Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A ROBUST STEGANOGRAPHY APPROACH WITH HIGH EMBEDDING CAPACITY USING UNIQUE VALUE EMBEDDING AND CODEBOOK

[1]SARDJOENI MOEDJIONO, [1]ACHMAD RIFAI, [1,2]TEDDY MANTORO
[1]Budi Luhur University, Computer Science Post Graduate Program, Jakarta
[2]Universitas Siswa Bangsa Internasional, Faculty of Science and Technology, Jakarta
E-mail: moedjiono@ budiluhur.ac.id, 1211600026@student.budiluhur.ac.id, teddy.mantoro@usbi.ac.id

ABSTRACT

Steganography is the art of hiding data and an effort to conceal the existence of the embedded information. There are a lot of data to be embedded such as text, image, audio, and video. An information hiding system is characterized by having three different aspects that contend with each other. These are capacity, security, and robustness. In steganography area, the common method used to hide a secret data is LSB (Least Significant Bit). LSB provides the high embedding capacity, however, when the secret data is larger than cover data, the cover data would be dramatically distorted. The distorted cover data can attract the attacker to perform steganalysis method. This study is carried out to overcome the embedding capacity problem without producing a significant distortion in cover data. The experiment is tested by hiding audio signals in image file. The idea is to convert the audio signals into native data representation (unsigned integer 8) and to find its unique values. The image will be modeled its codebook in order to obtain a great embedded image quality using LBG (Linde Buzo Gray) algorithm. The result shows a high PSNR (Peak Signal to Noise Ratio) for extracted audio file and low RMSE (Root Mean Square Error) for image file.

Keywords: *Audio signals, Steganography, LBG, LSB, Codebook, Embedding capacity.*

1. INTRODUCTION

Steganography is the art of hiding data and an effort to conceal the existence of the embedded information [1]. There are a lot of data to be embedded such as text, image, audio, and video. An information hiding system is characterized by having three different aspects that contend with each other these are capacity, security, and robustness [2, 3]. In steganography area, the common method used to hide a secret data is LSB (Least Significant Bit) [4]. LSB provides the high embedding capacity, however, when the secret data is larger than cover data, the cover data would be dramatically distorted. The distorted cover data can attract the attacker to perform steganalysis method [5]. LSB coding permits for a huge amount of data to be encoded by replacing the least significant bit (LSB) of each sampling point with a binary information [6]. The embedding capacity of standard LSB method is calculated using

$$\text{Capacity} = (W * H)/8 \quad (1)$$

$$\text{Capacity} = (W * H * 3)/8 \quad (2)$$

Where W is the image width and H is the image height [7]. Suppose there is a grayscale image with W = 200 and H = 150. Therefore, the embedding capacity is 3750 bits. If the image is RGB, the embedding capacity would be 11250 bits . If there is an audio signals with three seconds duration, the data of audio signals would be N, where N > 100000 data and the bits to be embedded would be

$$\text{Embedded Bits} = N * 8 \quad (3)$$

This study is carried out to overcome the embedding capacity problem without producing a high distortion in cover data. The idea is to equalize a range of value of audio signals identically to image file (0 to 255), which is done by converting the audio file to native format (unsigned integer 8). The maximum embedding capacity is calculated using Eq (3). In standard LSB method, if the capacity exceeds the cover image size, the data hiding process cannot be done. To overcome this problem, the unique value from audio signals is taken. Let X be the audio signal with 332506 x 1 size and I be the grayscale image cover with 200 x 150 size. Since the range of value for audio signals

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is 0 to 255, the possibility of unique value is 255, using Eq (3) the image cover should not be less than 2040 bits. In this way, the maximum capacity problem can be solved. The other contribution is to overcome the steganalysis attack. Theare are several methods for detecting standard LSB such as chisquare attack, RQP (Raw quick pair), and RS Steganalysis [8]. The chisquare attack identifies Pairs of Values (POVs) which consist of pixel values, quantized DCT coefficients or palette indices that get mapped to one another on LSB flipping. After message embedding, the total number of occurrence of two members of certain POV remains same. Statistical chisquare test could be used for detecting the hidden messages [9, 10]. The RQP method is based on analyzing close pairs of colours created by LSB embedding. It has been shown that the ratio of close colours to the total number of unique colours increases significantly when a message of a selected length is embedded in a cover image rather than in a stego image. RS steganalysis also could be used for detecting LSB embedding in colour and grayscale image. Theoretical analysis and experimentation show that the proportion of regular and singular groups form curves quadratic in the amount of message embedded by the LSB method. RS steganalysis is more reliable than chisquare method [10].

