detect what percentage of photos are manipulated

6. REFERENCES

[1] Gani, R., &Kusumalestari, R. R. (2013). Photojournalism An Introduction (N. S. Nurbaya (ed.)). SimbiosaRekatama Media.

[2] Irwansyah, I., & Yudiastuti, H. (2019). Image Engineering Digital Forensic Analysis Using Jpegsnoop And Forensically Beta. Jurnal Ilmiah Matrik, 21(1), 54–63. https://doi.org/10.33557/jurnalmatrik.v21i1.518

[3] Mahardika, F., Khatulistian, A. D., &Kuncoro, A. P. (2018). Forensic.com Photo Review with Error Level Analysis and JPEG Techniques to find out the Original Image. Journal of Informatics: JurnalPengembangan IT PoltekTegal, 03(01), 71–75.

[4] Ela, A., Color, D. A. N., Array, F., &Berbasis, C. F. A. (2015). Integrated Digital Image Authentication System With Error Level Analysis (Ela) And Web Based Color Filter Array (Cfa). Computer Science and Information Systems, 12(2), 873–893. https://ejournal.unib.ac.id/index.php/rekursif/article/view/952

[5] Sugiantoro, B., Prayudi, Y., Informatika, M., Industri, F. T., & Indonesia, U. I. (2018).Analysis of Object Fitness Detector in Digital Image Using Matlab Through Sift Algorithm Method. 1(1), 20–27.

[6] YuliSulistyo, W., Riadi, I., Yudhana, A., Dahlan, A., StudiTeknikElektro, P., & Ahmad DahlanJalanSoepomo, U. (2018). Image Authenticity Detection Analysis Using Error Level Analysis Technique WithForensicallybeta. Seminar NasionalInformatika (SEMNASIF), 2018(November), 154–159. http://www.jurnal.upnyk.ac.id/index.php/semnasif/article/ view/2632

[7] Faroek, D. A., Umar, R., &Riadi, I. (2020). Image Authenticity Detection Using Error Level Analysis (ELA) and Principal Component Analysis Methods (PCA). Format : JurnalIlmiahTeknikInformatika, 8(2), 132. https://doi.org/10.22441/format.2019.v8.i2.006

[8] Sharif, N. M., Ali, M. N. S., & Abdullah, M. Y. H. (2014). Visual literacy on photographic images in digital forensic investigation. JurnalKomunikasi: Malaysian Journal of Communication, 30, 159–176. https://doi.org/10.17576/jkmjc-2014-30si-10

[9] Rahman, F. M., Putra, R. R. J., &Wihardi, Y. (2020).Statistical Analysis and Image Masking Implementation Based on Error Level Analysis Results on Digital Images. JATIKOM: JurnalAplikasi Dan TeoriIlmuKomputer, 3(1), 22–28.

[10] GedeNengahBayuDarmawan, I., Made Arya Sasmita, G., &WiraBuana, P. (2019). Development of Image Modification Detection Method Using Error Level Analysis Method. JurnalIlmiahMerpati (MenaraPenelitianAkademikaTeknologiInformasi), 7(1), 29. https://doi.org/10.24843/jim.2019.v07.i01.p04

[11] Sari, T., Riadi, I., &Fadlil, A. (2016). Image Forensics for File Engineering Detection Using Error Level Analysis. 2(1), 133–138. http://ars.ilkom.unsri.ac.id

[12]Saputra, A. P., &Widiyasono, N. (2017). Digital Forensic Analysis on File Steganography (Case Study: Drug Trafficking). JurnalTeknikInformatika Dan SistemInformasi, 3(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

[13] Wijayanto, H., Prabowo, I. A., &Harsadi, P. (2018). Optimization of Exif Metadata Shrinkage Using Null Value Substitution Techniques in the Case of Digital Image Security.JurnalIlmiah SINUS, 16(1), 1. https://doi.org/10.30646/sinus.v16i1.327

[14] Riadi, I. (n.d.). Email Forensic from Phishing Attack using Network Forensics Development Life Cycle Method.

[15] Lasaharu, S. (2021). Network Forensic on Web-Based Applications using Network Forensic Development Life Cycle Method. 1–7.

[16] Zaenudin. (2018).Forensic Metadata For Digital Evidence Correlation Analysis. 10(1), 85–89. https://dspace.uii.ac.id/handle/123456789/9452

[17]Priyadi, D. P., Budiyanto, U., Studi, P., Informatika, T., Informasi, F. T., Luhur, U. B., Utara, P., & Lama, K. (n.d.).Checking Image Authenticity Using Cryptographic Algorithm Advanced Encryption Standard 128 (Aes), Vigenere Cipher And Steganography Least Significant Bit (Lsb) Based On Android On Cv. Wiratama. 128, 1–7.

[18] AutoridadNacionaldelServicio Civil. (2021). 済無No Title No Title No Title. AngewandteChemie International Edition, 6(11), 951–952., 2013–2015.

[19] Al-Fajri, M. R., M.Kom, C., &Yusup, D. (2021). Image Forensic Analysis In Detecting Engineering Image Files With The Nist Method. JUSTINDO (JurnalSistem Dan TeknologiInformasi Indonesia), 6(2), 84–90. https://doi.org/10.32528/justindo.v6i2.5120

[20] Harahap, F. (2021).Detect Photo Manipulation With Forensicallybeta and Imageforensic Tools. orgDenganMetode Error Level Analysis (ELA). 2(3).

[21] Wijayanto, H., Prabowo, I. A., &Harsadi, P. (2018). Optimization of Exif Metadata Shrinkage Using Null Value Substitution Techniques in the Case of Digital Image Security.JurnalIlmiah SINUS, 16(1), 1. https://doi.org/10.30646/sinus.v16i1.327

[22] N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab, and R. Salleh, “An evaluation of Error Level Analysis in image forensics,” in 2015 5th IEEE International Conference on System Engineering and Technology (ICSET), 2015, pp. 23–28.

[23] J. Lorenzo-Navarro, M. Castrillón-Santana, and D. HernándezSosa, “On the use of simple geometric descriptors provided by RGB-D sensors for re-identification,” Sensors for re-identification,” Sensors, vol. 13, no. 7, pp.8222–8238, 2013.

[24] Pasquini, V. Conotter, and G. Boato, “RAISE - A Raw Images Dataset for Digital Image Forensics,” Proc. 6th ACM Multimed. Syst. Conf., 2015.

[25] M. Fauzi Rahman, “Digital Image Forensics: Metadata and Error Level Analysis To Detect Image Manipulation,” UniversitasPendidikan Indonesia, 2018.