Penerbit Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

A Security Enhanced Robust Image Hiding Algorithm from Digital Signature

E. Noroozi [*,1,a], *S. M. Daud* [1,b] *and A. Sabouhi* [2,c]

[1]Advanced Informatics School (AIS), Universiti Teknologi Malaysia, Malaysia, Kuala Lumpur
[2]Advanced Software Engineering of Computer Science Kuala Lumpur, Malaysia
[*,a]*nerfaneh2@live.utm.my*, [b]*salwani@ic.utm.my*, [c]*Ali_sabouhi@yahoo.com*

Abstract – *The objective of this study is to adopt of digital signature as a stego-image into the cover image enhance the robustness of image steganography. Implementing an encryption algorithm in the spatial domain steganographic method can contribute to increasing the degree of security. The ability to create dynamic digital signature is highly related with the integrity and robustness of the image steganography. Unfortunately, there is wide variety of attacks that effect on quality of image steganography, although there are methods for data hiding but they are still very weak in resisting of attacks. Hence the benefits of this encryption algorithm are computational efficiency, digital signature with the size as small as 8 bytes and minimize bandwidth in comparison with other digital signature methods. In messages with the sizes smaller than 1600 bytes, the hashed file reduces the original file up to 8.51%.*

Keywords: Security, Cryptography, digital signature, Steganography, PSNR

1.0 INTRODUCTION

Ever since people have succeeded in making connections among themselves, the issue of confidential (private) connection came to attention. At first; the application of confidential connection was mostly in martial issues. With the development of civilization, the use of ciphering in issues like politics became essential. Ciphering systems developed with the passage of time, but up until before the Second World War, ciphering was considered as a form of art. In the Second World War and after the issuance of the article of Shannon, ciphering was then followed as science. Figure 1 shows a ciphering system.

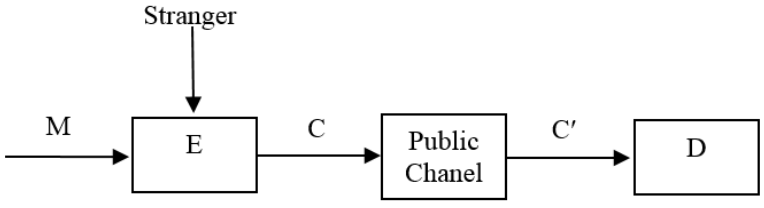


Figure 1: Block Diagram of Encryption System

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

In this figure, the M plain text by E converter is converted to C cipher text and is entered in the insecure channel. The enemy can eavesdrop and intend to reach to the plain text (the passive attack) or after receiving the C cipher text, intend to change it (the active attack). The receiver by receiving C′ text and using the D converter deciphers the cipher text. With accordance to the kind of the enemy attack, there are two essential issues of security and authenticity in the message in ciphering. The D converter is to maintain the security of the message and as for maintaining the authenticity of the message; the E converter should remain confidential (private). In the ciphering systems, there are two important divisions. In one of the divisions, the ciphering systems are divided to block and stream cipher systems [1].

2.0 CRYPTOGRAPHY AND DIGITAL SIGNATURE SCHEME

The idea of digital signature was taken from the manual signature. Therefore, digital signature should have all the properties of manual signature. The main properties of manual signature are easy production, easy identification and difficult when it comes to its fabrication [2]. Digital signature is produced by machine. The machine considers the input prepared by the signer thus produces a tail. To prevent fabrication, no one else should be able to produce the tail which requires the concealment of the input of the machine [3]. Nonetheless, digital signature should not be fixed. This is because the fabricator can add these tails to every message. Thus, digital signature should be dependent on the message. Considering the above mentioned issues, the properties of digital signature can be stated as the followings: the signature should not be forgeable by anyone including the receiver and the sender should not deny his signature. Since Diffie and Hellman proposed digital signature, various methods for digital signature have been raised to attention. According to the functions applied in them, digital signatures can be divided into 3 classes; i. Signatures based upon symmetric systems, ii. Signature based upon public key systems, iii. Signature based upon conversions independent of ciphering systems. Many of the methods of digital signature in symmetric systems are single-use [4].

