Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

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

HIGH LEVEL SECURITY BASED STEGANORAPHY IN IMAGE AND AUDIO FILES

[1] M.SHADY AL-RAHAL, [2] ADNAN ABI SEN, [3] ABDULLAH AHMAD BASUHIL

[1]PHD student., Department of Computer Science, College of Computing and Information Technology, kau

[2]PHD student., Department of Computer Science, College of Computing and Information Technology, kau

[3]Assoc Prof., Department of Computer Science, College of Computing and Information Technology, kau

E-mail: [1] shady.rahal1986@gmail.com, [2] adnanmnm@hotmail.com, [3] abasuhail@kau.edu.sa

ABSTRACT

As the use of the Internet for information exchange has spread widely, there is an increase in the skills of attackers. Nowadays, it has become very important of ensuring the protection of a transmitted information, assuring its safe delivery to the receiver side and overcoming risks of any future attack. Steganography is one of the most important approaches for hiding secret information and send it safely to the intended side without drawing attention about its existence. In this paper, we present a general model to protect confidential information by hiding it within other innocent information (image or audio file) that suits different types of data (text, image, or audio). Our information hiding model is based on using the least significant bit technique, so that an attacker will have no clue about the existence of any secret message. In advance to hiding a secret information, this information will be passed through encryption and randomizing stages to strengthen it against possible attacks. The experimental results of our proposed approach showed high level of security and transparency compared with the previous proposed approaches.

Keywords: *Cover_Object, Hidden_Data (Secret Message) , Stego_Key, Stego_Object, LSB, Attacker.*

1. INTRODUCTION

Steganography is the science that deals with communication in a manner of complete silence so that secret message will not be discovered [1, 2]. Moreover, the process of hiding a secret message within other medium is logically possible in digital world because of the symmetric nature of data storage in computers, as they can interpret 0s and 1s language. Furthermore, compared to cryptography, steganography has superior advantages. This is because the final aim of cryptography is to make a secret message be unreadable, on the other hand, steganography aims to hide the communication itself among the users.

Previously, there are many steganography techniques based on the used cover. These methods can be classified into three major classes: text-based cover [3, 4, 5], that encodes a secret message by generating a text file that contains the secret message, taking first letter of every word in the text. The secret message can be extracted. However, the major challenge here is to generate innocent text cover so that its meaning will not change after hiding the secret message. The second class is image-based cover [6, 7, 8]. It encodes secret message by changing some statistical properties of the cover and use testing hypothesis to extract the message; e.g. use of Discrete Cosine Transform (DCT). Finally, audio-based cover [9, 10, 11, 12], where a secret message is encoded within the confused part of the signal, we can measure the value of the deviation from the original signal to extract secret message, for an example the distortion of digital audio.

However, all the previous mentioned approaches are suffering from a main problem which is related to the attacker himself in the case of being expert or very skeptical. Using LBS (least significant bit) is considered as one of the most powerful ways to achieve good tradeoff between the distortion caused by hiding and the invisibility, since the impact of hiding in LSB has the lowest level of distortion in comparison to hiding within MSB (most significant bit). In addition, LSB-based approach could be applied in both audio and image covers. Although this method is strong, it could be broken by an expert attacker for some reasons. First of all, hiding based on LSB without making sure that the stego-key is distributed between only the communication parties involved in the system in a safe way may put the whole process under a unsafe situation in the case of revealing this stego-key by an attacker. Second, hiding in LSB in the same flow (i.e., in sequence way) makes it vulnerable to break, since it is very simple to use the LSB and then extract the secret message. Finally, although using cryptography to support the technique, this also could be broken by applying advanced cryptographic analysis.

In this paper, we proposed a new model for hiding in both audio and image files based on LSB method where an optimization is done so that it will be invulnerable against attacks. To distinguish our approach from the previous works, after encryption we used special randomization method based on several steps (ZigZag, jumps, different layers, start shifting, and special coding scheme rather than ASCII).

2. Related Work

Steganography approaches could be classified based on various criteria. For example, [13] provided classification for methods of steganography depending on the used technique focusing on steganalysis. Steganalysis was divided into two categories statistical and signature. Each one is branched into specific and universal. However, steganography could be classified depending on the cover type that contains the secret message intended to be hidden. According to this, we presented various proposed approaches that used either text, image, or audio file as a cover.

