Evolution in Electrical and Electronic Engineering Vol. 3 No. 3 (2022) 808-816
© Universiti Tun Hussein Onn Malaysia Publisher's Office

EEEE

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/eeee
e-ISSN :

FKEE Form Validity Verifications using Steganography Technique; Comparison Between Least Significant Bit (LSB) and Single Value Decomposition (SVD)

Nur Syafiqah Ali Sabri[1], **Siti Hajar Aminah Ali**[1]*

[1]Department of Electronic Engineering, Faculty of Electrical and Electronic Engineering,
Universiti Tun Hussein Onn Malaysia, Batu Pahat, 86400, MALAYSIA

*Corresponding Author Designation

DOI: https://doi.org/10.30880/eeee.2022.03.02.095
Received 28 June 2022; Accepted 2 October 2022; Available online 30 April 2022

Abstract: Faculty of Electrical and Electronic Engineering (FKEE) UTHM has used the new way of processing crucial forms with student and instructor signatures to validate such document. To validate FKEE forms and safeguard academician signatures, a system is presented. This system has two primary menus: (1) the generation of signature images with embedded matric numbers and excel files, and (2) the administration staff's form validity verification. Academicians must log in and select "Embedding" This menu requires the academician's signature and student's matric number. The technology generates an Excel file with steganography data. The academician staff will then share the signed form and excel file with the student. To validate the form, administration staff must select "Extraction" to decode the Excel file and extract the student's matric number. This project concludes that Least Significant Bit (LSB) can validate documents by extracting matric numbers. Next, it has 100% accuracy by testing the system with 3 different signature images. Single Value Decomposition (SVD) fails because it can only embed the hidden watermark but not extract the matric number-based watermark to its original image. This project's goals are finally met.

Keywords: Steganography, Embedding, Extraction, LSB, SVD

1. Introduction

In response to the pandemic Covid-19, the Malaysian government issued the Movement Control Order (MCO) under the Prevention and Control of Infectious Diseases Act 1988 and the Police Act 1967. One Standard Operating Procedure (SOP) is to limit the number of employees in the office to reduce the likelihood of infection between employees. Only 30% of office staff are allowed to remain in the office, while the rest must work remotely (WFH). Since most workers are at home and meetings are banned, most work is done online. Administrative staff manage documents regularly, with some requiring signatures. Virtual signatures are challenging to handle since they can be hacked and misused. Digital signatures should be kept protecting the signer.

Corresponding author: aminahh@uthm.edu.my

This project aims to create a way for Academicians Staff to safeguard their signature by generating an Excel file as proof of authorization, and for Admin to decode the Excel file and produce the hidden message. This is the ideal way as a digital signature system cannot be established without Certify Authority (CA) approval. Adding a covert watermark to a Word document and converting it to a Portable Document Format (PDF) for copyright is easy. Hidden watermark extraction is tricky and still being studied. Adobe Photoshop may be used to add a watermark to a document or photo by creating a translucent layer [1].

This project compares Text Steganography of LSB and Image Steganography of SVD. LSB protects the virtual signature by establishing a hidden message behind it that can only be deciphered by a program utilizing an Excel file containing a steganography picture [2]. This system must be easy to understand for the user to complete the design. SVD uses both picture input as signature and embedded watermark image, resulting in watermarked image extraction. If concealed watermarking is utilized, it can only embed with the signature, and how to extract the watermark image back to the original image using a different code is under investigation [3].

2.0 Methodology

This section focuses on how the project is progressing and how the project's goals are being reached, as well as how the project's data will be analyzed. The LSB and SVD techniques for project workflow were also discussed in this chapter.