Image steganography is about making use of the limited powers of the human visual system (HVS). Anything that can be embedded and put in a bit stream can be hidden and concealed in an image. Steganography has come quite far in the recent years by the development of powerful graphical computers [5]. Monochrome and grayscale images use 8 bits for each pixel and are able to show 256 different colours or shades of grey. Digital colour images are normally stored and saved in 24-bit files and they use the RGB colour model, also known as ‘true colour’ [6]. The variety of image steganography techniques are: First, the substitution technique in spatial domain. In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object [7]. It is the simplest method for hiding data but spatial domain steganography algorithm is not highly secure against different attacks such as compression and transformations [8]. Next, Transform domain technique means the various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images. Thirdly, is spread spectrum technique which means the message is spread over a wide frequency bandwidth that requires minimum bandwidth to send information [9]. Fourth is the statistical technique which the cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of the cover image.

Penerbit
Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

3.0 PROPOSED ALGORITHM

Digital signature usually encodes the signature in a file separated from the original image, thus require extra bandwidth to transmit it. Scheme extracts the signature from the original image and embeds them into the image, avoiding additional signature file. In this algorithm by doing operation on first 100 bytes, the first byte is read by fetch function. On the condition that, the rate of the loaded bytes is zero, we will change it to 1. So that these loaded bytes will be set in 32 different bits and the second byte from 100 byte block. On the condition that this is the last byte, the result will be put in 32 bytes and changed in hexadecimal and displayed and if it is not the last one, the result will be multiplied in 32 different bites and with the result, less than 32 bites, from the left side, zero will be added to fill dates in that 4 bytes. If the result is more than 4 bytes, it puts lower 32 bits and we do it till the last byte. Placing embedded data in the original file is a kind of saving in sending data. For this reason, operational process cannot be conducted on 3 bits; definitely the operation must be performed on one byte. In this case, we need an algorithm that can modify the original file, with 5 bits, in the left side is equal to '0' (00000 + data), and 3 bits in the least significant bit is the embedded data. With the use of public key encryption method, we consider a private key with named password. By choosing Load Key, the in case private key is entered in the software's memory (Figure 2).

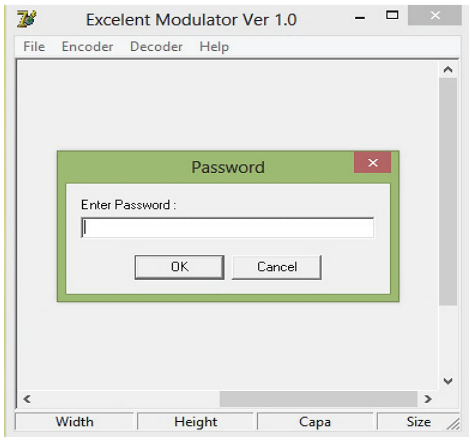
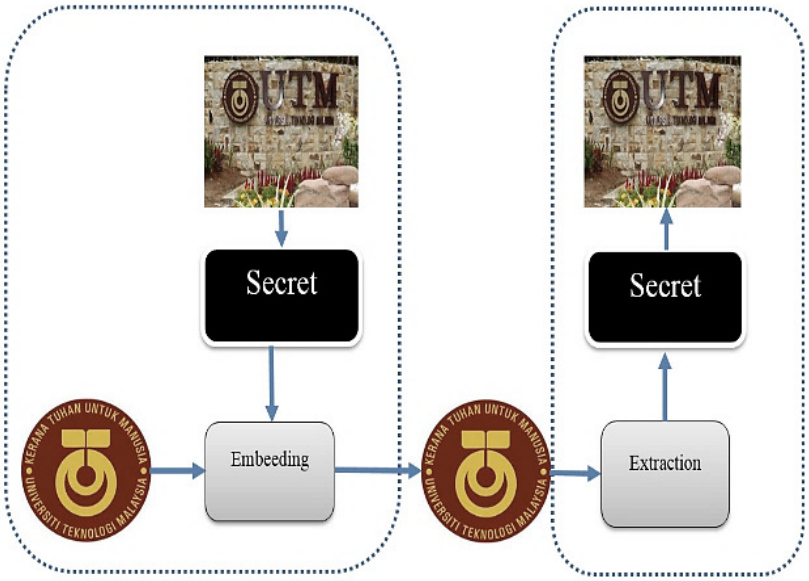


