A New Steganography Technique Using Magic Square Matrix and Affine Cipher

Waleed S. Hasan Al-Hasan, Muhammad Mun'im Ahmad Zabidi, Ab Al-Hadi Ab Rahman
Faculty of Electrical Engineering, Universiti Teknologi Malaysia,
81310 Johor, Malaysia.
wsh_waleed@yahoo.ca

***Abstract*—The need for methods to provide effective protection of data has become necessary due to the huge growth of multimedia applications on networks. Steganography is one of the most widespread approaches to protecting data. The challenge of steganographic methods is to create a rational balance between the quality of the file and the size of data that can be transferred. In addition, the robustness of the technique and security of the obscure data are key factors in determining the effectiveness of the algorithm. In this paper, a new steganography approach is proposed to fulfill the requirements of steganography which are imperceptibility, payload, and robustness. First, the cover image is converted from RGB color space to YCbCr color space. Then, Cb or Cr channel is selected to hide the secret data. The secret data is encrypted using Affine Cipher to increase its security. The Magic Square Matrix is applied to embed the secret code onto the Cb or Cr component using ISB (Intermediates Significant Bits) approach. Finally, the cover image is evaluated after applying the salt-and-pepper noise. The results show that the new proposed method not only improves the security of the payload but can also withstand against attacks.**

***Index Terms*— Steganography; Stego-image; ISB; Magic Square; Affine Cipher.**

I. INTRODUCTION

In this modern era, information security is very important because the world has become a global village. The need for approaches to providing effective protection of private data has become necessary because of the huge growth of multimedia applications. It is therefore important to create techniques that protect the media from unauthorized, unethical and illegal use by the attackers or hackers.

The most popular techniques for dealing with data security are Steganography and Cryptography. Cryptography is a method of protection for data storage using a secret key during data transfer. Encryption is still a successful method to protect stored data and to transmit over the network. With the growing use of networks for sending and receiving data globally, it has become more difficult to maintain the data security. Steganography protects information by preventing the detection of hidden messages [1]. The advantage of steganography over cryptography is that the messages do not arouse interest in themselves.

Two procedures are used in steganography. The first procedure is embedded consists of two inputs: payload and cover image (host image). The payload is the secret message that is going to be embedded whereas the cover image is an image used as a cover which contains the embedded message. After the embedding process is completed the resulting image is called stego-image and is ready for transmission to the receiver. The second procedure is a detector. The input for the detector is the stego-image, and the detector can recognize the secret message through an extraction process [2]. As a result, the stenography is considered a method of information protection that can utilize the host media as a cover for instance images, audio or video.

II. BACKGROUND OF THE PROBLEM

Several techniques have been proposed to conceal data inside the cover image. The most popular approach is the Least Significant Bit (LSB) technique, which is based on substituting the least significant bit with bits of embedded information inside the cover data of some or all bytes [3]. A slightly more secure system is by sharing secret keys between sender and receiver, which allows only certain pixels to be changed and in this way it would be difficult to retrieve the message without having the "Stego_key".

In steganography, it is very hard to embed a large amount of data and to preserve high image quality at the same time. Therefore, if it is required to have more payload steganography algorithm, its image quality will be low and vice versa [4].

Several techniques have been developed to increase the reliability and security of hiding data, but all of them have some disadvantages. GLM (Gray Level Modification), PVD (Pixel Value Differencing Method), and DWT (Discrete Wavelet Transform) are examples of steganographic techniques [2]. In fact, it is important to ensure that the most suitable technique is used for a particular application. However, imperceptibility, payload capacity, robustness against manipulation and statistical attacks are the main factors that should be taken into consideration.

Today, the important question is how we can increase the amount of the imperceptibility, robustness and maintaining the high quality of the image? In this research, the ISB method, Affine cipher and Magic square are applied to embed a large amount of secret data, while preserving the high image quality as compared to previous methods and to show high tolerance to statistical attacks such as noise.