Those of steganalysis methods are intended to detect the hidden message in cover image. Therefore, the method will be successful if the message can be read from a cover image. Unfortunately, the steganalysis methods may only have a unique audio values, without the indeces, the audio signals could not be reconstructed perfectly. To solve the secret key, the permutation could be used, but it will produce a lot of solutions. The permutation could be used using

$$N! / (N - (\max (X))! \quad (4)$$

Where N is total of unique value, X is maximum unique values. The maximum unique values is used as the upper bound of solution possibility. Suppose the total of unique value is 119 and the maximum of unique value is 255, using Eq (4), the trials should be 119! / (119 – 255)!. It produces a lot of solution possibilities.

The experiment is tested with hiding audio signals to image file in order to show that the larger secret data bits (audio signals) can be hidden in the lower cover data bits (image file) with efficient embedding bits.

This study contribues in conveying a new technique for hiding audio file in image file with considering the security and efficiency. This work is divided into two phases, the first is encoding phase and the second is decoding phase. In encoding phase, the generated indeces will be stored in one matrix as a key, the indeces are used for audio file construction (Section 3) the result shows a great PSNR (Peak Signal to Noise Ratio) for extracted audio file and RSME (Root Mean Square Error) for image file (Section 4).

2. RELATED WORK

There are a lot of researches to improve embedding capacity. Genetic algorithm (GA) has been proposed to increase embedding capacity. The proposed steganography scheme embeds message in integer wavelet transform coefficients by using a mapping function. This mapping function based on GA in an 8x8 block on the input cover color image. After embedding the message optimal pixel adjustment process is applied. By applying the OPAP the error difference between the cover image and stego image is minimized. Frequency domain technique is used to increase the robustness of proposed method. GA is used to increase the hiding capacity of image and maintains the quality of image [11].

The modified LSB has been proposed to increase robustness of audio steganography by reduced distortion LSB coding [12]. The audio signals is used to cover data which can provide the large embedding capacity. The vector quantization based is proposed to increase the embedding capacity. It used a codebook with a dictionary sort to embed a secret data [13]. The permuted address vector (PAV) is proposed to increase the embedding capacity with improving the embedding security [14]. The similarity based in image steganography is proposed to overcome the degradated image quality after embedding process. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels [15]. The modified optimum pixel adjusment (OPA) algorithm and haar wavelet transform is proposed to overcome the embedding capacity in image steganography [16]. The most inspiring of this work is the index based steganography using two images which has been proposed by [17]. They used the data image as for embedding a secret image, then the data image and stego image will send to receiver.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

There are a lot of researches about embedding capacity problem in LSB method. It means that this problem is important to be considered. Because it can affect the cover data quality when the imbalance embedding distortion occurs. This study is carried out to create a robust steganography technique with high embedding capacity without producing a significant distortion in cover data. This study also used an LSB method as the embedding technique because of its simplicity.

3. PROPOSED METHOD

The basic idea of this work is to adopt the index base steganography which has been proposed by [13], [14], and [17]. The differences with this work are in the reduction of the embedded bits in order to decrease the embedded quota and using the unique value in order to prevent the steganalysis methods attack. This work is divided into two phases, the first is encoding phase and the second is decoding phase.

