Hiding Secret Text inside a Dynamic Handwritten Signature as Steganography Application

Fahad Layth Malallah[1], Ayad Hussain Abdalqadir[2], Mohammad Aldabbagh[3], Ammar Waisy[4]

[1&4]Cihan University, Sulaimaniya Iraq. [2&3]Mosul University, Mosul/ Iraq.

[1]Fahad.laydh.86@gmail.com

Abstract

One of the defects with Cryptography is that, when an opponent sees the message in the encrypted form, they might suspect that the message might carry something important, therefore, they will try to roll back the encrypted form to its original one by using all possible methods. The target of this paper is securing text inside an online handwritten signature in order not to raise any suspicion coming from the attacker. This type of protection named *Steganography*, which is hiding media inside another media. Here, Least Significant Bit (LSB) method is used. The hosted media is online signature that is consisting of three time series trajectories as: *x[t]*, *y[t]* and the pen pressure *p[t]*. The result has shown that the hidden secret message in the source party has been reconstructed successfully with the same secret message in the destination party with a recognition rate is 100%. However, the drawback of this method is a slight distortion to the stego-signature, and hides fewer texts than other media.

Keyword: Information security, Steganography, Handwritten signature, Hiding, De-hiding.

پوختە

یەکێک لە کەموکوڕیەکانی شفرەکردن ئەوەیە کە کەسی نەزان کاتێک دەبینێت پەیامێک شفرەکراوە، یەکسەر وادەزانێت زانیاریی گرنگی تێدایە، لەبەرئەوە لەوانەیە هەموو هەوڵێک بدات کە پەیامەکە بگەڕێنێتەوە سەر باری سەرەتا و شفرەکە بشکێنێت. ئامانجی ئەم نووسینە ئەوەیە کە پەیامێک لەناو واژۆیەکی ئۆنلاینداا بشارێتەوە بە مەبەستی پاراستنی ئاسایشی پەیامەکە و بۆئەوەی هیچ گوومانێک بۆ کەس دروست نەکات و نەکەوێتە بەر هێرش. ئەو بیرۆکەیە پێیدەگوترێت ستیگنۆگرافی بە واتای شاردنەوەی میدیایەک لەنێو میدیایەکی تردا . لێرەدا بیرۆکەی ناگرنگترین بیت LSBبەکاردەهێندرێت. میدیای خانەخوێ دیرۆکێکی سێ هەنگاوییە وەک x(t), y(t), p(t). ئەنجامەکان ئەوە نیشاندەدەن کە پەیامە شاردراوەکە بە ڕێژەی سەرکەوتنی ١٠٠% دەناسرێتەوە و دەگەڕێتەوە. خاڵە لاوازەکانی ئەم بیرۆکەیە ئەوەن کە شێواندنێکی کەم لە واژۆکەدا ڕوودەدات و هەروەها پەیامی کەمتریش هەڵدەگرێت.

الملخص

احد عيوب علم التشفير هو ان المتطفل يرى الرسالة انها مشفرة مما يولد عنده شك بان الرسالة تحمل معلومات مهمة، لهذا سوف يحاول استرجاعها الى صيغتها الاصلية بكل الطرق الممكنة. الهدف من هذه الورقة العلمية هو حماية الرسائل داخل توقيع اليد لرفع مشكلة شك المتطفل. هذا النوع من الحماية يسمى علم الاخفاء الذي هو اخفاء بيانات داخل وسائط اخرة . هنا في هذ البحث طريقة البت الاخير تم استخدامها. نوع الوسائط المستخدمة هي توقيع الذي يتكون من ثلاث اشارات (x[t]، y[t]، p[t]) . نتيجة هذ البحث انه تم التحقق من ان الرسالة المسترجعة هي نفس الرسالة المخفية بالضبط اي ان نسبة النجاح في الاتسترجاع هي 100% ، على اية حال، ضعف هذه الطريقة هو قليل من التشويه للتوقيع عندما يحمل الرسالة وايضا عدد قليل من الحروف التي يمكن احفائها في التوقيع.