This research intends to achieve the following objectives:

- To adopt the affine cipher in the secret messages of the proposed technique to make it highly secure.
- To propose an improved steganography technique for color images based on the Hybrid method combining Intermediates Significant Bits (ISB) and Magic square to increase the security.
- To evaluate the robustness, the performance of the proposed method against salt pepper attacks is analyzed.

III. Image Steganography Evaluation Parameters

The color and smoothness (visual specification) of an image are disturbed when a large amount of data is embedded in the image. The basic concept of the steganography is to hide information (cover data) without giving any clues to the attacker, but the specification that how the secret is embedded in the image is very important. Some essential factors must be considered in the image during the steganography process:

- *Capacity*: Defined as the number of maximum bits that can be embedded in a given cover file with a negligible probability of detection by a third party. Embedding capacity is the amount of information that can be embedded in a given cover medium and is larger than steganography capacity [5]. Indeed by having a vast amount of secret data, the appearance of the cover media will alter.
- *Imperceptibility*: Defined as the strength of changes regarding the visual appearance of the cover image when the message is embedded. In simple terms, the appearance or format of cover images must remain natural to the observer after hiding the secret data because the steganography method is not considered a success if a third party suspects the existence of the secret message.
- *Robustness*: Defined as refers to the amount of distortion that can be endured by the cover image before the hidden message is destroyed [6]. Since the purpose of steganography process is to hide the existence of the secret data, the message should be embedded in such way that it cannot be easily extracted from the cover medium.
- *Security*: Defined as the assurance of keeping the secret data unreadable to the adversary when attacks extract it.

IV. Proposed Steganography Method

This work proposes a new hybrid technique for hiding data composed of two different techniques. First, we use an affine cipher for encrypting the secret message. Second, the encrypted message is embedded using a hybrid method based on Intermediate Significant Bits (ISB) and Magic square. Figure 1 and Figure 2 show the embedding and extraction processes flowcharts respectively.

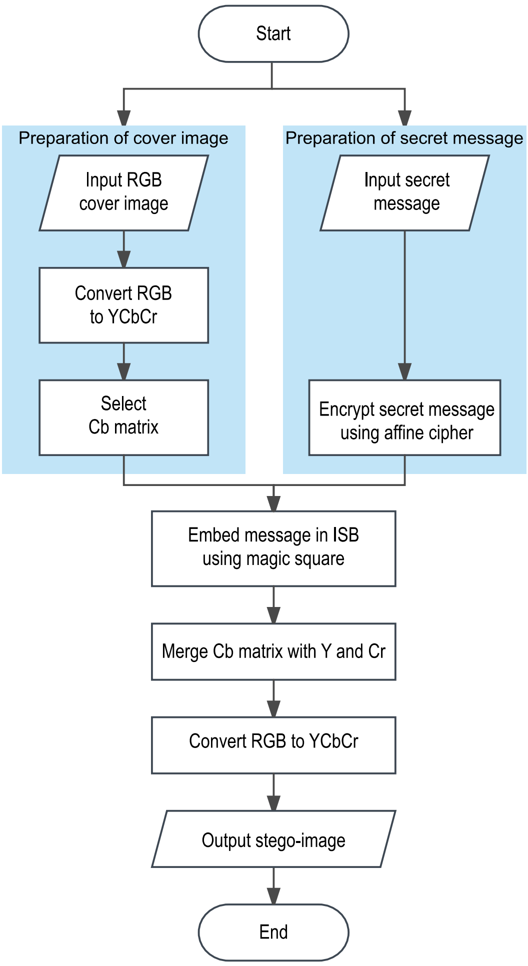

Start
Preparation of cover image
Input RGB cover image
Convert RGB to YCbCr
Select Cb matrix
Preparation of secret message
Input secret message
Encrypt secret message using affine cipher
Embed message in ISB using magic square
Merge Cb matrix with Y and Cr
Convert RGB to YCbCr
Output stego-image
End

