Steganography Method with Digital Visible Watermarking Least Significant Bit Technique on Interactive Learning Media

Komang Ayu Triana Indah[1], Ni Wayan Wisswani[2], I Nyoman Kususma Wardana[3], and Ida Bagus Putra Manuaba[4]

[1,2,4] Information Technology Department, Politeknik Negeri Bali, Bali, Indonesia
[3] Electrical Engineering, Politeknik Negeri Bali, Bali, Indonesia
triana_indah@pnb.ac.id

Abstract. The issue of multimedia users in learning systems still stems from traditional patterns based on paper textbooks and evaluations in the classroom that are vulnerable to cheating, such as copies and leaks of questions from national exams, illegal use of media materials in the form of presentations and websites, and piracy of media substances. This calls for the development of new encryption technologies that incorporate specific data into other digital data, such as learning materials and assessment documents, utilizing the principles of steganography and the techniques of visible watermarking and least significant bit (LSB) encoding. To prevent digital test leaks and cheating during student evaluation, steganography—the science of communicating by using data in digital media so that the data cannot be known by others—is crucial to the evaluation process in this system. This application was developed using the Laravel Framework, Bootstrap V5.0, PHP8.3 JS for DOM software, and a MySQL relational database. The stages of concept, design, material collection, assembly, testing, and distribution are all included in the study process, which employs digital multimedia production using the Luther-Sutopo Method. The outcomes of this application include digital features for instructional materials that can be accessed on the website platform, as well as an interactive learning system.

Keywords: Digital Visible Watermark, Least Significant Bit, Multimedia

1 Introduction

The use of attractive or engaging images, videos, and sounds in multimedia to spark students' interest in learning is known as multimedia. When compared to other methods of material delivery, multimedia can also make it easier for pupils to receive some materials. The Multimedia Development Life Cycle (MDLC) approach, which consists of six stages—Concept, Design, Material Collection, and Assembly—can be used to generate multimedia. Through a digitalization process that includes file security (using the Steganography method) and watermarking patterns on instructional materials,

A. A. N. G. Sapteka et al. (eds.), *Proceedings of the International Conference on Sustainable Green Tourism Applied Science - Engineering Applied Science 2024 (ICoSTAS-EAS 2024)*, Advances in Engineering Research 249,
https://doi.org/10.2991/978-94-6463-587-4_29

learning media technology converts paper-based materials into digital media for use in student evaluations. A web-based multimedia application that uses steganography to digitally visible watermark learning documents to identify authentic assessment materials when gathering homework assignments and test results for students. It is anticipated that this research will support teachers in their instruction and assessment of the material, as well as improve students' comprehension of the material. In this study, Bootstrap v5.0, the Laravel Framework, and the PHP 8.3 JS for DOM program were used to develop the application (Rosmiyati & Mulyana, 2018).

2 Methodology

One Watermarking is one area of steganography. One way to preserve copyright is through watermarking, which is a private way to add information (embedding) into digital data media like text, photos, audio, and video (Kumar, 2019). Even after the digital data has been processed, transmitted, or redistributed, the information that has to be inserted must still be accessible. Digital watermarking refers to the information that will be introduced into digital data, while original data (host data) refers to the digital data that is inserted. The following five user interface concepts can serve as the architectural paradigm for designing interactive multimedia applications (Akter et al., 2014).

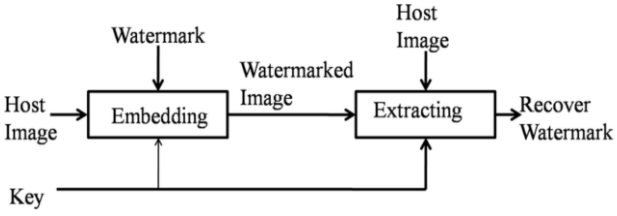

Figure 1. Embedding and extracting process of digital watermarking

By incorporating an undetectable secret signal into the host signal and keeping it there at all times, the watermarking technology encrypts data. The procedure for embedding and retrieving digital watermarking is depicted in Figure 1. when the watermark is extracted digitally by being included in the host signal. The choice of watermark structure and embedding approach has a significant impact on the effectiveness of a watermarking scheme. The resilience and invisibility of digital watermarking are two distinct metrics that can be used to assess its quality (Rasak & Zubair, 2018). The requirement of the original image to detect the watermark is known as non-blind watermarking, while the blind technique does not require the original image. Another way to classify watermarking is to transform domain watermarking and spatial domain watermarking. The watermarking scheme at the beginning of the process is in the spatial domain, where the mark is added by modifying the pixel value of the text that has been formatted in JPEG form. Some spatial domain watermarking approaches are based on modifying the least significant bit (LSB) of both: the host image and the

marked image of an image based on the assumption that LSB data is generally insignificant. In the image representation process, high-frequency signals are placed precisely in the pixel domain, while low-frequency signals. The process of inserting and extracting digital watermarking of host signals with keys is called as digital watermarking insertion process (Akter et al., 2014).