1.1 Introduction

Information security involves in many aspects, such as confidentiality, integrity, availability and authentication (Malallah, Syed, Rahman, Wan, & Yussof, 2014). There are many ways to achieve confidentiality, which is secrecy assurance of revealing something to public. One of which is Steganography, it is the science of hiding the information inside other information so that the hidden information appears to be nothing to the human eyes. The term Steganography is retrieved from the Greek words *stegos* meaning covert and *grafia* meaning writing defining it as *covert writing* (Poornima & Iswarya, 2013),(Coronado, 2013). The file that contains the embedded information inside of it, is called as *stego* file. Various types of file formats such as video, audio, image can be covered inside a covered media. In addition to Steganography, Cryptography can also fulfil the confidentiality security property but the difference between them is that, in Steganography, the attacker will not try to decrypt the message because she/he does not know that the secret information is inside the Stego file. There are various types of media for steganographic technique such as, Image, network, video, Audio and text.As shown in (Figure 1). First, the image steganography, this takes the cover object as image in steganography. Generally, in this technique pixel intensities are used to hide the information. Second, The Network Steganography, is taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc., where protocol is used as carrier by exploiting unused header bits of TCP/IP fields(Handel & Sandford II, 1996).

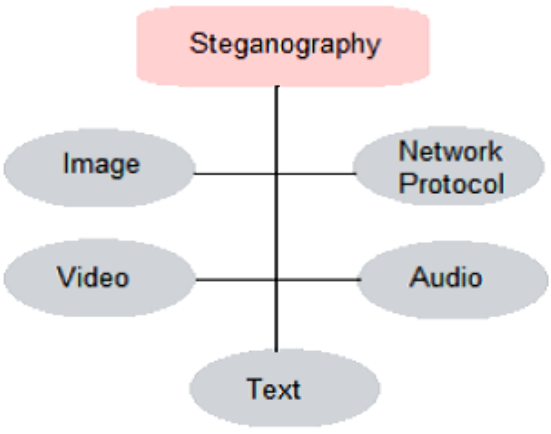

Figure 1: Represents various types of digital media for steganography.

Third, the video Steganography, this technique hides any type of files or information into digital video format. Audio steganography, audio is used as a carrier for hidden information; it is a very significant medium due to Voice Over IP (VOIP) popularity.

Fifth, the ext teganography, which is run by hiding information inside text files.

Dynamic handwritten signature is a human being signature that is taken by tablet or Personal Digital Assistance (PDA), its represented data are time series of both *x[t]* and *y[t]* trajectories as well as pen pressure *p[t]* for each dot. Handwritten signature biometric is deemed as a non-invasive and non-intrusive process by the majority of the users for this application. Furthermore, it has a high legal value for document authentication, as well as being dependent on by both commercial transactions and governmental institutions (Malallah et al., 2013).

The motivation of this paper is that, one of the defects with cryptography is that, when an opponent or an attacker sees the message in the encrypted (scrambled) form, they might suspect that the message might carry something important; therefore, they try to roll back the encrypted form to its original one using all possible attack methods. Our target of this paper is, securing text inside a handwritten dynamic signature without any suspicion coming out from the attacker. In this case, the attacker does not know there is a text inside the image. Therefore, the attacker will not try to get its original form. Figure 2 describes the advantage of Steganography over another type of security operation which is cryptography. It is obvious that, in cryptography the person has doubt about what he reads. On the other side, in the Steganography case the person is careless because he has seen a beautiful image. He doesn't know that the secret writing lies inside it.

Moreover, Steganography has many applications that draw a big motivation to navigate in this research. It varies among the user requirements such as copyright control by hiding a secret code inside a copyrighted document, covert communication for confidentiality manners, smart ID's for authentication. Motivation can be summed up by using dynamic handwritten signature as a carrier for the secret text but the problem here is, how does this signature features carry the secret information.

The Objective of this research is to hide or disguise a secret message or text inside a dynamic handwritten signature in order to achieve either covert communication or document copyright or secret authentication. Furthermore, the aim of this research is to overcome the Least Significant Bit (LSB) weakness, which is fragile, by using the online handwritten signature media, whereas even if the stego file format has been changed, the secret writing won't be destroyed.

This paper is organized as follows; Section 2, covers literature reviews about Steganography. Section 3, explains our proposed concept methodology of the text hiding inside dynamic handwritten signature. Section 4، depicts the Matlab Graphical User

Interface (GUI) as implementation in this research. Section 5, comprises results and discussions of this paper. The last section, concludes the paper and outlines the future work.