First group, using text file as cover (i.e., the secret information will be embedded within a text file). A method to hide a secret message into a text file written with Hindi text where it depends on Hindi letters and its diacritics and numerical code to hide the secret message is provided in [3]. The authors mentioned strong point in their work which is that their proposed approach could be applied to similar Indian languages. Similarly, [4] provided an approach to embed a secret information within Arabic and Persian text file depending on several intersections between these two languages. It used vertical displacements of points to insert and hide the secret message. In their proposed work researchers presented a scheme based on cryptography using SSCE, where the secret key will be directly exchanged between the sender and receiver for both hiding and extracting a secret message[14]. Other researchers have elected certain letters from certain words as hiding place for secret message [15]. In the simplest form, for example, the first words of each sentence are elected in a manner that places the first letters of these words side by side. Similarly [16] followed the same key idea, but it used the null space and it is applied on American daily traditional speech.

Second group, using image file as a cover (i.e., the secret information will be hidden within an image file). Targeting capacity of embedded data, [6] depended on LSB where a mixture between ideas of random pixels processing and stegokey was done. It used pixel indicator technique for randomizing. The researchers in [7] only used one level of security to protect the embedded message where encryption was done before hiding within LSB based on ISC algorithm. It proved the effectiveness not to decryption theoretically. An approach that used image file as a cover is presented in [8], where it used the DCT transformation to hide the secret information in the high frequency coefficients avoiding dealing with low frequency to keep the quality of resultant image after hiding. The work in [17] used both edge detection and LSB method to hide a text file within an image. Moreover, the work in [18] provided an optimization for LSB method that targeted the level of distortion caused by hiding processing regardless of any additional security level.

Third group, using audio file as a cover (i.e., the secret information will be hidden within an audio file). A group of researchers in [9] provided a double approach where a level of encryption for hiding data is created based on ASCII coding before inserting the secret message in the audio file. Although [10] achieved steganography depending on LSB, its final objective was to test that this method is weak under revealed confidential embedded information term and it needs to be supported enough, and this is considered as drawback. It mentioned that its advantage is that it is simple to implement. The researchers in [11] took into consideration adding a level of security depending on encryption using modified Vigeneve cipher algorithm, but the difference was that it focused on hiding only text file within the audio file. In addition to this, it benefited from the Blum technique to transposition the audio file after embedding the secret information to make the attacker to be confused. The research in [12] depended on converting the audio file using DCT transformation as a first step. The second step was using Huffman encryption to be applied on the secret message. After that, embedding will be done. The extraction phase will be achieved using the inverse transformation. It should be mentioned that [19] decided the requirements of hiding in an audio file where the cover must hold different types of the secret data using password.

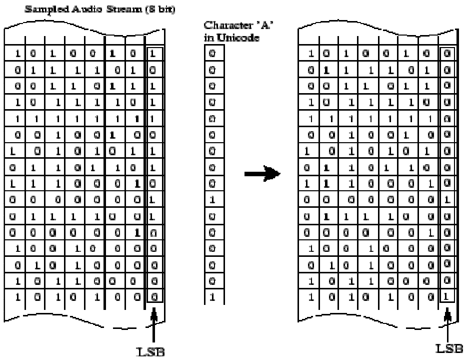
3. THE PROPOSED HIDING MODEL

Our proposed model uses mainly cover of type image or audio file to hide (text, image, or audio). To hide information, we need two files: Cover_Object file and second file is Hidden_Data that includes the secret information to be protected. After combination, a new file called Stego_Object will be generated. Thus, the parts of steganography could be expressed as follows:

Cover_Object + Hidden_Data = Stego_Object (1)

Our proposed model is based on substitution system. This system hides secret message by substituting parts of the cover that never harm it like least significant bit to achieve invisibility of changes caused by hiding the secret information. In other words, take advantages of the low sensitivity of human eye to see nuances between Cover_Object and Stego_Object, the process of substituting least significant bit of Cover_Object with bits of secret message will not lead to a noticed distortion compared with the higher significant bits. Figure 1 shows the substitution process.