Figure 2: Generate Private Key in Steganographic System

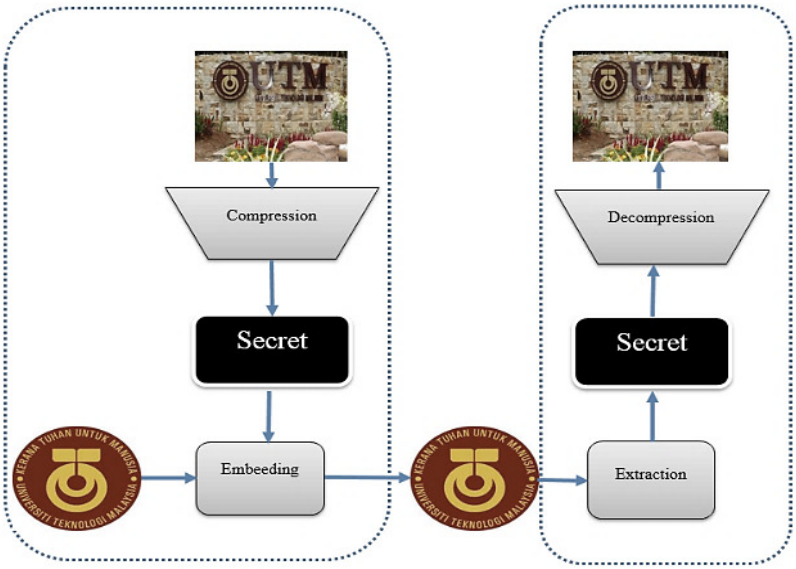
In the sender section, from the Encoder menu, we choose the select bmp image that is applied for choosing cover image. For making stego image, we have two kinds of buffer for putting the cover image into it. One of them is the normal buffer that we use in the import file to normal buffer switch for putting the cover image into it. Next, when we want to embed a large file size into the cover image and in this case, we should compress it and then put it into the cover image thus resulted in creating a compress from normal switch (Figure 3).

Penerbit
Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015



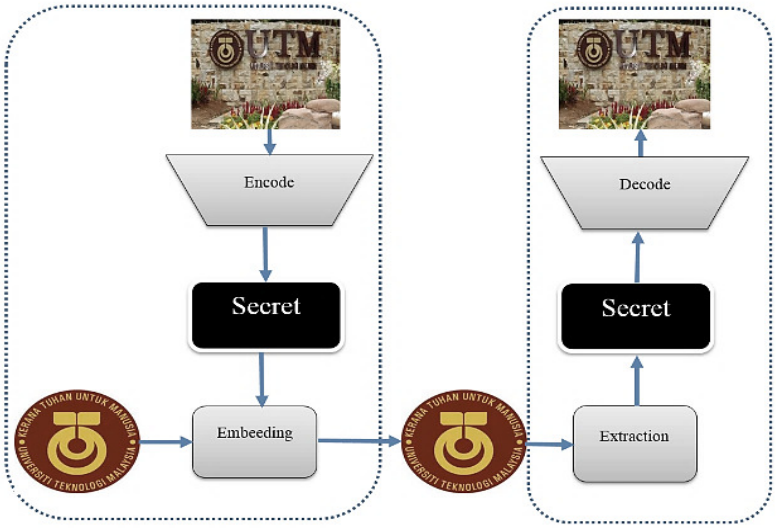
(a)



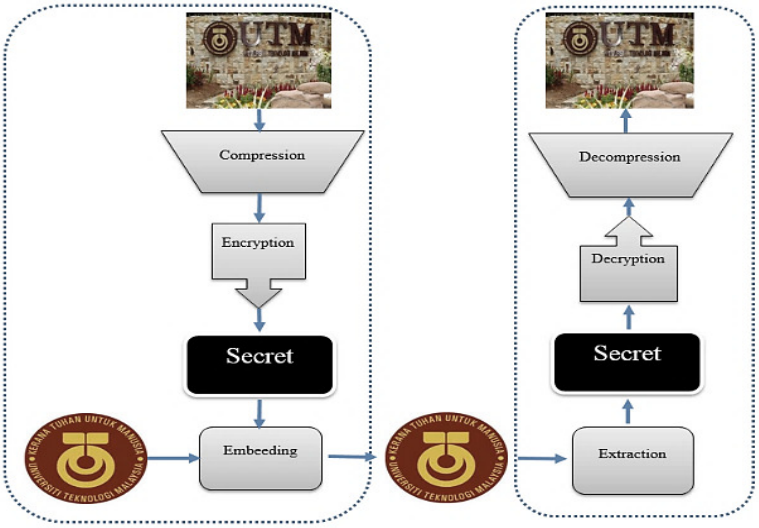
(b)