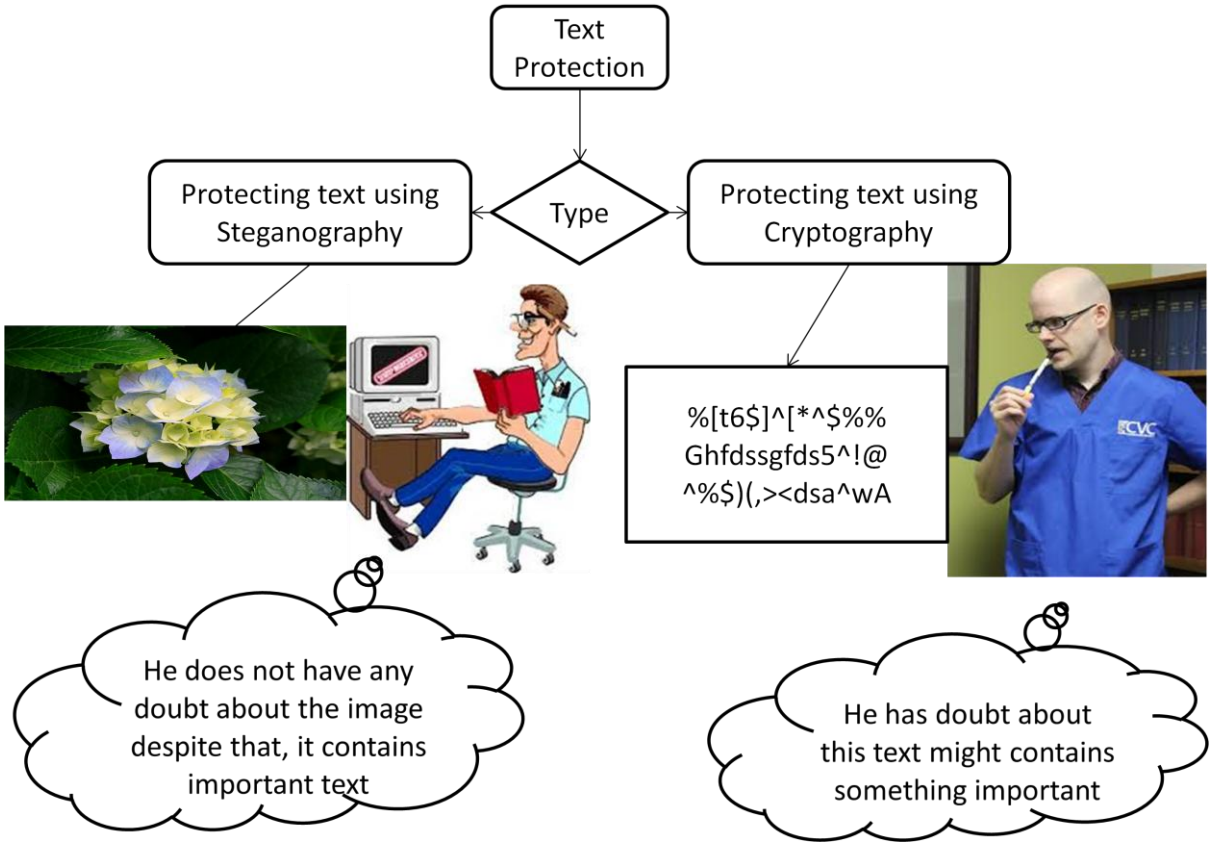

Figure 2: Describes the Difference between steganography and cryptography.

1.2 Literature Review

In the past, hiding was used by selecting a person to send message by shaving his head off, then, a secret message is written on his head and after that they let his hair grow again. Then, the intended receiver will again shave off the hair and see the secret message(Poornima & Iswarya, 2013). Also, during the Second World War the secret message was written in invisible ink so that the paper appears to be blank to the human eyes, then, the secret message is extracted back by heating the liquids such as milk, vinegar and fruit juices (Poornima & Iswarya, 2013). Computer system has been increasingly deployed in the past few decades. Generally the Steganography implementation is divided in into two types. First, the fragile Steganography, if the file is modified, then the secret information is destroyed. For instance, the information is hidden in the .bmp file format, if the file format is changed into .jpeg or some other format, the

hidden information will be destroyed. The advantage of fragile is that it is required to be proved when the file is modified.

Second type is a robust Steganography, in this case, the information is not easily destroyed as in fragile Steganography. Robust Steganography is more difficult to be implemented than fragile (Cummins, Diskin, Lau, & Parlett, 2004). In (Figure 3), Steganography operation is illustrated; cover image is used to hide the embedded message by using *stego* key to output a *stego* image or a *stego* file. After that, a *stego* file is sent to the destination party. Then an extraction operation is takes place by using the *stego* key in order to output the embedded message in the receiver party.

Figure 3: Basic steganography diagram depicts sender and receiver parties.

In terms of computer system, there are various ways to achieve Steganography, one of them is putting the intended text in the Least Significant Bit (LSB) for each gray scale or decimal number. In this case, altering LSB is not going to change much information of the image as the human being eyes cannot recognize this small difference of the image pixels. Therefore, the attacker will not observe that text.