2.1 Flowchart of the SVD Technique

Figure 1 shows the technique of the SVD to produce the watermarked image as an output. It is started by applying the SVD technique to the input image of the signature. The basic idea behind the SVD technique of watermarking is to find the SVD of the image and the altering singular value to embed the watermark [4]. To start the process, the image of the watermark as an input of the program and the value of alpha will be asked by the program. The value of alpha is required to produce of new SVD to calculate the Wimg and produce the watermarked image. Next, the value of alpha will determine the final outcome of the resulting image whether it will be a blurry or clear result image as the alpha value indicates the compression value of the watermark image. However, the SVD technique can only be used for embedding systems as the extraction system is still being studied. Therefore, another technique has been used to determine the objective of this project.

2.2 Block Diagram of the Overall System using LSB Technique

The Least Significant Bit (LSB) method is the easiest way to embed secret information. By replacing the minimum weighting value of a sampled speech signal with binary bits of secret information data, the secret information can be hidden in the speech [5]. Figure 2 depicts the system block diagram for the LSB method. Form validity is the primary motivation for recommending this system to academics and administrators. In the embedding tab, the academic staff begins by adding an image of the signer's signature before hiding the matriculation number. Afterward, the system can generate an Excel file as an output, which is required by the student as proof to the administration for verification purposes. Next, the administrator begins to be entering the system by inserting an excel file into the extraction tab in order to extract the matric number's concealed message.