Figure 1: Embedding Phase

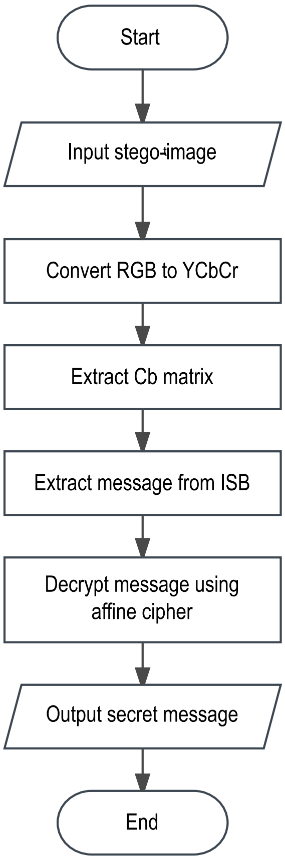


Figure 2: Extraction Phase.

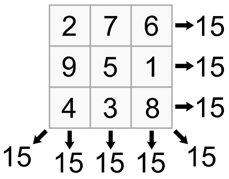
A. *Embedding Process*

The embedding phase consists of activities to hide and protect the data as secret in the cover image. The sender through different algorithms encodes and compresses the data to include the bit stream in the cover image and inserts the data into the bit-stream. Further, the secret key is defined and its location is known only to the sender and receiver. The secret key is at the first position of the bit stream within the image. The sending process consists of the following procedure:

- *Affine Cipher* (Encrypting the Secret Message): The Affine cipher belongs to the family of mono-alphabetic substitution ciphers. In this type of ciphers, each letter is encrypted using the algebraic function by mapping the alphabetic character to its numeric correspondent and restored to a letter. The affine cipher formula can be interpreted as standard switch cipher which is controlled by a rule that which letter will be replaced by which another letter. The function used to encipher each letter is ($ax+b$) mod (26) where b is the shift-magnitude.
- *Converting Pixel Values to YCbCr*: The image coder converts the RGB colour space images to YCbCr colour space if the RGB colour space was used. The YCbCr separates the luminance and chrominance in the image. The Cb-channel is responsible for chrominance in the blue direction while the Cr-channel is responsible for the chrominance in red direction while the Y-channel is responsible for the luminance.
- *Embedding*: Embedding algorithm is very important to complete the steganography process. There are many algorithms used to embed the image with the secret data. However, the main goal is to ensure that the secret data is hidden and not detectable by others in the cover image. In our research, we used the Magic Square matrix order for hiding the bits of ASCII codes of the characters and the ISB method to hide each bit in the pixels of the cover image.

The "Magic Square" is an arrangement of numbers from 1 to n^2 (n-squared) in an $n\times n$ matrix, with each number occurring exactly once, and such that the sum of the entries of any row, any column, or any main diagonal is the same. It is not hard to show that this sum must be $n\times(n^2 + 1)/2$. The order of magic square is used to hide the bits of ASCII code for each character. The cover image is divided for 3×3 magic squares matrices and the bit hidden in order of magic square as shown for example in Figure 3.

The ISB method is used to hide the bits of character in each pixel of the image. One character consists of 8 bits and each pixel consist of one byte (8 bits) therefore we need 8 pixels to hide one character. The Least Significant Bit (LSB) can be used, but it is very easy to detect because most data hiding algorithms use it. On the other hand, the Most Significant Bit (MSB) contains most of the pixel information and using this bit alters the pixel value significantly. In our approach, the intermediate bits or Intermediate Significant Bits (ISB) are used instead. We will use b1 to hide the bit as shown in Figure 4.