Image Steganography is classified into two domains: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform domain applies image transformation and manipulation of algorithm, examples of this technique are Discrete Fourier transformation technique (DFT), Discrete cosine transformation technique (DCT), Discrete Wavelet transformation technique (DWT). In general, Spatial domain techniques are classified into: Least Significant Bit (LSB), Pixel Value Differencing (PVD), Edges Based data Embedding method (EBE), Random Pixel Embedding method (RPE), Mapping pixel to hidden data method, Labelling or

connectivity method, Pixel intensity based method, Texture based method, Histogram shifting methods. A number of researchers have proposed various techniques for these domains, intended readers may refer(Luo, Huang, & Huang, 2010) (Chhajed, Deshmukh, & Kulkarni, 2011; Muttoo & Kumar, 2008) (Shejul & Kulkarni, 2011).Other steganography techniques are based on distortion or masking and filtering operations, more details in(Bansal & Singh, 2012).

Neither Steganography nor Cryptography is deemed as "turnkey solutions" to open systems privacy, but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems(Malallah, et al., 2013).

Recently, different methods of hiding have been evolved regarding steganography application, one of them in (Szczypiorski & Mazurczyk, 2016) Steganography in IEEE 802.11 OFDM symbols, it is about insertion of hidden data into the padding of frames at the physical layers of wireless area network (WLAN), here performance analysis is based on a Markov model, and maximum steganographic bandwidth is as high as 1.1 Mbit/s. Another work which is steganographic schemes embed the secret payload inside image (Sedighi, Cogranne, & Fridrich, 2016). Also in (Khan, Ahmad, & Wahid, 2016) a proposed technique for data hiding in cover images by using Variable least significant bits (VLSB), this method uses a secret stego-key comprising a reference point, and variation of the number of bits to be hidden with varying indices of pixels in the cover image. The secret key adds an extra feature of security to steganography, making it much immune to steganalysis. However, hiding operation inside image is called fragile steganography and considered as a drawback of it, because any changing at image format, the message will be damaged and difficult to be got back the hidden message.

Steganography work with video media also has been presented in (Yadav, Mishra, & Sharma, 2013) by using LSB technique, this kind of media has a lot of space to be hide inside video as considered the advantage of this media (video) for the Steganography. However, it has a complex work and the reconstructed method must be accurate enough to get the hidden message back. This scheme of video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. Also another work which is hybrid method between cryptography and steganography has been presented in (Saraireh, 2013)

for gaining more secured method. The goal of this hybrid is to provides a robust and strong communication system that able to withstand against attackers, the idea is the filter bank cipher is used to encrypt the secret text message, it provide high level of security, scalability and speed. After that, a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients.

The new method of this paper is the cover media, which is used as online handwritten signature. It has never been used in the literature as media and also has advantages of being non-fragile stego-media in the contrary with an image and video media.

1.3 Methodology

The aim of this paper is to hide a secret code inside online handwritten signature. The Least Significant Bit (LSB) technique have been used due to its several advantages, which are less suspicious to human eyes, high perceptual transparency and simple to implement. Moreover, to eliminate the LSB technique defect as it is fragile steganography type as discusses in 1.2 literature review. As usual everything in this life has its disadvantages as a contrast, the disadvantages is extremely sensitive to any kind of filtering, scaling, rotation, cropping, adding extra noise that will lead to destroying the secret message.

Online signature consists of decimals numbers, which are features represented of the signature as x[t], y[t] time series trajectories and p[t] as the pressure of the pen. The process starts by converting both: the *stego* media and secret writing text to binary system numbers. The *stego* media in our case is online signature, which is the media that the text shall be hidden in. Then, put each bit of the binary number of the secret writing in the LSB of each binary feature either *x[t]* or *y[t]* or *p[t]* time series according to the secret text length requirement. In other word, the length of the secret writing specifies which *stego* media features will be exploited to fill in, whether exploiting only x[t] time series or with y[t] or with p[t]. Figure 4 shows a block diagram of the proposed method. This figure contains both processes of Hiding and De-hiding operations. With regard to the De-hiding process, it occurs after a transmission to the *stego* signature that carries the secret writing through Internet.