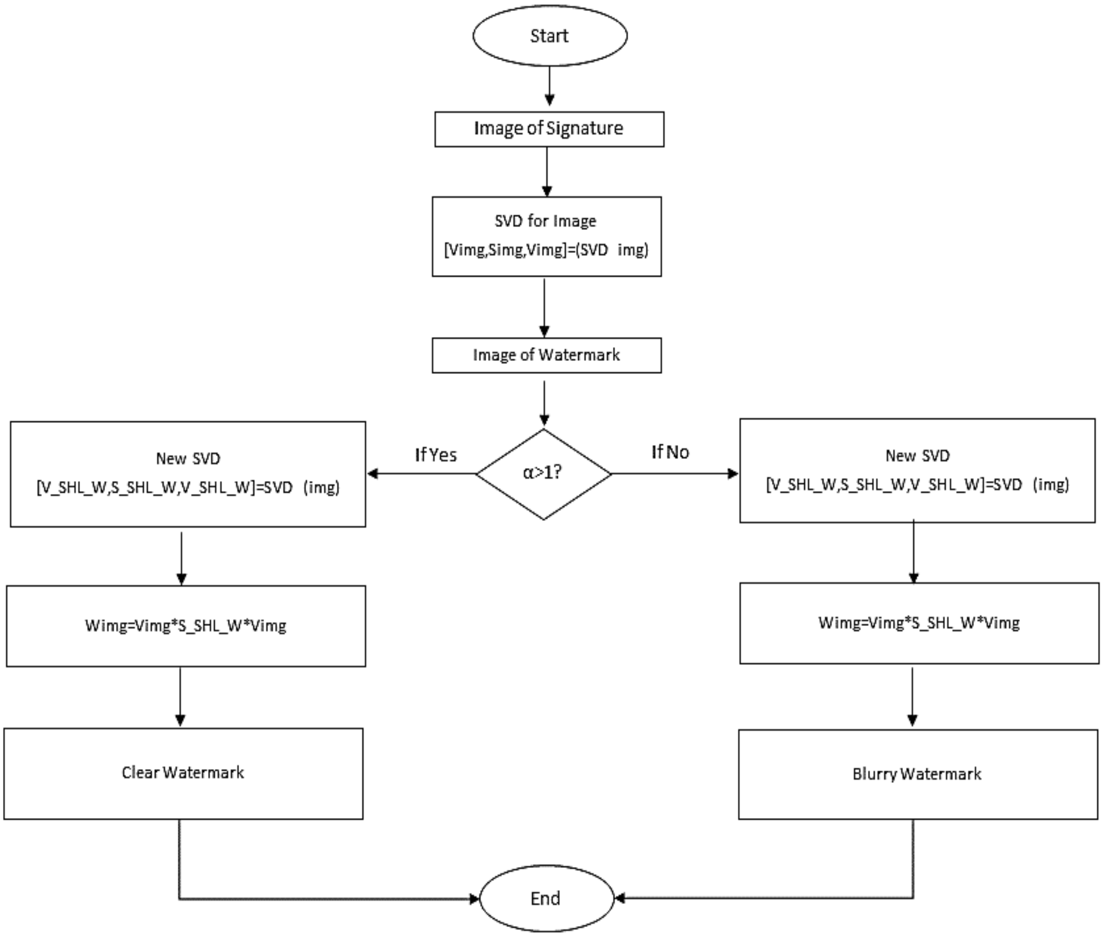


Figure 1: Flowchart of Embedding system using SVD technique.

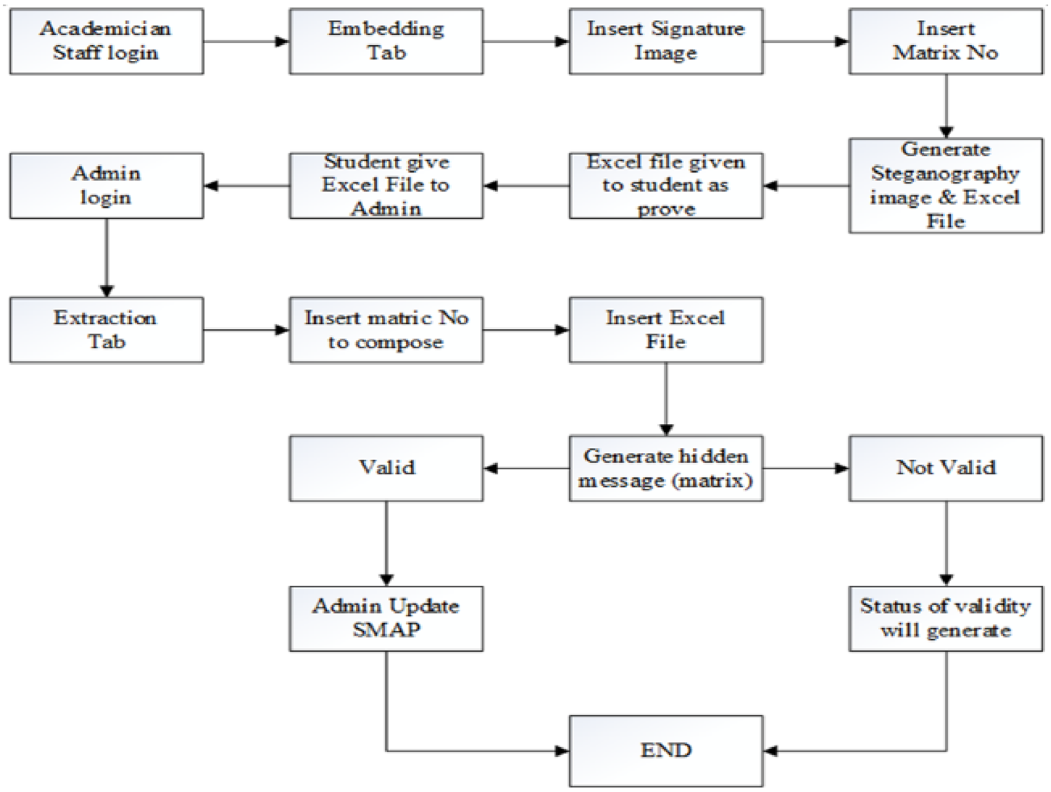

Academician Staff login
Embedding Tab
Insert Signature Image
Insert Matrix No
Generate Steganography image & Excel File
Excel file given to student as prove
Student give Excel File to Admin
Admin login
Extraction Tab
Insert matric No to compose
Insert Excel File
Generate hidden message (matrix)
Valid
Not Valid
Admin Update SMAP
Status of validity will generate
END