3.1 Encoding Phase

The audio signals is chosen and the cover image as well. The image will be reshaped into N x 2 size [13]. The reshaped image will be modeled its codebook using LBG method. The steps of LBG method are as follows:

Step - 1: Choose a random value from training data to be an initial value.
Step - 2: Set k = 0.
Step - 3: Set Threshold = α.
Step - 4: Perform this following process for each training input.
Step - 5: Compute the euclidean distance between training data and initial value (CB_k) using

$$d(x_j, \hat{x}_i) = \frac{1}{k}\sum_{m=1}^{k}[x_j(m) - \hat{x}_i(m)]^2 \quad (4)$$

Step - 6: Search the nearest codeword among CB_k
Step - 7: Compute the centroid of each cell to obtain the new codebook CB_{k+1},
Step - 8: Compute the average distortion for CB_{k+1} using

$$D_{m+1} = D[(Ym, P(Ym))] = \frac{1}{n}\sum_{j=1}^{n}\min_{\hat{x}\in Ym} d(x_j, \hat{x}_i) \quad (5)$$

Step - 9: If the distortion > α, go to step 4 and set k = k +1, otherwise stop the algorithm.

At this point, the codebook and indeces are obtained from image file, this codebook will be matched its values to the audio file and the indeces will be used for reconstructing image from codebook. This algorithm may take a long time to converge, it depends on the image quality and the chosen inital value. This codebook will be used for encoding phase, the index of pixel value which is used for enbedding bits will be stored in one matrix.

In audio signals preparation, the audio signals will be read as an unsigned integer 8 native format (0 to 255) in order to obtain the same range value with image file. The audio data will be taken its unique data, because the embedding process does not need a duplicate data. In Eq (3), total unique data is multiplied by eight in order to get the required capacity in image file. The next process is embedding every data bit in audio data to the last image bit. At this point, for one audio data value will need eight image data values, therefore, the last bit for every eight values is changed and it containts the audio data information. To track the data information for reconstruction purpose, the indeces embedded data in image file is stored. At this stage, the output from those processes are image codebook along with the indeces and embedded image codebook along with the indeces. The embedded image codebook will be sent to receiver. The steps of embedding process are:

Step - 1: Get the unique values of audio signals.
Step - 2: Choose the pixel of image file sequentially.
Step - 3: Embed the first bit of audio signals value to the chosen pixel.
Step - 4: Store the index of pixel
Step - 5: If the bit is not depleted, go to Step 2, otherwise go to Step 6.
Step - 6: If the audio signals values are not depleted, go to Step 3, otherwise stop the algorithm.

The unique values of audio signals have been embedded to the sequence of pixel in codebook. This codebook is called stego codebook. The stego codebook will be reconstructed to the stego image using indeces which is obtained from LBG method. From this process, the stego image and stego indeces will be obtained. In order to be able to construct audio signals from stego image, the embedded indeces should be mapped. The process of embedded bits mapping are as follows:

Step – 1: Iterate every stego image.
Step – 2: Iterate every stego codebook.

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step – 3: Set i = 1
Step – 4: Find the intersection value of stego image and codebook.
Step – 5: Set i = i + 1
Step – 6: Stored the index of intersection value
Step – 7: If i < 8 go to Step 4, otherwise stop the algorithm.

The stego image, stego indeces, and embedded indeces will be obtained and ready to send to receiver. Figure 1 shows the Venn diagram of embedded bits mapping process and Figure 2 shows the illustration of required files to be sent to receiver.

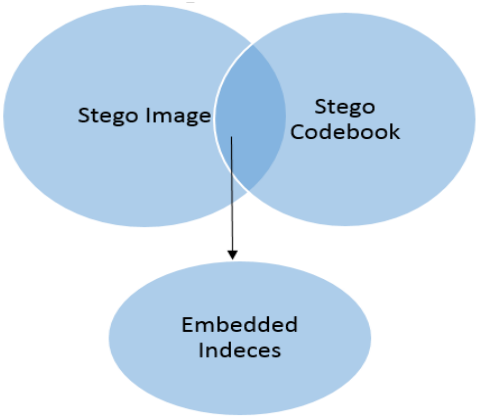

Figure 1: Venn Diagram of Embedded Bits Mapping

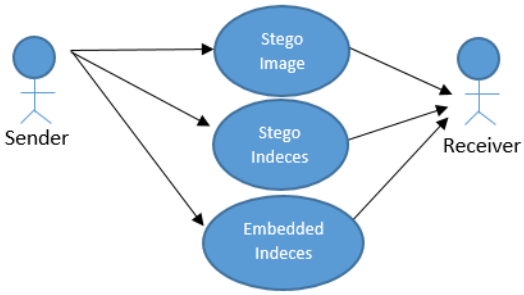

Figure 2: The Illustration of Key Sending to Receiver

In this process, only the unique values are embedded in cover data. It means, the maximum bits to be embedded is only 0 to 255. With those values, the cover data would not be too distorted.