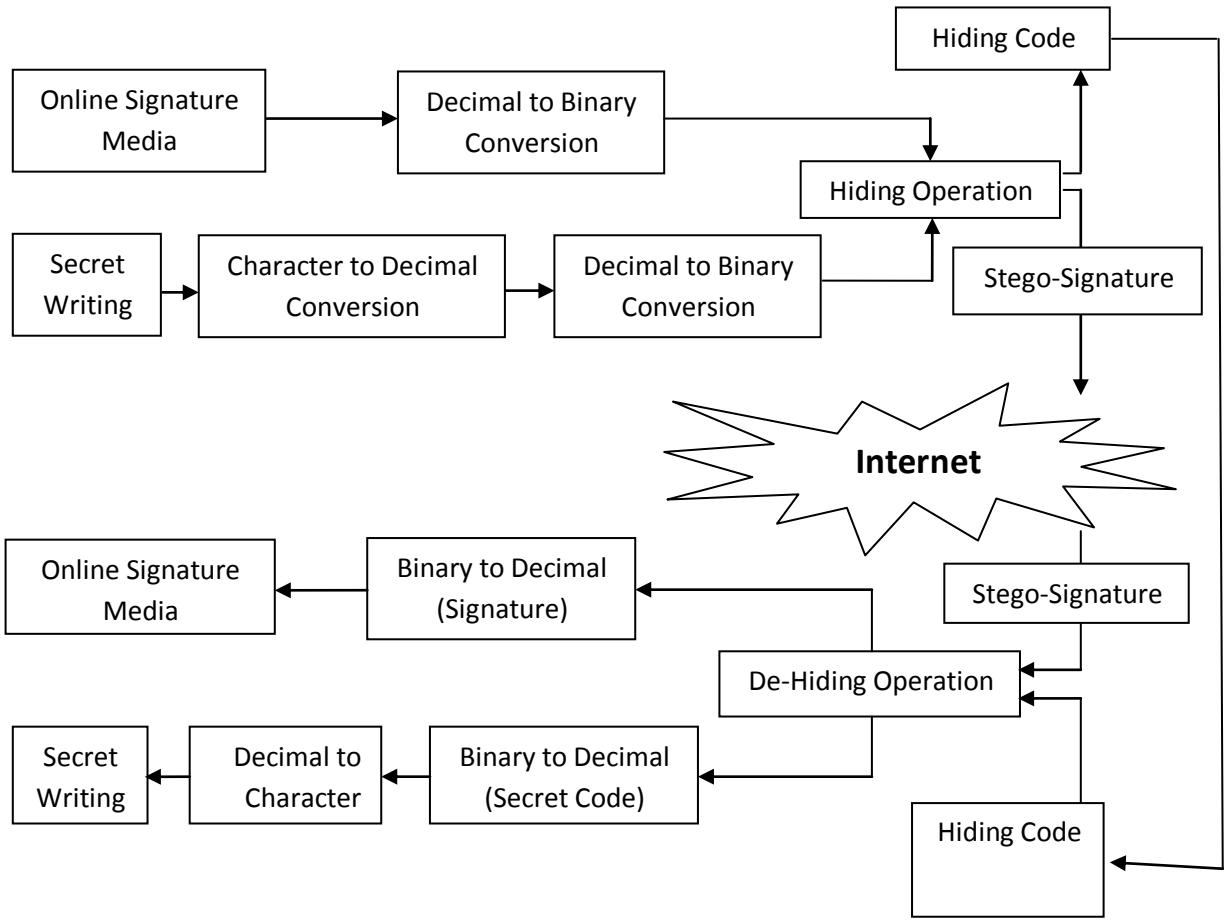

Figure 4: Block diagram of the major steps of the proposed method.

Matlab 2013 image processing software was used in this study. Whereas, a Graphical User Interface shall be used to design this proposed method. Following sections will explain both processes of Hiding and De-hiding with LSB in details:

A. LSB (Least Significant Bit)

The most frequently used steganography method is the technique of LSB substitution (Handel & Sandford II, 1996). In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 2^8=256 variations. A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique, where the least significant bits of the pixels is replaced by the message which bits are permuted before embedding.

This steganography technique exploits the faintness of the human visual system (HVS). HVS cannot notice the variation in luminance of color vectors at the higher frequency side of the visual band. An image can be represented by a collection of pixels as in shown in (Figure 5). The individual pixels can be represented by their optical characteristics like 'brightness' and 'contrast' .The characteristics image will have 24 bits, representing 8-bit for each of the three color values (Red, Green, and Blue) at each pixel. Consisting blue there will be 2^8 different values of blue. The change between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye.

(A) Cover image (B) Stego image

Figure 5: Shows the original cover-image and the steganography image.

Figure 5-(A) shows the original cover image, whereas (B) is the steganography image that secret text has been embedded into the cover image.