2	7	6	→15
9	5	1	→15
4	3	8	→15

Figure 3 Magic Square

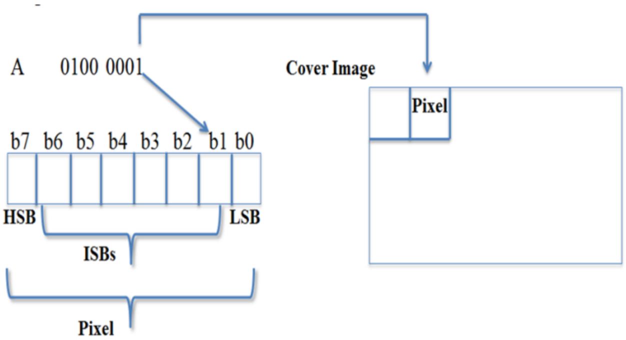


Figure 4: Intermediate Significant Bit (ISB) Method

B. *Salt-and-Pepper Noise*

Salt-and-pepper noise is a form of noise sometimes seen on images. It presents itself as sparsely occurring white and black pixels. An effective noise reduction method for this type of noise is a median filter or a morphological filter. For reducing either salt noise or pepper noise, but not both, a contra harmonic mean filter can be effective. In our method, the data will be protected because the bits which contain the data are the ISBs not in MSB or LSB which this noise attacked.

C. *Extraction Phase*

The receiver should reliably recover the hidden data within the Stego-image. Thus for the recovery of the original message another procedure is required. The steps of the recovery functions, which will be performed in this phase, are the following:

1. Convert the RGB to YCbCr
2. Select the Cb component.
3. Extract secret data by using the inverse process for Magic square and ISB method
4. Decrypt the secret data to get the original text by using Affine Cipher.

V. Results and Analysis

The data used in this study is explained briefly. These cover images used consists of four standard RGB images of 512×512 pixels plus some others. They are Lena, Baboon, Airplane, Goldhill, Sailboat, Tiffany and Peppers. These images contain different colours and help to obtain precise results for evaluating the imperceptibility.

Furthermore, arbitrary plain text is used as the secret message. To evaluate the quality of stego-image, the peak signal-to-noise ratio (PSNR) of each image is measured:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (1)$$

where MSE = the Mean Square Error between two pixels.

$$MSE = \sum_{i=1}^{r*c} \frac{(g_i - g'_i)^2}{r*c} \qquad (2)$$

where, r and c are the number of rows and columns in the image, g_i and g'_i are the cover and stego- images respectively.

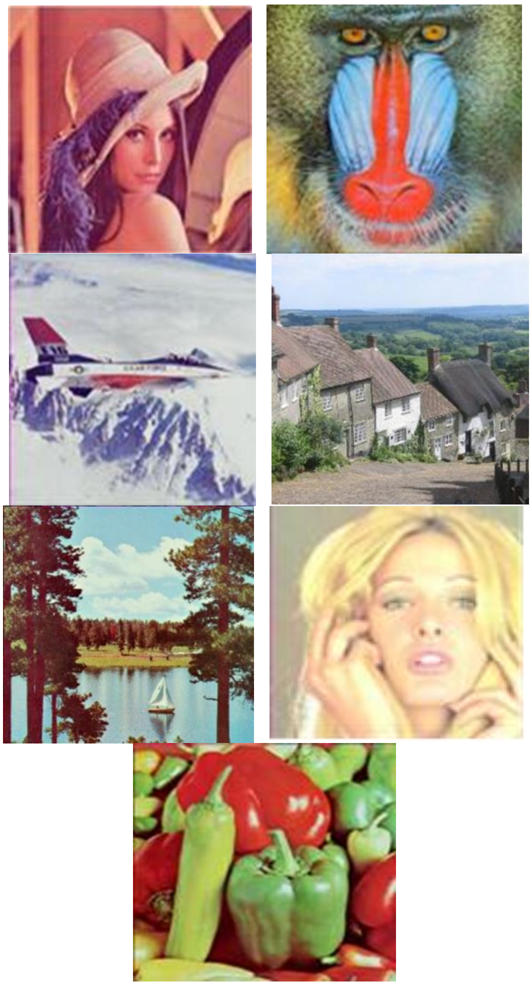


Figure 5: Images used in imperceptibility assessment.

A. Imperceptibility Result of the Proposed Method

The proposed method ensures that all the decimal codes of the affine cipher code are hidden inside the cover. The proposed method is based on the imperceptibility of the system and Tables 1 below show the result of the proposed method process in db.