Figure 2: Block diagram of Overall System

2.3 Flowchart of Embedding System

Based on Figure 3, firstly, the user needs to insert the signature image as an input to start the embedding process. Secondly, the coding read the image in grayscale because less information needs to be provided for each pixel and resizing the image to 256x256 pixel allows to make the image smaller or larger without cutting anything out. Thirdly, the user needs to insert the input of the student's matric number as approval of signature to be used only by the mentioned student. Fourthly, the length of the message is set to 8 bits as it is the smallest number of bits that could hold a single character by assuming using the American Standard Code for Information Interchange (ASCII) standard. Fifthly, the coding need to convert the decimal to binary value to convert the character array to a numeric array. Sixthly, traversing means going from one block to another until all blocks are reached. Seventhly is to check If more bits are remaining to embed, it can find the Least Significant Bit (LSB) of the current pixel, find whether the bit is the same or need to change, update the output to input and increment the embed counter. Finally, producing the output the form of a Portable Network Graphic (PNG) image and an excel file of the steganography image.

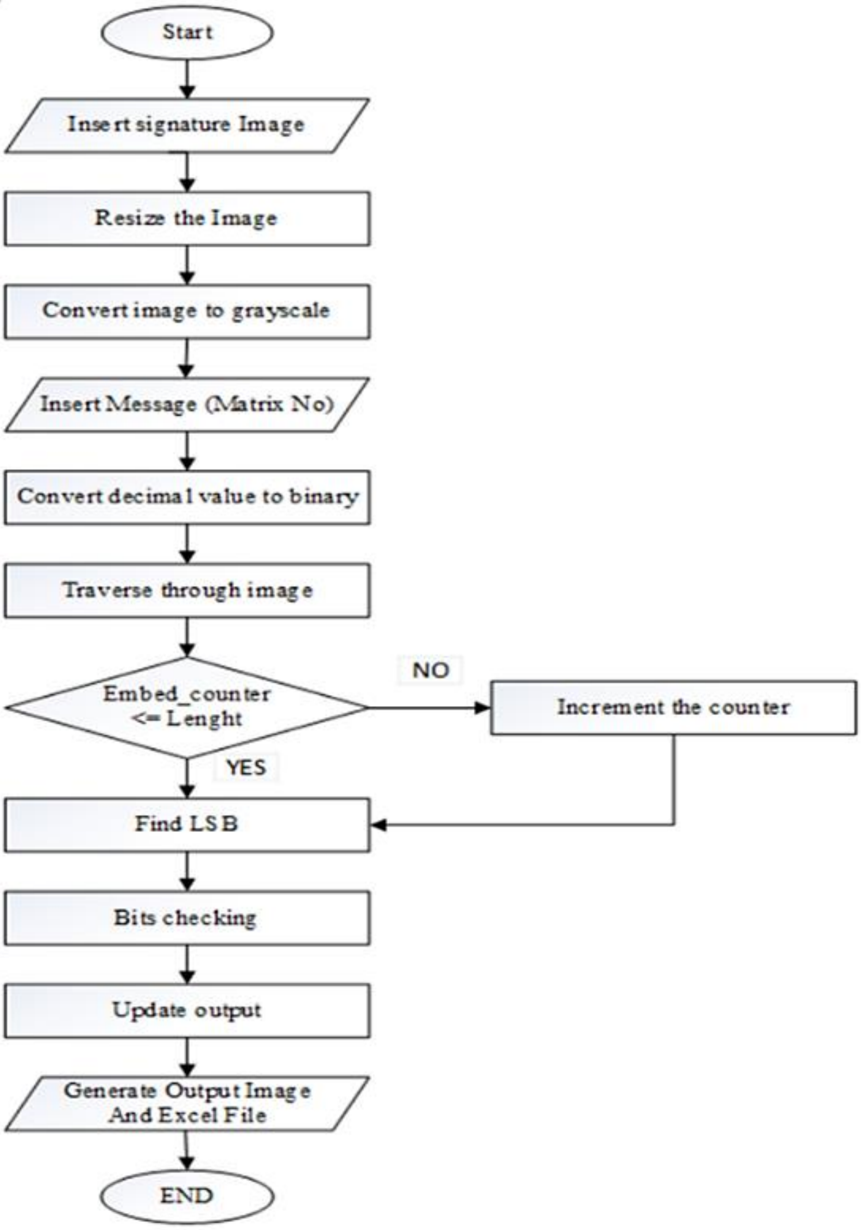


Figure 3: Flowchart of Embedding System

2.4 Flowchart of the Extraction system

Based on Figure 4, the extraction part of the steganography image is a lot simpler than the embedding process, firstly it needs the user to provide the excel file of the steganography image to extract the hidden message embedded. Secondly, the coding is set the height and the width for traversing the image data contained in the excel file. Thirdly, set the number of characters, its length and the value of the counter to ensure all the message extracted is the same as the original input message. Fourthly, check if more bits remain to be extracted, it can store the LSB of the pixel in extracted bits or change the increment of the counter first if the message length is different from the setting. Sixthly, the ASCII value from binary all bits in the columned table gets. Seventhly, after all the binary and bits are extracted from the image, it converts the extracted bit to characters and finally displays the output of the hidden message.