B. Hiding Operation

For hiding the text in the dynamic signature, LSB has been used in this paper**.** Hiding process is achieved by attaching the secret text within the dynamic signature (online signature), the signature is three dimensions which is *(X, Y, P)* and any one of them is between (1-256) numbers, any LSB of any number of text will be hiding in the LSB of any one of dimension *(X)* , if the text is greater than (256) will go to dimension *(Y)*, after that dimension *(P)* will be used, then the stego-signature is sent through internet. Accordingly, the hiding code will be constructed as a result of the hiding operation. This code is the number of bits of each character of the secured text. (Figure 6) explains the idea of attaching secret bits into the online handwritten signature features.

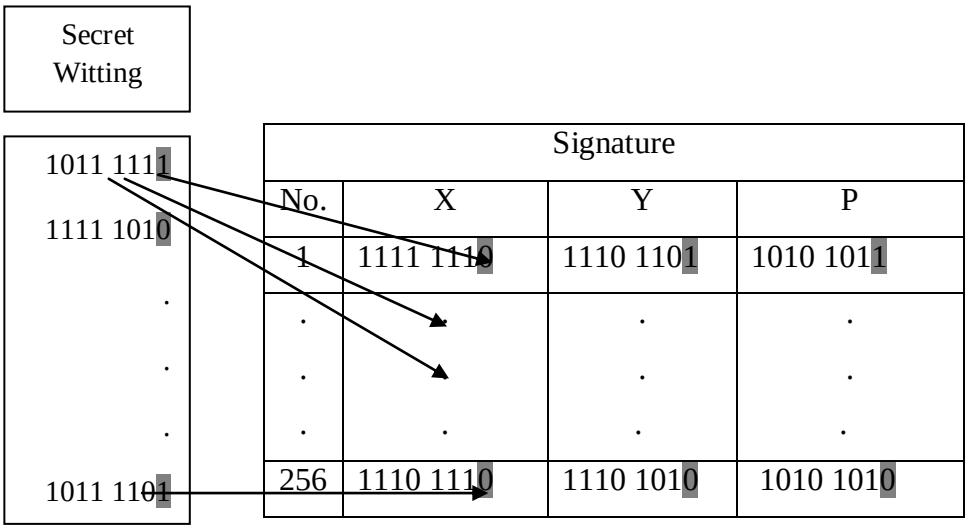

Figure 6: Hiding Process by using Least Significant Bit (LSB).

C. De-hiding Operation

In the De-hiding operation, the secret text is re-constructed through internet by using both the received stego-signature and the de-hiding code,. In the de-hiding code, the length of each character is known as a number of bits. Certainly, extraction starts with dimension *(x)* by returning any LSB bit of dimension *(x)*. Accordingly, all LSB bits in dimension *(y)* and *(p)* will be collected and formed as characters depending on the hiding code length. Figure 7 explains the procedures of the reconstructed bits of the secret writing.

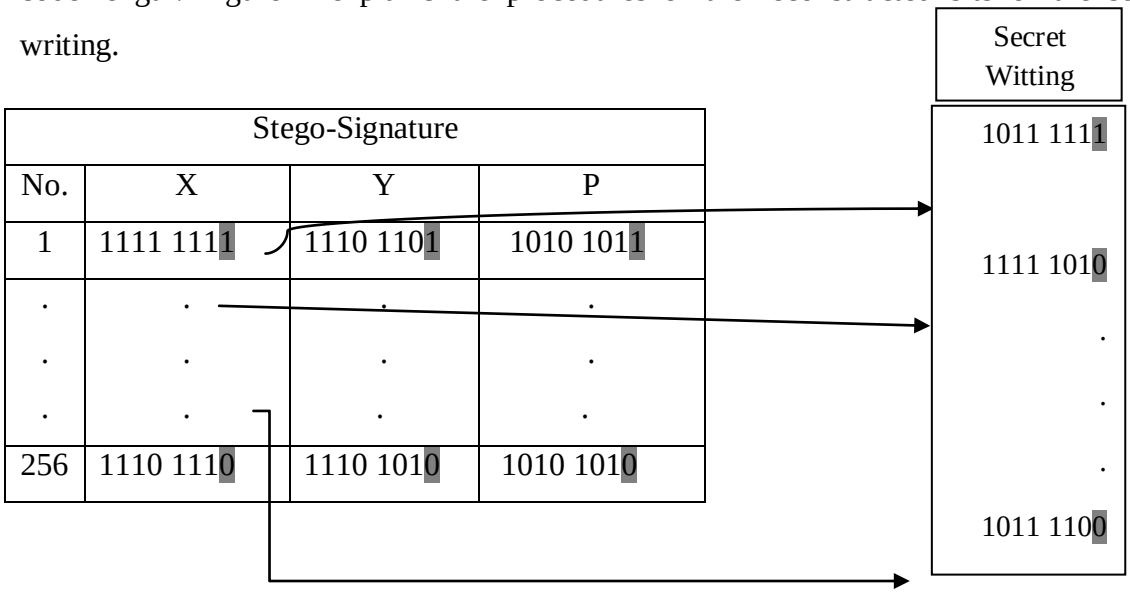

Figure 7: De-Hiding Process by using Least Significant Bit (LSB).