Table 1 depict the results of the proposed method in terms of imperceptibility for two different channels using Cb and Cr, to embedding rate ranging from 1KB to 32KB, and seven variants images, namely, Lena, Baboon, Tiffany, Goldhill, Sailboat, Peppers and Airplane are employed as host images. The results have revealed that the imperceptibility for both color channels is almost identical whereby, the PSNR decreases as the embedding rate increases. For example, in Table 1, the PSNR was 58.65 dB when the embedding rate was 1KB and gradually decreased as embedding rates increased. Furthermore, the PSNR of the Cb channel is higher than that of Cr channel with the embedding rate from 2KB to 16KB.

Table 1
Imperceptibility Results of the Proposed Method.

Embedding rate		1KB	2KB	4KB	8KB	16KB	32KB
Lena	Cb	58.65	55.77	52.96	49.97	46.96	43.88
	Cr	58.96	55.96	52.96	49.83	46.82	43.83
Baboon	Cb	58.87	55.94	52.97	49.91	46.9	43.86
	Cr	58.56	55.55	52.73	49.91	46.88	43.89
Airplane	Cb	59.02	55.95	52.82	49.87	46.97	43.92
	Cr	58.58	55.46	52.34	49.31	46.24	43.3
Goldhill	Cb	59.02	56.02	53.11	50.1	47.05	44.16
	Cr	59.26	56.31	53.36	50.08	46.97	44.03
Sailboat	Cb	59.18	55.96	52.91	50.02	46.94	43.9
	Cr	58.9	55.9	52.89	49.86	46.81	43.84
Tiffany	Cb	58.98	56.06	53.19	50.15	47.09	43.97
	Cr	58.89	55.99	53.24	50.2	47.28	44.37
Peppers	Cb	59.1	55.96	52.99	50.08	47.05	44.06
	Cr	58.85	55.88	52.88	49.86	46.91	43.88

Figures 6, 7, 8, 9, 10,11 show the difference between the using of the two-channel Cb and Cr on all the seven images used in this experiment by embedding rate 1KB, 2KB, 4KB, 8KB 16KB and 32KB respectively. Figure 12 summarizes the results from the abovementioned figures.