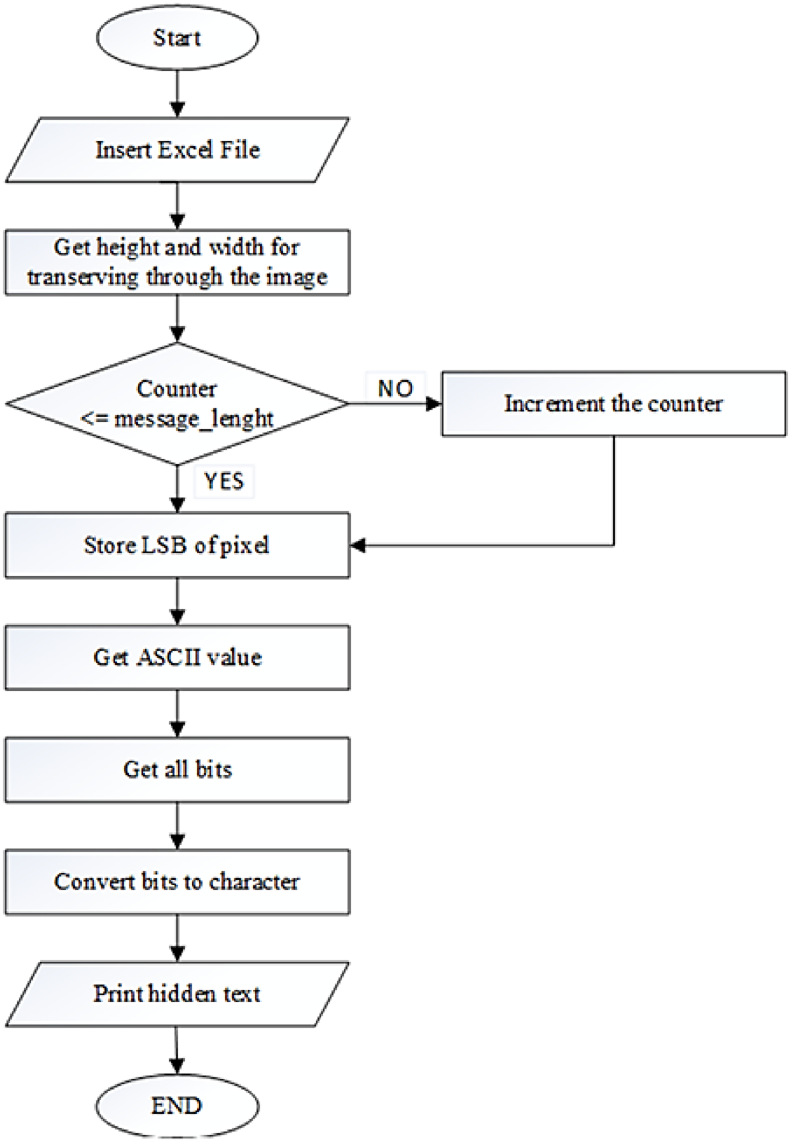


Figure 4: The flowchart of the Extraction System

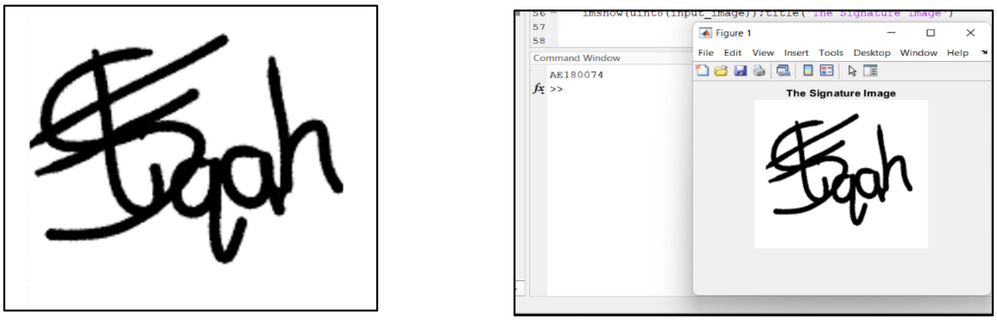
3.0 Results and Analysis

For each stage of implementation, this section examines the experimental results and project development validity from verification progress made utilizing the LSB technique. This section presents raw data in the shape of the image. The information is acquired because of the various testing.

3.1 Effectiveness of Image Extraction using different methods.

Based on Figure 9, Figure 10, Figure 11, and Figure 12 can be observed that all the cropping methods can be used as they will not affect the quality and data stored