2.1 Interactive Learning

Interactive by incorporating an undetectable secret signal into the host signal and keeping it there at all times, the watermarking technology encrypts data. The procedure for embedding and retrieving digital watermarking is depicted in Figure 1. when the watermark is extracted digitally by being included in the host signal. The choice of watermark structure and embedding approach has a significant impact on the effectiveness of a watermarking scheme. The resilience and invisibility of digital watermarking are two distinct metrics that can be used to assess its quality.

2.2 Visible Watermarks

One branch of steganography is watermarking. Watermarking is one solution to protect copyright which is a technique for inserting (embedding) information into digital data media such as images, text, audio, and video in a confidential manner. The information to be inserted must be retrievable even if the digital data has been processed, distributed, or redistributed. The information that will be inserted into digital data is called a digital watermark, while the digital data that is inserted is called original data (host data). Digital data that has been inserted with a watermark is called watermarked data. Watermarking is the right solution to prevent copyright infringement (Venugopala & Sarojadevi, 2014).

2.3 Steganography

Watermark Data High Steganography is a science of communicating using the presence of communication or messages in digital media so that other people cannot know that there is a message in the media. Steganography is also the art for hiding a message so that the message cannot be known by third people, but the secret of the message can only be known by the sender and recipient of the message. Steganography is widely used in secret communication science where secret data is hidden or disguised in several multimedia objects such as audio, video, and images. Digital Watermarking with Least Significant Bit Technique One branch of steganography is watermarking. Watermarking is one solution to protect copyright which is a technique for inserting (embedding) information into digital data media such as images, text, audio, and video in a confidential manner. The information to be inserted must be retrievable even if the digital data has been processed, distributed, or redistributed. The information that will be inserted into digital data is called a digital watermark, while the digital data that is inserted is called the original set much higher than the bitrate, and then the bitrate may rise very high for short periods. If the transfer rate is set close to the bitrate, it places a

limit on how high the bitrate can increase within a short period (Kumar, 2009). Least Significant Bit (LSB) is an algorithm that in the process reads bits from a particular source so that the value of the last bit can be changed according to the desired bit. In the stegowater process, the LSB method is involved in the steganography process, header creation, and after the watermark process. The stages in the implementation of LSB are divided into 3 stages.

First Stage: Obtaining bit values, both from the image side and from the stego-text that will be used as the last bit value. The image obtains its bit value from the image intensity, while stego-text can utilize the ASCII code in converting letters to binary values or vice versa (Venugopala & Sarojadevi, 2014).

Second Stage: The decimal value obtained is processed to obtain the smallest bit value, equation (1) can be utilized.

$$k = Bst \bmod 2 \tag{1}$$

where:
k: The smallest bit value of Bst Bst: Binary from the image/stego-text

Third Stage: Entering the bit value into the image bit value. If Bc(x,y) is mod by 2 and has a value of k, then there is no change in the value of Bc(x,y). But if not, then the value of k will be tested. If k is 0, then continue to equation (2), while if k is 1, then continue to equation (3).

$$Bc'(x,y) = Bc\ (x,y) - 1 \tag{2}$$

$$Bc'(x,y) = Bc\ (x,y) + 1 \tag{3}$$

where:
Bc(x,y): Image bit value
Bc'(x,y): Image bit value after processing
k: Smallest bit value of Bst
If a watermark image is made into a grayscale image, which only has one intensity value, then if the intensity value on the pixels of the watermark image that has been converted into a grayscale image is used to increase or decrease the intensity value of the RGB channel of an image with the same position and intensity variation of each pixel as the watermark image will produce dark and light variations in the pixels of the image that will be watermarked with the same positions as the positions on the watermark image. In the stegowater process, the Grayscale method is only involved in the watermarking process (Tirkel et al., 1994).