1.4 Implementation

A Graphical User Interface (GUI) has been deployed using Matlab, 2013. The process is similar to software that comprises two windows. First one is used for hiding the secret message which shall be owned by the source party (hider person) as shown below in Figure 8. The second window shall be owned by the second party (de-hider person) as shown in Figure 9. The second party (destination party) must receive two things: first, the stego-signature as .txt file, which carries the secret message information, second, a secret code that has been generated during the hidden operation.

A. Hiding Window

The basic online handwritten signature steganography can be fulfilled by using the designed software programme whose picture is shown in Figure 8. It simply works by putting the text that needs to be secured in the secret text box. After that, by clicking the **Hide** button, the secret text will automatically be converted into binary representation then attached to the online handwritten signature as explained using LSB method. Then, by clicking the **Show Path** to be informed about both: where is the stego-signature is stored, and where is the corresponding secret code stored, which is used for the reconstructing the secret message in the destination party.

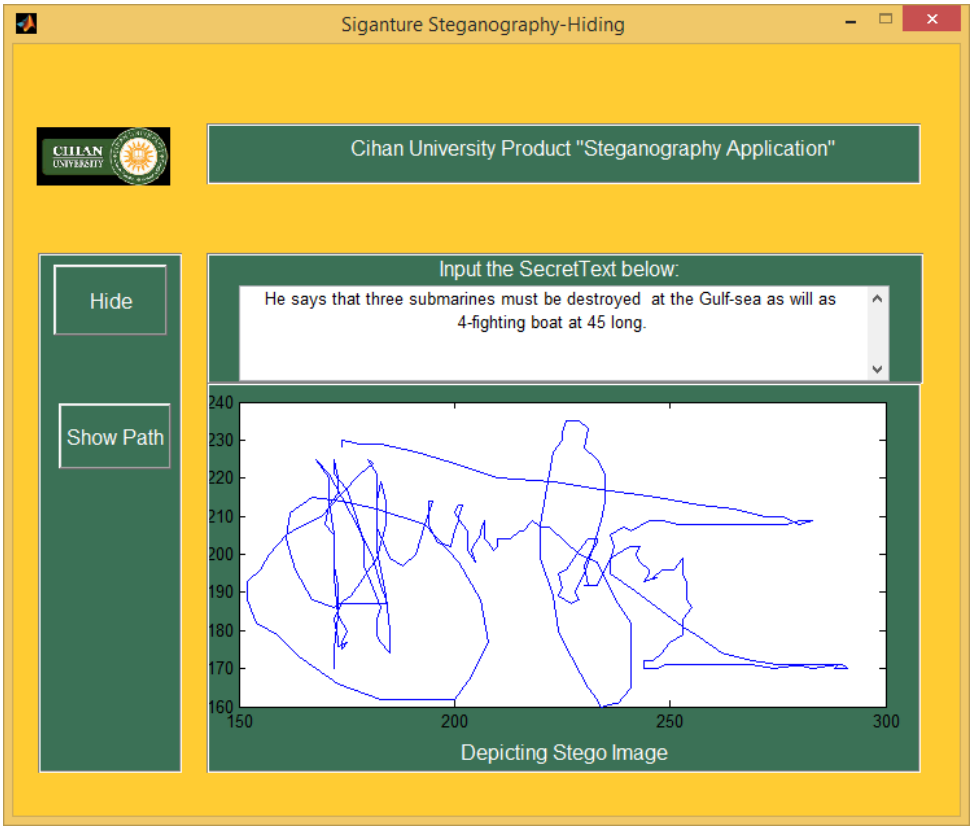

Figure 8: Secret text window for hiding operation.

B. De-hiding Window

To return the hidden text using the de-hiding code, the reconstructed message will appear in the text box of the de-hiding window which is shown in Figure 9 by clicking the De-hide button.

Figure 9: Secret text window for de-hiding operation.

1.5 Result and Discussion

This message has been hidden and then de-hidden, as it is obvious to see there is not any difference between them. The message before hiding is:

"He says that three submarines must be destroyed at the Gulf-sea as well as 4-fighting boats at 45 long."