3.2 Decoding Phase

In this phase, the stego image, original codebook indeces, and the stego indeces is received. The stego codebook is constructed using original codebook indeces. Since the stego codebook is constructed, the audio signals can be constructed perfectly using stego indeces. The stego indeces will find the embedded bits in the image pixel, with obeying the rules in Section 1, for one bit of audio signals will be embedded in 8 pixels image sequentially. The output of this process is a unique value of audio signals data. The next process is to construct the audio signals given the unique value and stego indeces. The decoding process has been done without raising the suspicions of the others. Since the bits is embedded to the only one pixels (in pixel's LSB), the image would be not dramatically distorted. The steps of decoding phase are as follows:

Step – 1: From stego image, find the unique values of audio signals.
Step – 2: From the obtained unique values, order the unique values using embedded indeces.

The ordered unique values is called extracted audio signals. Figure 3 shows the illustration of decoding phase.

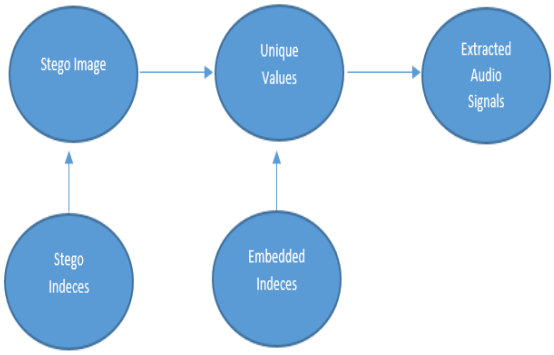

Figure 3: Illustration of Decoding Phase

3.3 Possibility of Constructing the Audio Signals

The steganalysis methods may be able to get the unique values from cover image, but they could not reconstruct the unique values perfectly without the embedded indeces. As mentioned earlier, to solve the embedded indeces, the permutation could be used, but it will produce a lot of solutions. The permutation could be used using

$$N! / (N - (\max(X))! \quad (6)$$

Where N is total of audio signals data, X is maximum unique values. The maximum unique

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

values is used as the upper bound of solution possibility. Suppose the total of unique value is 12100 and the maximum of unique value is 255, using Eq (4), the trials should be 12100! / (12100 – 255)!. It produces a lot of solution possibilities. In this way, the steganalysis methods will not be able to detect the constructed audio signals, it means the secret data is secure.

4. EXPERIMENTAL RESULT

The experiment is tested by hiding audio signals in image file to proof that the smaller cover data can be used to hide the larger secret data. This experiment used two wav files as secret data (1330166 x 2 size and 270629 x 1 size) and four image files (two RGB image and two grayscale image) with 256 x 256 size as cover data. The best result is obtained when the RMSE (Root mean square error) is low and PSNR (Peek signal to noise ratio) is high [18]. The RMSE and PSNR are calculated using

$$RMSE = \sqrt{\frac{1}{PQ}\sum_{m=0}^{P-1}\sum_{n=0}^{Q-1}[G(m,n) - R(m,n)]} \quad (7)$$

$$\text{PSNR} = 10\log_{10}\left(\frac{MAXi^2}{MSE}\right) \quad (8)$$

In Eq (7), the G and R is the original image and stego image, the differences between two pixels is calculated. In Eq (8), the MSE is the Eq (7) without root for two audio files (before embedding and after extracted). Max_i is the maximum possible value for every pixel or audio data. Table 1 shows the required capacity for 2 wav files.

Table 1: Required capacity for 2 wav files

Audio Files	Unique Value	Required Capacity
Secret1.wav	112 bits	896 bits
Secret2.wav	119 bits	952 bits

Total unique data for Secret1.wav is 112 bits and using Eq (3), the total required capacity is 896 bits and total unique data for Secret2.wav is 199 bits and the total required capacity is 952 bits. Figure 4 and Figure 5 show the original signals of the both audio files.