in the image. All the images are still can extract the hidden data of matric numbers without fail. By performing this test, it is proven that the system is valid to use and has good security over the embedded image.

i. Crop the image using Snipping Tools



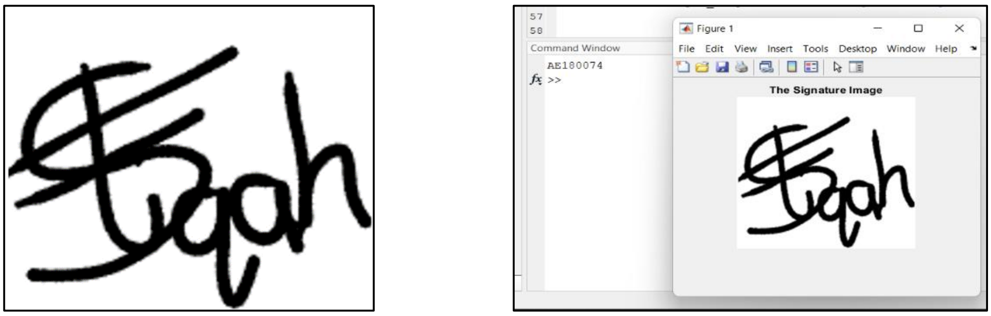
```
imshow(uint8(input_image));title('The Signature Image')
```

```
Command Window
  AE180074
fx >>
```

(a) (b)

Figure 9: (a) The image cropped using snipping tools and (b) the result of extracted matric number using the cropped image by snipping tools

ii. Crop the image using Photoshop

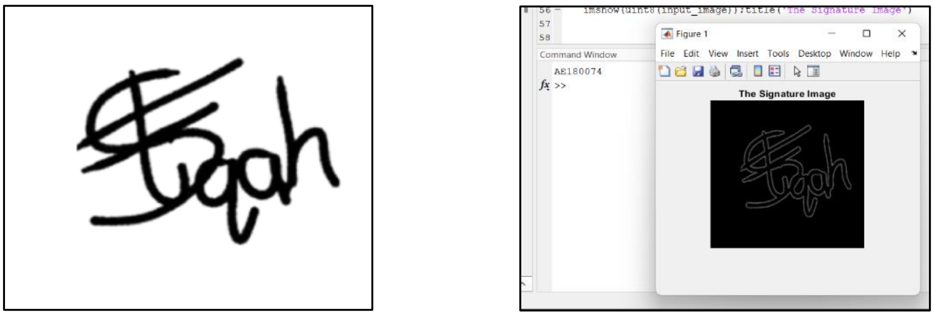


```
Command Window
  AE180074
fx >>
```