And after the de-hiding, we can see the same message as:

"He says that three submarines must be destroyed at the Gulf-sea as well as 4-fighting boats at 45 long."

De-hiding secret message in online handwritten signature is new method, and is rarely used nowadays, it has advantages like when changing the stego-file format from .txt to another format, the file is still exists as numbers. Unlike hiding in image, when an image format is changed from .jpeg to .png for example, all the hidden secret information will be shuffled and the secret message will be destroyed, accordingly, it is going to be unable to be reconstructed. On the other hand, the setback of hiding inside online signature is the number of character that might be hidden in the signature is fewer than other hosting media such as image or video or audio.

The maximum number of bits of secret text can be calculated according to the signature length. Here, the length is 3 as (x,y,p) multiplied by 256 (length of each dimension) which equals 768 bits. Once the maximum ASCII code length is 8-bit, this project carries 96 ASCII characters as (768/8).

1.6 Conclusion

Steganography relies on hiding a covert message in unsuspected multimedia data and is generally used in secret communication among acknowledged parties. In this research, a message has been secured by hiding it inside an online handwritten signature, which consists of three features (x,y) as a position trajectories as well as the pressure of the pen (p). The method of the implementation is based on the Least Significance Bit (LSB), which is proved that it is very successful when used with online signature features, because, even if the format of the stego-signature changed, the message will be the same. In other words, the message can protect itself against any format changing. Conversely, the message will be destroyed in case the hiding media is an image or a video. The recognition of the reconstructed the message is 100%, as it is clear that the hidden secured text is the same as exactly before hiding and after de-hiding operations.

In future work, to gain a more robust securing text, we might be using both steganography pipelined along with cryptography by choosing a suitable methods that must be compatible.

References

Bansal, K. L., & Singh, A. (2012). Use of Textual Compression in Steganography and Cryptography. *International Journal of Innovative Research and Development|| ISSN 2278–0211, 1*(8), 109-115.

Chhajed, G. J., Deshmukh, K. V., & Kulkarni, T. S. (2011). Review on binary image steganography and watermarking. *International Journal on Computer Science and Engineering, 3*(11), 3645.

Coronado, A. S. (2013). Principles of Computer Security: CompTIA Security+™. *Journal of Information Privacy and Security, 9*(1), 70-72.

Cummins, J., Diskin, P., Lau, S., & Parlett, R. (2004). Steganography and digital watermarking. *School of Computer Science, The University of Birmingham, 14*, 60.

Handel, T. G., & Sandford II, M. T. (1996). *Hiding data in the OSI network model.* Paper presented at the International Workshop on Information Hiding.

Khan, S., Ahmad, N., & Wahid, M. (2016). Varying index varying bits substitution algorithm for the implementation of VLSB steganography. *Journal of the Chinese Institute of Engineers, 39*(1), 101-109.

Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE transactions on information forensics and security, 5*(2), 201-214.

Malallah, F. L., Ahmad, S. S., Yussof, S., Adnan, W. W., Iranmanesh, V., & Arigbabu, O. (2013). A Review of Biometric Template Protection Techniques for Online Handwritten Signature Application. *International Review on Computers and Software (I. RE. CO. S.), 8*(12).

Malallah, F. L., Syed, S. M. B., Rahman, A. A., Wan, W. A. B., & Yussof, S. B. (2014). Non-Invertible Online Signature Biometric Template Protection via Shuffling and Trigonometry Transformation. *International Journal of Computer Applications, 98*(4).

Muttoo, S., & Kumar, S. (2008). *A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm.* Paper presented at the IEEE, 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE.

Poornima, R., & Iswarya, R. (2013). An overview of digital image steganography. *International Journal of Computer Science and Engineering Survey, 4*(1), 23.

Saraireh, S. (2013). A Secure Data Communication system using cryptography and steganography. *International Journal of Computer Networks & Communications, 5*(3), 125.

Sedighi, V., Cogranne, R., & Fridrich, J. (2016). Content-adaptive steganography by minimizing statistical detectability. *IEEE transactions on information forensics and security, 11*(2), 221-234.

Shejul, A. A., & Kulkarni, U. L. (2011). A secure skin tone based steganography using wavelet transform. *International Journal of computer theory and Engineering, 3*(1), 16.

Szczypiorski, K., & Mazurczyk, W. (2016). Steganography in IEEE 802.11 OFDM symbols. *Security and Communication Networks, 9*(2), 118-129.

Yadav, P., Mishra, N., & Sharma, S. (2013). *A secure video steganography with encryption based on LSB technique.* Paper presented at the Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on.