The first experiment used RGB image is called "rubik.jpg"

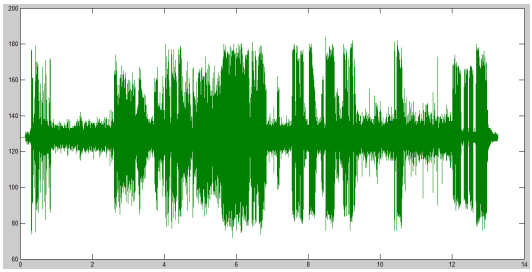

Figure 4: Original Audio Signal of Secret1.wav

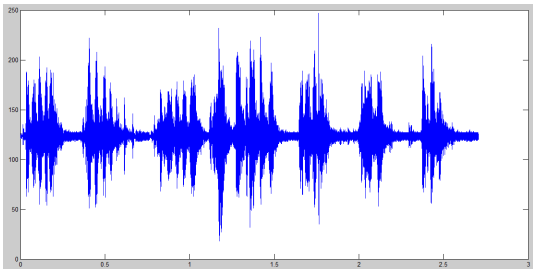

Figure 5: Original Audio Signal of Secret2.wav

Figure 6 shows the original cover image of rubik.jpg in RGB form and Figure 7 shows the original cover image of rubik.jpg in grayscale form, Figure 8 shows the original cover image of caric.png in RGB form and Figure 9 shows the original cover image of caric.png in grayscale form.

Figure 6: Original RGB Form in rubik.jpg

Figure 7: Original Grayscale Form in rubik.jpg

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The codebook size used in this experiment is 1024. Those sizes are chosen because the required capacity > 500 bits. Those images will be embedded the audio signals (Secret1.wav and Secret2.wav). The first experiment is hiding Secret1.wav to RGB rubik.jpg using 1028 codebook. Figure 9 shows the stego image for RGB rubik.jpg.

Figure 9: Stego RGB Form in rubik.jpg

In plain view, the distortion of stego image is not really visible. It means, the secret data has been successfully embedded. The second experiment is hiding Secret1.wav to grayscale rubik.jpg. Figure 10 shows the stego image for grayscale rubik.jpg and Figure 11 show the stego image for grayscale caric.png.

Figure 10: Stego Grayscale Form For rubik.jpg

Figure 11: Stego Grayscale Form For caric.png

In plain view, the distortion of stego image is not really visible. It means, the secret data has been successfully embedded. After embedding process, the stego image will be transformed to codebook stego by using stego indeces in order to obtain the unique values and the unique values will be orderd using embedded indeces. and Figure 12 shows the extracted audio files signals from RGB stego image and Table 2 shows the whole stego image RMSE results in RGB image.

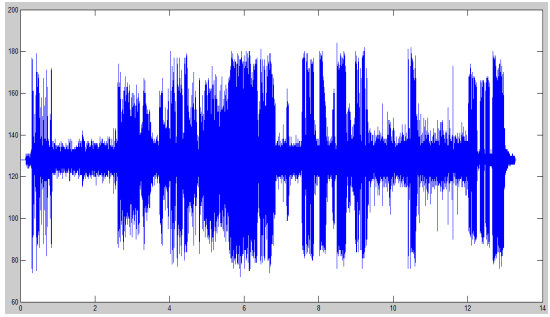

Figure 12: Extracted Audio Signals Secret1.wav

Table 2 shows the whole RMSE results using RGB image.

Table 2: Stego Image RMSE Results In RGB Cover Images.

Secret	Cover	R	G	B
Secret1	rubik.jpg	1.1033	0.9460	0.956
Secret1	caric.png	1.2432	1.4923	1.231
Secret2	rubik.jpg	1.5033	1.3460	1.756
Secret2	caric.png	1.3412	1.1211	1.942

Table 2: Stego Image RMSE Results In Grayscale Cover Images.