(a) (b)

Figure 10: (a) image cropped and (b) extracted matric number using the cropped image by photoshop.

iii. Crop the image from PDF using Photoshop



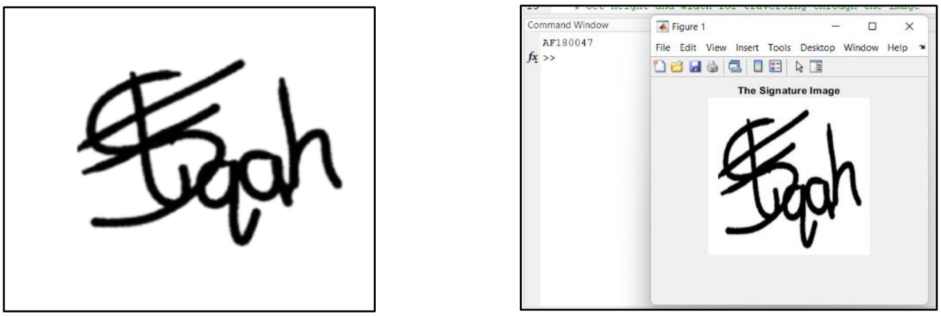
```
imshow(uint8(input_image));title('The Signature Image')
```

```
Command Window
  AE180074
fx >>
```

(a) (b)

Figure 11: (a) image cropped and (b) extracted matric number using the cropped image from PDF using photoshop.

iv. Crop the image from PDF using Snipping Tools



```
AF180047
>>
```

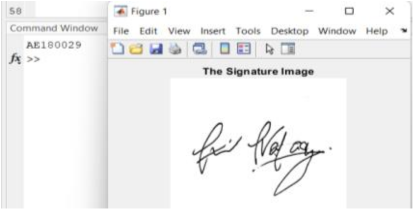
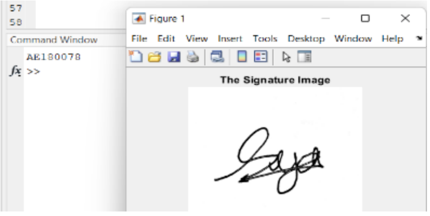
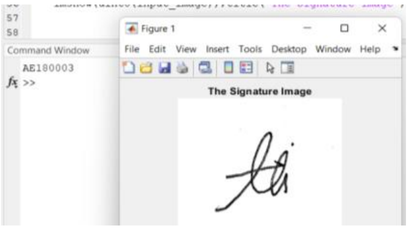
(a) (b)

Figure 12: (a) image cropped and (b) extracted matric number using the cropped image from PDF using Snipping Tools

3.2 Accuracy of the system

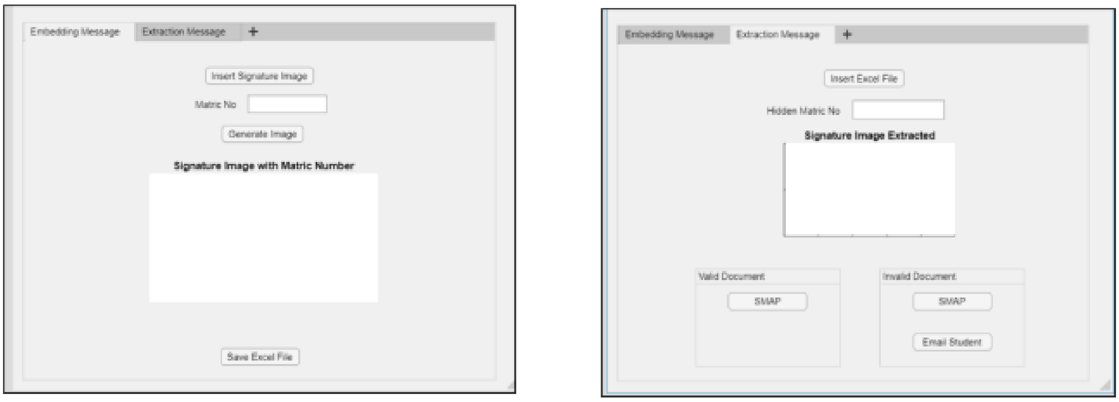
Based on Table 1, three different styles of signature are used to test the accuracy of the system. It is shown the accuracy of this system of different types of signature images is 100% accurate based on visual observation. This technique is able to be performing its task to hide a matric number in the signature image and extract it back without any fault data extraction.