As we mentioned above, the goal of hiding is protecting secret information without any doubt about its existence. This means that all parts of security (confidentiality, integrity, and availability) are needed. To deal with those major requirements and manipulating them, the following section includes expected problems and proposed solution.



1	0	1	0	0	1	0	1
0	1	1	1	1	0	1	0
0	0	1	1	0	1	1	1
1	0	1	1	1	1	0	1
1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0
1	0	1	0	1	0	1	1
0	1	1	0	1	1	0	1
1	1	1	0	0	0	1	0
0	0	0	0	0	0	0	1
0	1	1	1	1	0	0	1
0	0	0	0	0	0	1	0
1	0	0	1	0	0	0	0
0	1	0	1	0	0	0	0
1	0	1	1	0	0	0	0
1	0	1	0	1	0	0	0

0
0
0
0
0
0
0
0
0
1
0
0
0
0
0
1

1	0	1	0	0	1	0	0
0	1	1	1	1	0	1	0
0	0	1	1	0	1	1	0
1	0	1	1	1	1	0	0
1	1	1	1	1	1	1	0
0	0	1	0	0	1	0	0
1	0	1	0	1	0	1	0
0	1	1	0	1	1	0	0
1	1	1	0	0	0	1	0
0	0	0	0	0	0	0	1
0	1	1	1	1	0	0	0
0	0	0	0	0	0	1	0
1	0	0	1	0	0	0	0
0	1	0	1	0	0	0	0
1	0	1	1	0	0	0	0
1	0	1	0	1	0	0	1

Figure 1: Substitution Process.

3.1 PRPBLEMS AND SOLUTIONS

The first problem is the inevitable distortion output. If any change is done, the cover will be distorted. If the change is done to the least significant bit, the distortion will be unnoticed. Thus LSB technique is the solution. The second problem is what about if the attacker is naturally skeptical ? He will take LSB and check bits to know if it means something or not. As a result, the full process will be crashed. The solution is to add a stage to encrypt secret information (we used 3DES similar to [20]) before hiding in LSB, so that if the attacker was skeptical he must be able to decrypt data to get secret information. Third problem is what about if the attacker can be able to decrypt data? Thus, he will pass the previous difficulty and get secret information and the process will be crashed. The solution is to add another stage to randomize bits of secret message before hiding in LSB [21]. In other words, bits of secret message will not be put in the same places within LSB, but in other places generated by random algorithm, so that if the attacker can be able to decrypt data, he will be unable to discover random algorithm.

Final problem is what if the attacker is professional and be able to decrypt data and discover random algorithm? As a result, the full process will be also crashed. The solution is using failed attack [22] through inserting unimportant information within secret one, then applying the previous mentioned stages before hiding in LSB. This means that effort, energy, and time of the attacker will be lost in vain, and finally he will get unimportant information. It is known that encryption algorithm needs a key and random algorithm needs a seed. In our proposed model we used single key for both which is called Stego_Key. The sender hides his secret information within cover then sends it via internet and receiver needs Stego_Key to extract hidden data.

The task of RSA algorithm [23] is to protect the Stego_Key and delivering it safely to the receiver side. So, we must update the parts of steganography mentioned in section 3 to become as the following :
Sender side:

Cover_Object + Hidden_Data + Stego_Key = Stego_Object (2)

Reciever side:
Stego_Object + Stego_Key = Hidden_Data (3)

RSA algorithm ensures confidentiality and reliability by both public and private keys and LSB ensures least distortion that does not raise any doubts. If sending is done successfully without any problems, we can extract complete secret information which in turn means integrity, and this is exactly what we want. Figure (2) shows the whole process of steganography.

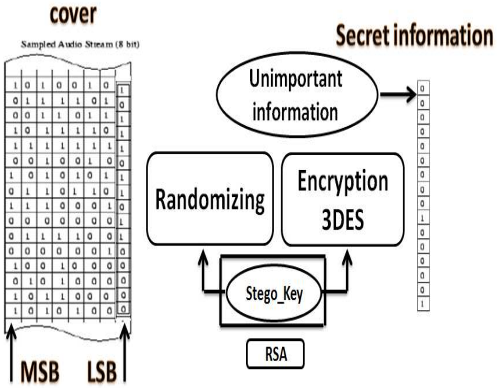


Figure 2: Steganography Process.