2.4 Steganography Data Collection and Analysis Techniques

A collection of resources, such as text, images, animations, and audio files, that have been gathered from a variety of sources. Coding/embedding is the process of adding a watermark on an image. Key entry may be required in conjunction with encoding, or it

may not. Only data (host data) must be in the form of keys. Watermarked data is digital information that has had a watermark added to it. Watermarking is the appropriate way to stop copyright violations (Kumar, 2019).

2.5 Inserting Watermarks

Files The process of inserting a watermark into an image is called coding/embedding. Encoding can be accompanied by key entry or not require a key. Keys are required to only be extracted by authorized parties. The lock is also useful for prevention The process of inserting a watermark into an image is called coding/embedding. Encoding can be accompanied by key entry or not require a key. Keys are required to only be extracted by authorized parties. The lock is also useful for preventing watermarks from being removed by unauthorized or responsible parties. Meanwhile, resistance to other processing processes depends on the watermarking method used watermarks from being removed by unauthorized or responsible parties. Meanwhile, resistance to other processing processes depends on the watermarking method used (Nida et al., 2021).

The steps for inserting a watermark in a digital file are as follows: 1. Carry out the process of inputting digital images, text orwatermark images. 2. Carry out the process of inserting the watermark. 3. Carry out the output process in the form of a watermarked image. 4. Carry out the extraction process from the watermark. When designing a watermarking application using the LSB method,a navigation structure is also used to display the pages in the application as in Figure 2 below.

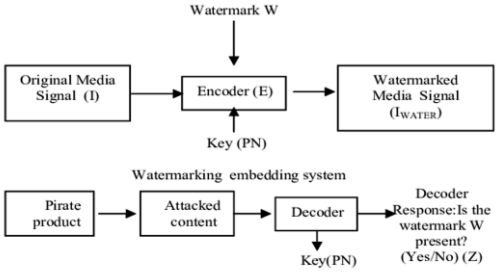

Figure 2. Watermarking decoding system

3 Result and Discussion

3.1 System Architechture

At this stage, the implementation of the watermarking application design using the PHP programming language, MySQL relational database, PHP8.3 JS software for DOM, Boostrap V5.0, and the Laravel Framework provides a GUI (Graphical User Interface) feature to make it easier to create the application display. Create a GUI in PHP using the GUIDE (Graphical User Interface Development Environment) facility. The resulting files have the extension .fig and .m. To start creating the application, type

guide in the command window, then select Blank GUI. Display the Command Window in PHP after that select Blank GUI in Create New GUI. The main display of the application can be seen in Figure 3 below.

Figure 3. System main page (in Indonesia language)

Figure 4. Manage material page (in Indonesia language)

Figure 5. Evaluation page (in Indonesia language)

In Figures 2 and 3 are the system dashboard displays for the teacher user interface. Teachers can add materials to the system, as well as carry out learning and evaluation processes through the available menu features. On the main dashboard, teachers can categorize materials based on class, material and lesson schedule.

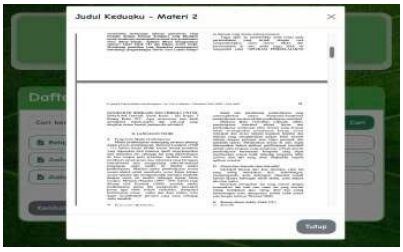

Figure 6. Material page and watermark process

Figure 7. Watermark file results on student material and evaluation feature

If the source document is a hard copy, there is a menu option in Figure 6 to digitize material document files. The content can be directly submitted to the upload material function if it is a softcopy document. Next, the digital file—especially the exam question file that will be sent to students—will have a watermark added by the system.

The file is available for students to work on both independently and in groups. Because it already has a watermark, the response file that will be given to the teacher cannot be shared with another file. It can be tested based on the conversation covered in the previous chapter. Using the outcomes of the watermarking application design, this application system was effectively transformed into an interactive multimedia application. This technique conceals messages or information by using the bits in the image file. The final bit of each color will be randomly chosen to conceal messages or information. These bit changes are difficult to see because they are intended to fool the human eye (Anisah et al., 2015).

3.2 Discussion

Testing the steganography application for inserting files into an image by collecting school exam document files that can be used as objects in inserting files into an image with LSB steganography (Nida et al., 2021).