Figure 3: Embedding Image (a) Normal Embedding, (b) Compression Embedding

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015



(c)



(d)

Figure 4: Embedding Image (c) Encoded Embedding, (d) Encoded Compression Embedding

In embedding the encoded compressed data, we choose the put compress to bitmap switch and save option so that the essential changes will be saved in the stego-image (Figure 4). We need to consider the various states that are in the sender and the user is privileged to choose the states with consideration of the condition of the attached file. What is stated will be made in the receiver.

3.1 Definition of Proposed Algorithm

We consider a random number between *"(0 .. 2^n-1)."* We then replace the chosen number with the first cell and in this order; we choose a random number for the second cell and replace the contents of the two cells (Figure 5).

Penerbit Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

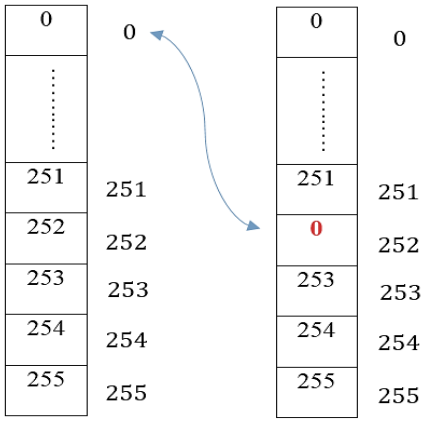


Figure 5: Block Diagram of Encryption System

In the first cell, there are 2^n states and in the second cell, there are2^n-1 states and etc., within this order in the last cell, there is 1 state that means:

$256 \times 255 \times 254 \times \ldots\ldots\ldots\ldots \times 1 = (2^n)!$. The number of Encode matrixes that are associated with n equals $(2^n)!$. We do this iteration 2^n times, so; we would have 2^n Encode matrixes, for n equals 8, consequently it equals $2^8 = 256$. In total, we should have 256 Encode matrixes that we have changed their names from E_0 to E_{255} which means 256 matrixes as a whole. After the first running of the Encode function, we would have a matrix with a named password that would be 256×256, and of the area of this matrix equals to: $S = \frac{n \times 2^n \times 2^n}{n} = (2)^{2n}$. If n equals 8, consequently it equals to 2^{16}=64 KB. Here we have created the password matrix. Encode operation is done by using this password.

4.0 PROPOSED ALGORITHM

The generation of a signature can be divided into two parts: feature hash function and encryption of hashed messages and embedding digital signature into image. We describe an effective technique for content-based image authentication that is based on the robust authentication signature. In this method, for every original data, one signature with a lengthy key is produced randomly. Digital signatures that are produced by public key can be applied in any cover-image that is necessary because in these methods digital signature is a function of the message and a lengthy key (private key). The digital signature is the electronic analogue of the handwritten signature. A signer can digitally sign a document with his/her secret key (Private Key), and embeds a signature on that cover-image as shown in Figure 6. To hide the digital signature we have to create a cover image. This cover image is divided into three matrices (Red, Green and Blue).

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

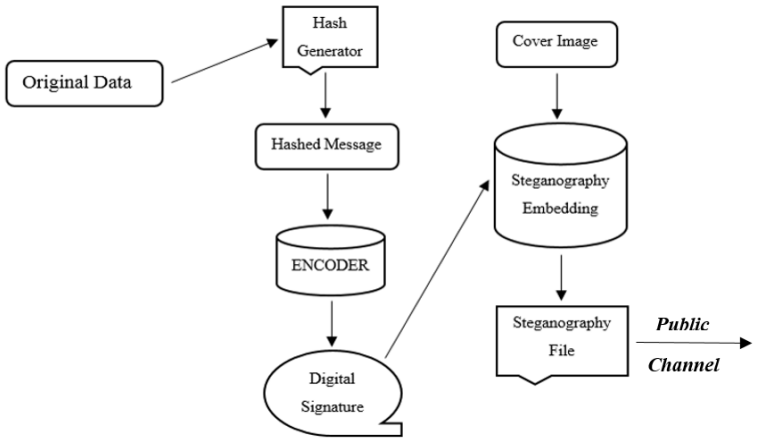


Figure 6: Generating and Embedding Digital Signature into Image in the Sender Side

Next, he/she sends the generated signature, a document and his\her public key to any verifier. Thus, an extractor can check the validity of the signature with the corresponding public key (Figure 7). The authentication and integrity is verified by comparing the signature and stego-image both extracted from the received image.