Secret	Cover	RMSE
Secret1	rubik.jpg	1,70889282226563
Secret1	caric.jpg	1,87401504077392
Secret2	rubik.jpg	1,94302940475839
Secret2	caric.png	2,48458578934893

The result shows, the lowest RMSE is obtained when using RGB image with for every component of R, G, and B in the range of 0 to 1. Table 4 shows the PSNR result from extracted audio signals in grayscale images

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: PSNR Extracted Audio Signals From RGB Cover Images.

Secret	Cover	PSNR
Secret1	rubik.jpg	144.2
Secret1	caric.jpg	101.5
Secret2	rubik.jpg	120.4
Secret2	caric.png	112.3

Table 4: PSNR Extracted Audio Signals From Grayscale Cover Images.

Secret	Cover	PSNR
Secret1	rubik.jpg	201.2
Secret1	caric.jpg	151.5
Secret2	rubik.jpg	160.4
Secret2	caric.png	132.3

The result shows, the great psnr is obtained when using grayscale image. The RGB image produces the lower RMSE for cover image and produces the lower PSNR for extracted audio signals.On the other hand, the grayscale image produces the higher RMSE for cover image and produces the higher PSNR for extracted audio signals. Figure 13 shows the extracted secret messages without embedded indeces and Figure 13 shows the extracted secret messages with embedded indeces.

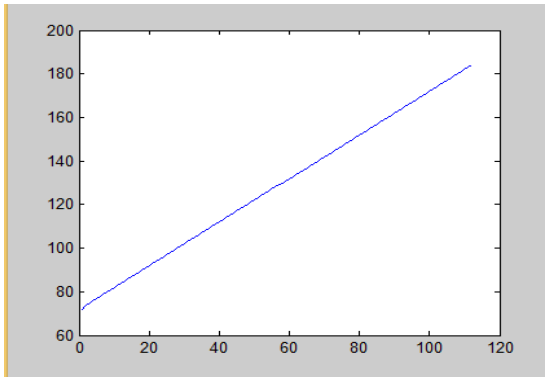

Figure 13: Extracted Secret Data Without Embedded Indeces

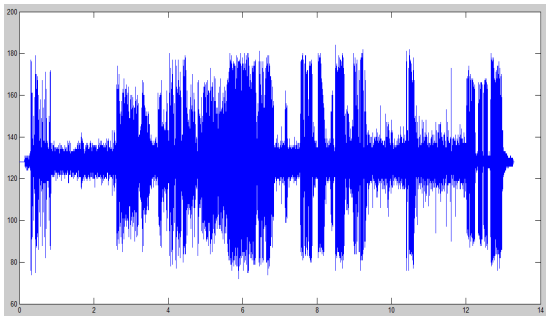

Figure 14: Extracted Secret Data With Embedded Indeces

Figure 13 shows the possibility of steganalysis methods to detect a secret key, but they will not be able to construct the audio signals perfectly as Figure 14. The steganalysis methods need to detect the stego key in using Eq (4) which will produce a lot of solution probabilities. It means, the proposed method can hide the secret data securely.

5. CONCLUSION

This study proved that the maximum embedding capacity problem can be solved using unique values data embedding. Since the data to be embedded is not overlaping, the total amount of data to be embbeded is reducing. The codebook can be used as an embedding media for audio files without producing the large distortion in image. The proposed method can be applied in two types of images RGB and grayscale perfectly. The embedding process only needs unique values of audio file and needs at most 2040 codebook size. It means, the maximum codebook size is only 2040 since the maximum range of native (unsigned integer 8) is 255. The most important thing in this method is indeces to be sent to receiver. The audio signals could be constructed by those indeces. The proposed method shows that the steganalysis method cannot reconstruct the audio signals perfectly without stego indeces. Eq (4) takes important role since the stego indeces could be retrieved usingy this equation. The proposed method also provides the robust method with 2 types of indeces, which are stego indeces and embedded indeces. The stego indeces is used to obtain the unique value in stego image. The embedded indeces is used to order the unique values to audio signals. As the steganalysis method could obtain the secret data in unique values by embedding indeces, it can reconstruct the audio signals similar from with the source from stego image.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. FUTURE WORK

This study used LBG method for modeling codebook, as we knew before, the LBG suffers local optimum. The LSB technique is used in this experiment in embedding process. The embedding process could be changed with another method such as subtitutions, phase coding, and genetic algorithm. The limitation of this method is in chosing the proper cover data. If the cover data is less than the required codebook size then the cover data could not be used. In the future work, the aritmethic method could be used to reduce the unique value, therefore, the embedding capacity would be higher than before. In the future work, the stego image should be able to construct the stego codebook in order to overcome compression attack. It means that there will be additional indeces to be sent to receiver in order to construct the stego codebook.