Table 1. Table of exam/material document file

No	Exam/material document file	
	Document name	File size
1	Exam Test.1.pdf	156,478 bytes
2	Exam Test.2.pdf	167,745 bytes

The next testing step is the implementation of the school exam document file security scenario. First, select the school exam document file and an image as the media to be encrypted. The encryption process produces a stego image which will later be used as an object to implement the detection. The following are the results of the encryption process of an original image with the school exam document file contained in Table 2 (Guo et al., n.d.).

Table 2. Table of results encryption process

No	Real document	File size	Stego document size
1	28,564,010 bytes	33,932 bytes	27,678,689 bytes
2	28, 564,010 bytes	158,155 bytes	27,678,689 bytes
3	28, 564,010 bytes	63, 254 bytes	27,678,689 bytes

Transferring the exam document files and stego pictures produced by the first stage's three encryption processes is the next step. Using Oracle VM VirtualBox software, a virtual machine is used to carry out this file transfer procedure. Identifying the school test document files and stego images that are being transferred is the final stage. It can be tested based on the conversation covered in the previous chapter. The outcomes of the watermarking application design were implemented to successfully transform this application system into an interactive multimedia application. This technique conceals messages or information by using bits in the image file. The final bit of each color will

be randomly chosen in order to conceal messages or information. These bit changes are intended to fool the human eye, making it difficult to see them (Anisah et al., 2015).

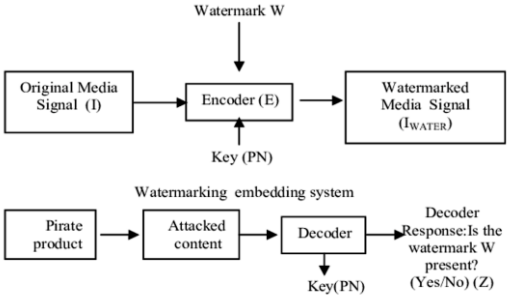

Figure 8. Watermark in data processing

The process of hiding digital data in a carrier signal is known as digital watermarking; the hidden data may or may not be related to the carrier signal. Digital watermarks can be used to identify the owners of the carrier signal or to confirm its integrity or validity. The digital watermarking technique consists of three primary components. putting a watermark inside. Using digital watermarking software, the first step is to add a watermark (text-based, image-based, or a combination of the two) to a document or file (Maity, 2009). Scanning media for watermarks. Extracting and decoding the data. In this case, secret or public keys and other parameters can be used to extend the watermarking encoder. The watermark is considered to be robust if it is embedded in such a way that the watermark can survive even if the watermarked CW data goes through severe distortions. A watermark extractor or detector involves a two-step process. Watermark retrieval is the first step that applies some scrambling algorithms to extract a sequence referred to as retrieved watermarks. Then, in the second step, the embedded watermarks are detected and extracted from a suspected signal of containing watermarks (Tirkel et al., 1994). The second step normally requires the analysis and comparison of the unreliable watermark with the original one, and the consequences could be several kinds of confidence assessments displaying the similarity between the extracted watermark and the original one. Watermark verification is done to prove the ownership status of a digital image. The extraction sub-process is also called decoding/extraction, which aims to reveal the watermark data inserted in the digital image. The decoding process can include the original image (non-blind watermarking) or not at all (blind watermarking), because some watermarking schemes do use the original image in the decoding process.

This application can be used to secure digital images. Inserting watermarks in the form of text or images into digital image files using the Least Significant Bit (LSB) method has been successfully carried out. For image files. The results of the watermarking process do not change the size of the original file significantly, whereas for the original file with the extension .jpg after the watermarking process, the file size is different from the original. This is due to the change from the .jpg extension to the .png or .bmp extension. To develop this application, the digital image file format produced after the watermarking process can be in the form of .jpg. Testing for the