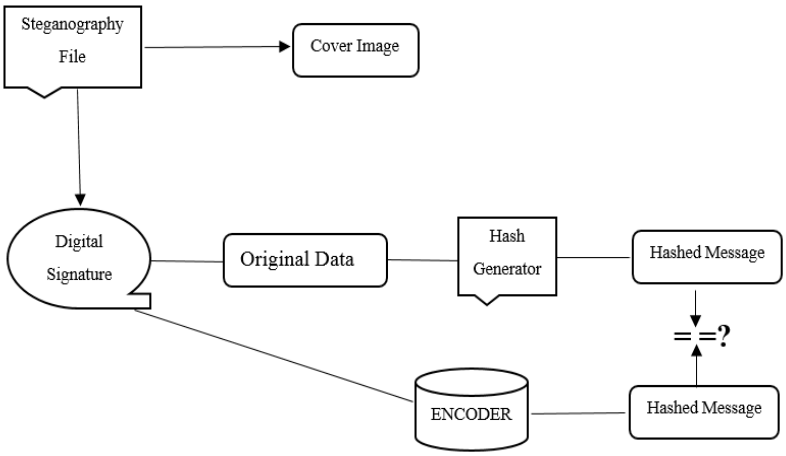


Figure 7: Verifying and Extracting a Digital Signature from the Image in the Receiver Side

Experimental results shown in this section is to demonstrate the performance of our proposed method. We used standard RGB (true colour) images as the cover image. In this section, some experiments were designed to prove the efficiency of the proposed scheme. First, we showed that the scheme is capable for image authentication. Secondly, the image quality after steganography insertion is investigated.

Penerbit Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

5.1 IMAGE AUTHENTICATION

This part focuses on the security of steganography organization and how the researchers measure the value of the cover multimedia file after they have embedded a secured message. The peak signal-to-noise ratio (PSNR) metrics is a prevalent and sound method that is used to evaluate the image quality and measure the likeness between two images and the size of it. It is described through the mean squared error (MSE) and for two *m x n* monochrome images I and K when one of them is a noisy approximation of the other. The prevalent measurements that are used are: signal to noise ratio (SNR), peak signal to noise ratio (PSNR), mean squared error (MSE) and root mean square error (RMSE).

The peak signal to noise ratio (PSNR) computes the peak signal to noise ratio between two images. The PSNR shown in Equation 2; MSE describes square error and Max shows the high cost of calories which is 255 (Ding et al., 2008). MSE is a squared error and PSNR is a peak signal to noise ratio that has been used for video and image doling out as reliability metrics (PSNR). It is a logarithmic demonstration of MSE and RMSE that shows the square root of (MSE). It is not that complicated to use these measurements as it is fast and their computation is easy to be understood hence the popularity. The MSE describe in Equation 1.

$$MSE= \frac{1}{m*n} \sum_1^m \sum_1^n (Aij-Bij)^2 (Aij)^2 \quad (1)$$

$$PSNR=10* \log \frac{(Max)^2}{\frac{1}{m*n} \sum_1^n \sum_1^m (Aij-Bij)^2} \quad (2)$$

Figure 8 illustrates the total length of the digital signature from original file with 124 Kb generate dynamic. Smaller hashed message (10 Kb) is embedded into the image as a stego-image and finally, the receiver is extracted from the cover image. (Table 1)