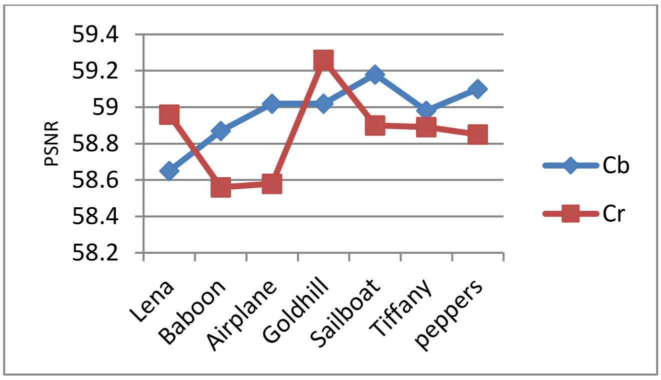


Figure 6: Imperceptibility using embedding rate 1KB

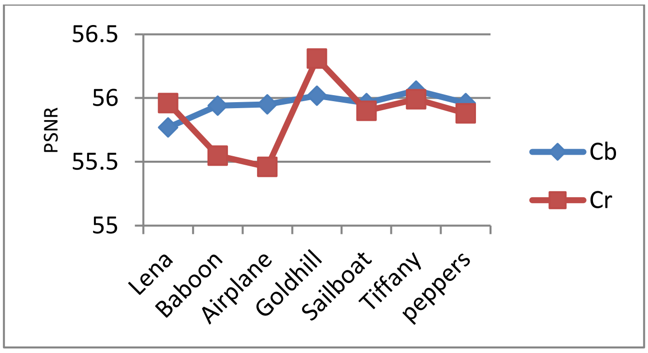


Figure 7: Imperceptibility using embedding rate 2KB

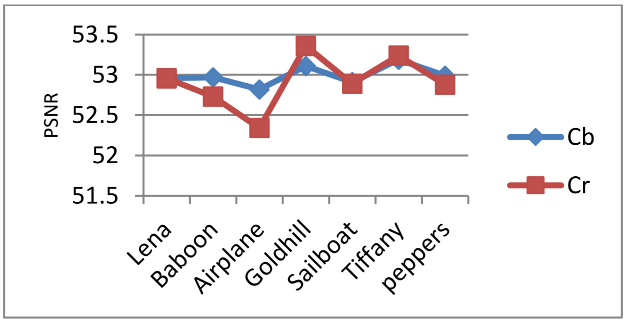


Figure 8: Imperceptibility using embedding rate 4KB

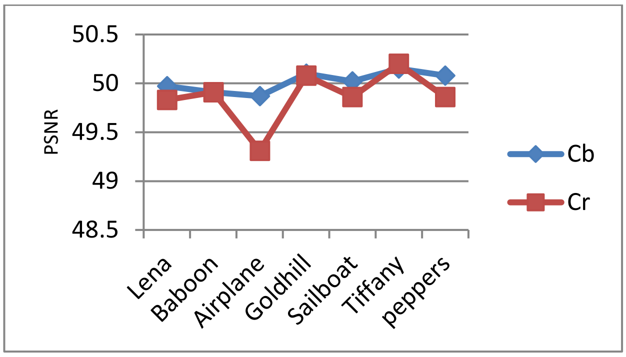


Figure 9: Imperceptibility using embedding rate 8KB

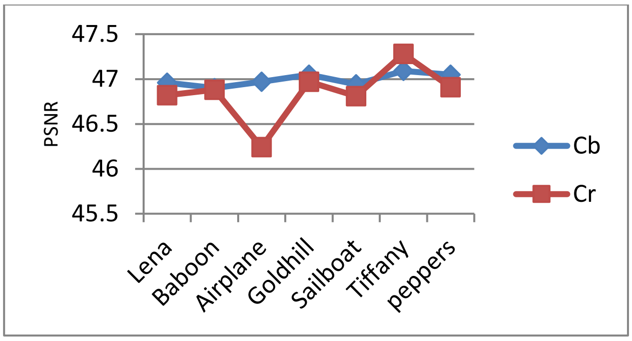


Figure 10: Imperceptibility using embedding rate 16KB

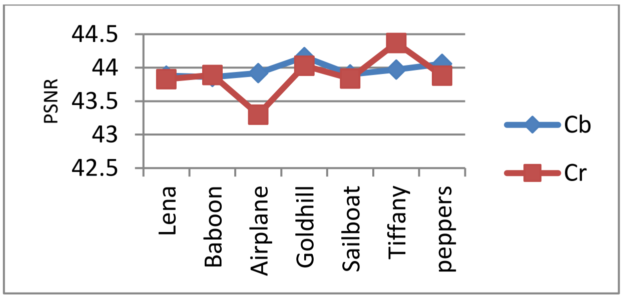


Figure 11: Imperceptibility using embedding rate 2KB

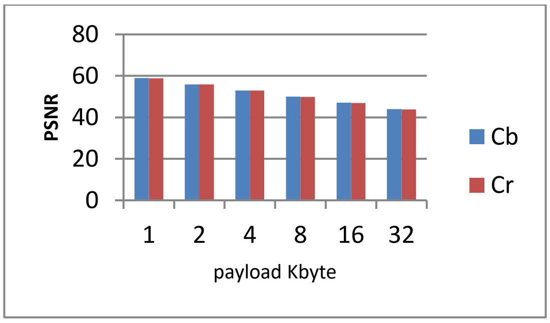


Figure 12: Imperceptibility with different payload sizes.