REFRENCES:

[1] A. Kumar, K.M. Pooja, "*Steganography A Data Hiding Technique*", *International Journal of Computer Applications*, Vol. 9, No. 7, 2010.

[2] B.A Usha, N.K Srinath, N.K. Cauvery, A. Nanjangud, A.M. Deshpande, and A. Rebello, "*A Survey on Secure and High Capacity Image Steganography Techniques*", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue. 3, 2014.

[3] A. A. Al-Ataby, and F.M. Al-Naima, "*High Capacity Image Steganography Based on Curvelet Transform*", *Developments in E-systems Engineering (DeSE)*, 2011.

[4] A. Daneshkhah "*A More Secure Steganography Method in Spatial Domain*" *in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*, 2011, pp. 189-194.

[5] K. Kiruba, S. Karthikeyan, and J.J. Priya, "*Reliable Detection Of Adaptive Pixel Pair Matching In Color And Grayscale Images*", *International Journal of Innovative Research and Studies*, Vol. 2, Issue. 7, 2013, pp. 203-213.

[6] K.U. Singh, "*LSB Audio Steganography Approach*", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 4, Issue. 4, 2014.

[7] M. Bashardoost, G.B Sulong, and P. Gerami, "*Enhanced LSB Image Steganography Method by Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression*", *International Journal of Computer Science Issues (IJCSI)*, Vol. 4, Issue. 2, No. 1, 2013.

[8] R. Chhikara and L. Singh, "*A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted*", *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 3, Issue. 4, No. 1, 2013, pp. 203-213.

[9] A. Westfeld, A. Pfitzmann, "*Attacks on steganographic systems", In: Proc. of Information Hiding*", Third Int. Workshop, *Dresden, Germany*, 1999, pp. 61–75.

[10] J. Fridrich, M. Goljan, "*Practical steganalysis of digital images-state of the art", In: Proc. SPIE Photonics West*", *Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, vol. 4675, 2002, pp. 1–13.

[11] A. Tripathy, D. Kumar, "*Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security*", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, Issue. 4, 2014, pp. 403-408.

[12] C. Parthasarathy, S.K. Srivatsa, "*Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding*", *Journal of Theoretical and Applied Information Technology,* Vol. 1, Issue. 1, 2009, pp: 080-086.

[13] H.B Kekre, A. Athawale, T. Sarode, S. Thepade, K. Sagvekar, "*Steganography Using Dictionary Sort on Vector Quantized Codebook*", *International Journal of Computer Science and Security (IJCSS),* Vol. 2, Issue. 4, 2010.

[14] A.A. AbdelWahab, "*A New Image Steganography Technique*", *Journal of Engineering and Computer Sciences,* Vol. 1, No. 2, 2008, pp. 109-117.

[15] A.A. Judice, P.S. Dhivya, J.D.S. Divya, A.H.S. Lekshmi, "*An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform*", *International Journal of Computer Science and Network Security,* Vol. 14, No. 3, 2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] A.A. Judice, P.S. Dhivya, J.D.S. Divya, A.H.S. Lekshmi, "*An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform*", *International Journal of Computer Science and Network Security,* Vol. 14, No. 3, 2014.

[17] P.B.U. Ivy, P.J. Kumar, S. Sureka, and G.U Maheswari, "*Index Based Steganography: A New Secure Approach For Image Steganography Using Two Images*", *Journal of Theoritical and Applied Information Technology*, Vol. 53, No. 2, 2013.

[18] H. Kuhad, A. Joshi, A. Gurpude, N. Chimankar, R. Maskey, and R. Thakur, "*Image Denoising By Hybrid Average Gaussian Filter For Different Noises*", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Issue. 34, 2013.