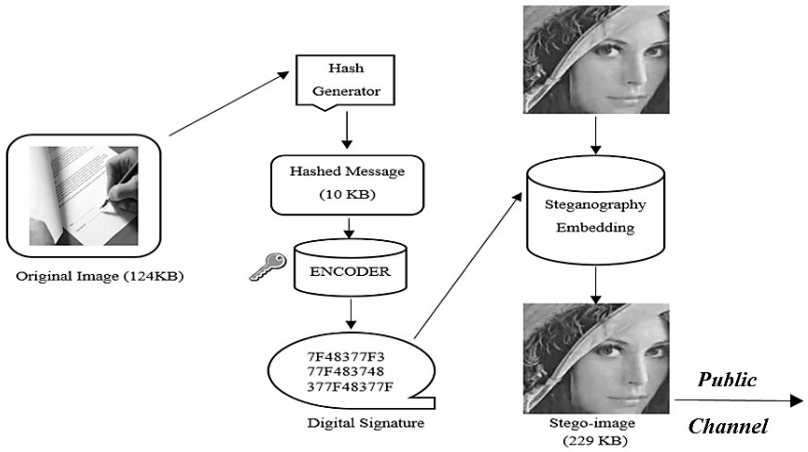


Figure 8: Block Image Authentication that Verifies the Originality of the Received Image

Penerbit Akademia Baru

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

Table 1: Block Diagram of Encryption System

Original File Size	**Hashed File Size**	**Digital Signature Size**	**Cover Image Size**	**PSNR (db)**	**MSE (db)**
124	10	1	229	54.21	0.2996

The researchers used 51Kb from the image to embed the information and the PSNR value for their approach is 4l.ldb [11]. Then again, Chang et al., [12] used 53 Kb from the image to hide the information. The PSNR value of their method is 34.84db. Moreover they [13] increase the capacity to 389 Kb while the PSNR value is only 4l. The MSE has been used to measure the efficiency of their proposed method and found that by hiding 50Kb, the MSE value is 2.07 db [14].

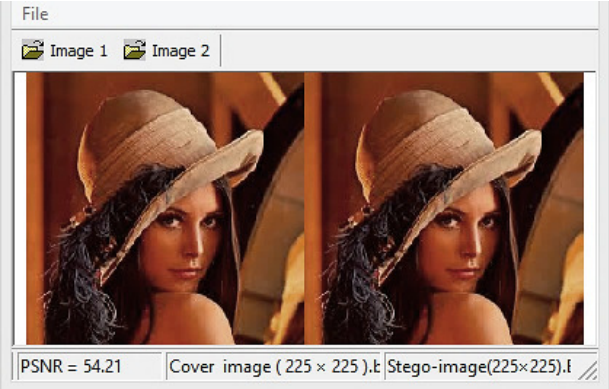


Figure 9: Psnr of Cover-image and stego-image

We calculated the PSNR and MSE values of the cover image and stego-image. These values are displayed in Figure 9. We used 229 Kb from the image to hide and embed the digital signature into image. The PSNR value from the method is 54.21 db and the MSE value is 0.2996db. It can be said that the larger PSNR, the better the quality of the images or the lower the distortion, the smaller possibilities of visual attack by the human eyes. When the Mean Square Error (MSE) approximates to zero, PSNR value comes close to infinity and it shows that a higher image quality is the result of higher PSNR and when PSNR value decreases,

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

there would be a bigger distortion between stego-image and cover image. Abbreviation and acronyms should be defined the first time they appear in the text, even after the have already been defined in the abstract. Do not use abbreviations in the title unless they are unavoidable.

4.1 Image Quality

We will show that the scheme is capable to image authentication. The 256*256 Lena image of 8-bit primary colour is used in these experiments. In signature generation, the image is divided to blocks of pixels. 9 bits are extracted from each block. The digital signature is extracted from the cover image and inserted back into the image as a stego-image. Then, a small area of the stego-image is manipulated. In the receiver's side, the digital signature is extracted from the image which has been manipulated. Then, the modified space is distinguished whether if the digital signature and stego-image are not the same in the corresponding blocks. Figure 10 shows a little square is put on the upper-right of the stego-image. In authentication, the differences in PSNR of the signature and stego-image indicate the modified area that is shown in Figure 10.