Table 1: The Accuracy of The System

Matric Number	**Image of Signature**	**Accuracy of Result**
AE 180029		 AE180029 >>
AE 180078		 AE180078 >>
AE 180003		 AE180003 >>

3.4 Overall GUI System

Figure 13 (a) consists of three buttons which is the first button will ask for the user to insert the image of their signature as input. Next, the second field will be a blank space for a user to insert a student's matric number. Moreover, Generate Image button will execute coding to embed the matric number with the signature image and display the steganography image as an output. Finally, the Save Excel File button will save the output in the form of an excel file to be used as proof of permission. The student will be required to send this excel file along with the related document to the admin for the next process to confirm the validity of the document. Based on Figure 13 (b), the system used for extraction purposes will start with inserting insert the excel file given by the student. Hidden Matric Number and Signature Image Extracted will be automatically appeared to tell whether the document is valid or not. After the status is known by the admin, they can have an option to update the system in the *Sistem Maklumat Akademik Pelajar* (SMAP). However, if the document is invalid because the matric number does not match or the excel file is not in the right format, the admin will have a choice to email the student as the rejection notice or straight away update the system in the SMAP.



(a) (b)

Figure 13: (a) GUI of Embedding Message tab and (b) GUI of Extraction Message tab

4.0 Conclusion

To summarize, this project is specially designed for additional security of virtual electronic signature by embedding the hidden message of Matric number behind the image of the signature. The matric number should not have appeared when it was used either in a confidential document or shared with the public. As explained in section 3, it is shown that the system of steganography by using the LSB technique is considered to be a success as it was able to perform its task of embedding and extracting the secret message. However, it is that believe there will still be a few things that can be considered for future work to ensure this system can be more effective and secure. Finally, it is demonstrated that the LSB technique is easier to do than the SVD technique, as it still does not identify the solution of the extraction part when used separately with embedding coding. Therefore, the SVD technique is not suitable to solve this project as this project is intended to check the validity of the document and it should perform the extraction part by itself.

Acknowledgement

The authors would like to express their gratitude to the Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia for its support.

References

[1] Photography Mad (2019). “How to Add a Watermark to an Image in Photoshop”. [Online]. Available: https://www.photographymad.com/pages/view/how-to-add-a-watermark-toan-image-in-photoshop. [Accessed November 21, 2021]

[2] M.S.A. Rahim, N.H. Shaari., N.H. Ghazali, “Invisible Watermarking on Grayscale Image” International Journal of Applied and Physical Sciences vol. 4 no. 3 pp. 103-109, 2018

[3] R. Bagheri, (2021). “Understanding Singular Value Decomposition and its Application in Data Science”. [Online]. Available: https://towardsdatascience.com/understanding-singular-value-decomposition-and-its-application-in-data-science-388a54be95d. [Accessed May 03, 2022]

[4] D. Pradha, “Implementation of Invisible Digital Watermarking Technique for Copyright Protection using DWT-SVD and DCT” IJAERS Research Journal vol. 4 no. 7 pp. 63-69, 2017

[5] Z. Wu, “Least Significant Bit. In Information hiding in speech signals for secure communication”. essay, Syngress. 2015