B. Salt-and-Pepper Measure for Robustness

The ever-useful Lena image is chosen in to evaluate the robustness of the proposed technique when stego-image is attacked. Table 2 shows the accuracy of the correct extracted character each time obtained after applying the salt and pepper attack on the stego image, for both Cb and Cr we apply 3 types of salt and pepper attack with different value 0.1, 0.2 and 0.3.

Table 2
The Accuracy of the Extracted Correct Character Each Time After Applies A Different Attack

Data	Cb			Cr		
size (KB)	0.1	0.2	0.3	0.1	0.2	0.3
1	98.24%	93.36%	90.04%	99.12%	94.63%	88.57%
2	99.07%	93.21%	89.01%	99.27%	93.75%	89.21%
4	98.85%	94.36%	89.11%	98.95%	97.75%	88.01%
8	98.93%	84.30%	89.18%	98.50%	93.90%	88.56%
16	98.75%	94.26%	89.20%	98.46%	94.20%	89.07%
32	98.80%	94.35%	88.78%	98.14%	93.60%	88.50%

The secret message that is embedded inside the stego-image is different, and the size of the groups is equal. The results show that the behavior of the salt and pepper attack is almost similar for both case Cb and Cr channel. This result confirms that the proposed method can achieve the aims of the steganography, where high embedding rate is produced with high robustness.

C. Comparison with Other Studies

For a validation test between the proposed technique and various well-known methods namely, DWT, the same size of the payload are used. The minimum value for PSNR should not be less than 30 for perceptual fidelity [7].

Table 3
Performance of the Proposed Method Against DWT

Method	Lena	Airplane	Tiffany	Baboon	Average
Proposed method	49.97db	49.87db	50.15db	49.91db	49.97db
DWT	46.08db	45.99db	46.13db	46.19db	46.09db

As shown in Table 3, the experimental results are using four images from the dataset namely Lena, Airplane, Tiffany and Baboon; the data used for testing was same for both method wish is 8 KB. The difference in PSNR is quite significant between the proposed method and the DWT method which is around 3 dB. As a result, the proposed method is capable of embedding a larger amount of secret messages without sacrificing image quality.

VI. Conclusion

This work proposes a new steganography technique using an affine cipher to encode the data payload and using an improved YCbCr method to hide these data. Color images were chosen to test the performance of this technique. In conclusion, the proposed method fulfills the requirements of steganography which are imperceptibility, payload, and robustness.

Acknowledgment

This work has been sponsored by the Faculty of Electrical Engineering, Universiti Teknologi Malaysia and the Malaysian Ministry of Higher Education under the Fundamental Research Grant Scheme (Vot No. 4F659).

References

[1] Neha Batra and Pooja Kaushik (2012). *Implementation of Modified 16×16 Quantization Table Steganography on Color Images*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[2] Ravi Saini (2014). *Review of Different Techniques of Image Steganography* International Journal of Computer Applications and Information Technology, Vol. 5, Issue I, Feb-March 2014.

[3] Chan, C. K. and Cheng, L. M. (2004). *Hiding Data in Images by Simple LSB Substitution,* Pattern Recognition, Vol 37, No 3. pp. 469-474.

[4] Nedeljko Cvejic and Tapio Seppänen, *Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method*, Proceedings of the International Conference on Information Technology: Coding and Computing IEEE(2004).

[5] Ramkumar, M. and Akansu, A. N. (2001). *Capacity Estimates for Data Hiding in Compressed Images*. Image Processing, IEEE Transactions on, Vol. 10, Issue 8, pp. 1252- 1263.

[6] Tariq Al, H., Mahmoud Al, Q. and Hassan, B. (2003). *A Test Bed for Evaluating Security and Robustness of Steganography Techniques*. In: Circuits and Systems, 2003 IEEE 46th Midwest Symposium on, 27-30 Dec. 2003. 1583-1586 Vol. 3.

[7] Chang-Chu Chen and Chin-Chen Chang (2007). *Secret Image Sharing Using Quadratic Residues, Intelligent Information Hiding and Multimedia Signal Processing,* IIHMSP 2007. Third International Conference on. 515 – 518.