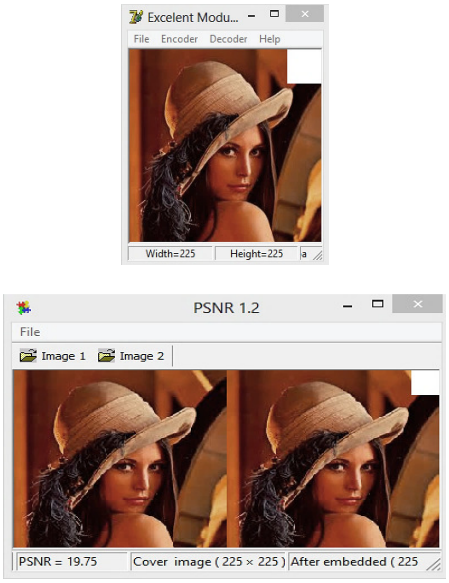


Figure 10: Psnr of Cover-image and Stego-image after Modifying

5.0 CONCLUSSION

Cryptography and image steganography are two popular techniques to provide security. One hides the existence of the message and the other distorts the message itself. Using cryptography, the data is transformed into some other gibberish form which the encrypted data were then transmitted. In image steganography, the data is embedded in an image file and the image file is transmitted. In this paper, a combined digital signature and image steganography scheme is proposed for image authentication. The proposed scheme extracts signature from the original image; avoiding additional signature file. Furthermore, the scheme would not only be able to verify the authenticity and the integrity of images, but also

can locate the illegal modifications. Experiments showed that our scheme is robust to changes while preserving good image quality, and capable for authentication. We have proposed better PSNR and MSE value where larger PSNR and lower MSE indicate better quality of the image or in other terms lower distortion.

ACKNOWLEDGEMENT

The authors would like to express greatest appreciation to Ministry of Education (MOE), Malaysia and Universiti Teknologi Malaysia for providing the grant to carry out this research work with vot number R.K130000.7838.4L073. Last but not least, the authors would like to thank Advanced Informatics School, Universiti Teknologi Malaysia for their support of this project.

REFERENCES

[1] E. Teske, Square- Root algorithms for the discrete logarithm problem, Proceeding of the Conference on Public Key Cryptography and Computational Number Theory, 2001, pp. 283-301.

[2] A. Sinha, K. Singh, A technique for image encryption using digital signature, Optics Communications 218 (2003) 229-234.

[3] K. A. Saadi, A. Bouridane, A. Guessoum, Combined Fragile Watermark and Digital Signature for H. 264/AVC Video Authentication, In EUSIPCO, Vol. 9, 2009, pp. 1-4.

[4] C. H. Wu, Self-Generated-Certificate Digital Signature", Genetic and Evolutionary Computing (ICGEC), Fourth International Conference on IEEE, 2010, pp. 379-382.

[5] J. Fridrich, Jiri, R. Du., Secure steganographic methods for palette images, Center for Intelligent Systems, Information Hiding, Proceedings of the Third International Workshop, IH_99 Dresden Germany, 2002, pp. 47-60.

[6] J. Fridrich, M. Long, Steganalysis of LSB encoding in color images, Multimedia and Expo, ICME, 2000 IEEE International Conference, Vol. 3, 2000, pp. 1279-1282.

[7] K. Sara, A new steganography method based on HIOP (Higher Intensity of Pixel) algorithm and Strassen's Matrix Multiplication, Journal of Global Research in Computer Science 2 (1) (2011) 6-12.

[8] A. A. Zaidan, F. Othman, B. B. Zaidan, R. Z. Raji, A. K. Hasan, A. W. Naji, Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography, Proceedings of the World Congress on Engineering Vol. 1, 2009.

[9] B. Swathi, K. Shalini, K. N. Prasanthi, A Review on Steganography Using Images, Asian Journal of Computer Science and Information Technology 2 (2012) 707-710.

Journal of Advanced Research in Applied Mechanics
ISSN (online): 2289-7895 | Vol. 8, No. 1. Pages 1-12, 2015

[10] J. Ding, B. Y. Yang, C. H. Chen, M. S. Chen, C. M. Cheng, New differential-algebraic attacks and reparametrization of rainbow, Applied Cryptography and Network Security, Springer Berlin/Heidelberg, 2008, pp. 242-257. \

[11] C. Wang, Ming, N. Wu, Tsai, C. S. Hwang, A high quality steganographic method with pixel-value differencing and modulus function, The Journal of Systems and Software 81 (2007) 150-158.

[12] C. C. Chang, T.S. Chen, L. Z. Chung, A steganographic method based upon JPEG and quantization table modification, Information Sciences 141 (2002) 123-138.

[13] C. C. Chang, H. W. Tseng, A steganographic method for digital images using side match, Pattern Recognition Letters 25 (2004) 1431-1437.

[14] D. C. Wu, W. H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (2003) 1613-1626.