watermark process with LSB is carried out in 2 stages. Namely, the encode stage testing and the decode stage testing. The stages in encoding testing are as follows: Original image capture, Select watermarking text, and Choose a watermark (Gani, 2018). This application is in the form of interactive audio-video compared to conventional learning (books). Digital image file format produced after the watermarking process can be in the form of .jpg. Apart from that, you can also add types of digital watermarks such as audio or video. Visibility of the watermark on the picture can be reduced by using no. of techniques. The simplest technique used for hidden watermarking is to hide the message bits in the Least Significant Bits (LSB) of the cover object. The advantage of this method is that even if a part of the stego image is cropped the receiver can still get the required message, as the message is embedded several times. The message for this case is considered to be very small as compared to the cover object. For example, for an 8-bit file, each pixel is represented by 8 bits: 10001100. The most significant bits (MSB) are to the left and the least significant bits (LSB) are to the right. If you change the MSB it will have a big impact on the color, however, if you change the LSB, it will have minimal effect. Now to take this method a step further, if we change only 1 or 2 least significant bits in the image, it will have a minimal effect because the human eye can only detect around 6 it's of color. In other words, the human eye cannot tell the difference of the last 2 bits being changed. For example, if we take 10001100 and change it to 10001111 for 10001110, it will all seem like the same color to the human eye. So we would only embed data in those bits. An example of this is: If the message converted to binary is 1101 0010, the first 8 pixels will be modified as follows: a) 1100 0101 becomes 1100 0111; b) 1111 0010 becomes 1111 0001; c) 1010 1111 becomes 1010 1100; d) 0010 0010 becomes 0010 0010

Figure 9. Document without watermarking

Figure 10. Document with watermarking

Figures 9 and 10 show the outcomes of watermarking learning evaluation materials and question documents using steganography techniques. Examines cannot transfer document files into other formats than those that have already been encrypted, therefore these two strategies can result in digital media—such as exam questions and materials—being more secure during the review process (Rasak & Zubair, 2018).

4 Conclusion

Digital photos can be secured with the help of this program. It has been accomplished to insert watermarks in the form of text or images into digital image files by employing

the Least Significant Bit (LSB) approach. Watermarked the original digital images with the extensions.png and.bmp remain largely unchanged following the watermarking process, however, the original file with the extension .jpg has undergone a major size alteration. The switch from the.jpg to the.jpg extension is to blame for this. Drawing from the research conducted, the investigator has developed a steganography tool and successfully implemented it to encrypt exam document files into stego document medium. The size of the original document and the generated stego document are almost identical. The transferred file displays the file name and file format, as observed in the detection test. This demonstrates that we can identify the encrypted file if we transfer the school exam document file directly without encrypting it with an image. The school test document files are packed into image media using image steganography before being delivered in an encrypted format. This ensures that only images are transferred in traffic and are verified to be safe.

References

Akter, A., Nur-E-Tajnina, & Ullah, M. A. (2014). Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. *2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014*.

Anisah, N., Harjito, B., & Suryani, E. (2015). Digital Watermarking image dengan menggunakan Discrete Wavelet Transform dan Singular Value Decomposition (DWT-SVD) untuk copyright labeling. *ITSMART: Jurnal Teknologi dan Informasi,4*(1).

Gani, S. (2018). Teknik invisible watermarking digital menggunakan Metode DWT (Discrete Wavelet Transform). *Jurnal Sains dan Seni ITS. 7*(2).

Guo, J., Qiu, W., Du, C., & Chen, K. (n.d.). A scalable video encryption algorithm for H.264/SVC. *Proceedings of The 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE2013)* 1165–1168.

Kumar, S. K. M. and S. (2009). Secure image steganography based on Slantlet transform. *Proceeding of International Conference on Methods and Models in Computer Science (ICM2CS)*, 1–7. https://doi.org/10.1109/ICM2CS.2009.5397983.

Maity, A. P. and S. P. (2009). Quality access control of image by encryption and data hiding. *2009 Proceeding of International Conference on Methods and Models in Computer Science (ICM2CS*, 1–7. https://doi.org/https://doi.org/10.1109/ICM2CS.2009.5397991

Nida, S. N., Purnamasari, D., Sasmita, W. A., & Ningsih, W. (2021). Penerapan Metode Least Significant Bit dan Discrete Cosine Tranform dalam Implementasi Steganografi Pada Citra Warna 24 Bit.

Venugopala, P. S., & Sarojadevi, H. N. N. C. (2014). Video watermarking by adjusting the pixel values and using scene change detection. *Fifth International Conference on Signal and Image Processing*, 259–264. https://doi.org/10.1109/ICSIP.2014.47.

Rasak, A., & Zubair, A. (2018). *Digital Watermarking Algorithms for Visible Watermarks*. June.

Rosmiyati, J., & Mulyana, T. M. S. (2018). Watermark using steganography and visible watermarking. *Jurnal Algoritma, Logika dan Komputasi, 1*(1).

Tirkel, A., Rankin, G. A., & Schyndel, R. G. V. (1994). *Electronic Watermark*.