4. IMPLEMENTATION

The application we propose in this paper is provided for users that need to protect their secret information through hiding it within image or audio file.

We have used JAVA to implement the application. The inputs are: Cover_Obiect (an innocent image or audio file), Stego_Key (key of encryption 3DES algorithm and seed of randomizing algorithm), and Hidden_Data (secret information). The output is : Stego_Object (image or audio file after hiding).

We concerned about randomization phase where it could be described through the following steps:

1. Zigzag Step: this step converts the 2D array into 1D array (Vector) without incremental order for cells which in turn means more randomization in spreading the secret message over all the cover. This provides more security specially when this step integrates with next steps.
2. Selecting Starting Value : unlike to the all the previous Stegano methods where they start form the first element to hide secret message, we can start the insertion from any position. This creates another obstacle against the attacker.
3. Selecting Jump Value : we modified the traditional step of selecting the next position to be assigned as a place to the next bit of the secret message by selecting a jump. In other words, instead of positions 1, 2, 3 …. Etc, the sequence will be as 1, 4, 7, … with jump equals to 3, for example. Integrating this step with previous steps can add a new level of security.
4. Selecting sequence of Layers (R, G, B) : this means that we did not select, similar to traditional way, neither one layer to hide the bits of the secret message nor all layers. In our proposed approach, we used different layers in each pixel to hide the secret message for example (R Then R then B then G). This means that the hiding will be according to RRGB sequence from the beginning to the end.

According to the randomization phase, the form of stego-key will be as shown in figure 3.

1	2	3	4	5	6	#	8
Original Secret Key							Start
#	10	#	12	13	14	15	16
	Jump		Sequence of Color layers as RRGBB				

Figure 3 : Stego-Key Structure.

Table 1 includes the packages and classes that are related to hide in image which are the similar to the ones used for audio.

Table 1 : Packages And Classes Involved In Our Implementation.

Package	Class	Description
GUI	MainFrame	Main interface of application.
	MainApp	Called to run program.
CryRand	CryptDes	Encryption by 3DES.
	Randomizing	Randomizing
	Chang To Number	Used to covert char set into numbers corresponding to ASCII table.
InsertGif	G_TxtLsbSteg	Read text file we want to hide, convert it into series

		or bits, then hiding in LSB.
	G_GifLsbSteg	Read image file we want to hide, convert it into series or bits, then hiding in LSB.
	G_MP3LsbSteg	Read audio file we want to hide, convert it into series or bits, then hiding in LSB.
Extract_G	G_Extract_Txt	Used for extracting text file from image file.
	G_Extract_Gif	Used for extracting image file from image file.
	G_Extract_Mp3	Used for extracting audio file from image file.
General Operations	BitOperations	To deal with bytes like getting LSB of specific byte.
	MessageDialog	To launch an suitable error message.

Figure 4 illustrates the flow chart of our proposed algorithm.

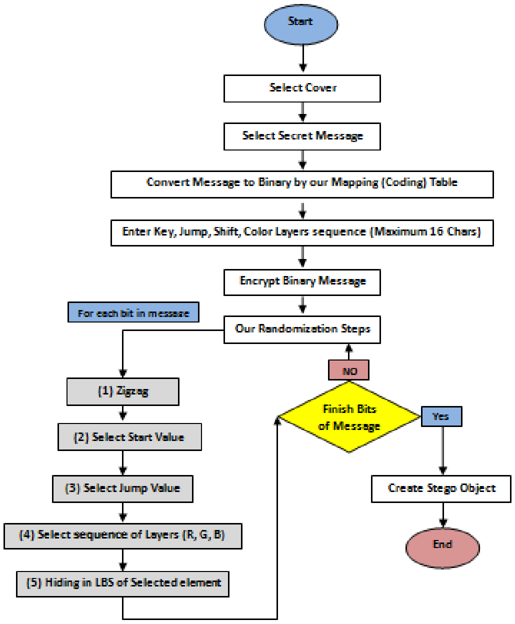


Figure 4 : Flow Chart Of Our Proposed Algorithm.

5. EXPERIMENTAL RESULTS AND EVALUATION

In order to test our application we do the following:

1- We wrote a text file.
2- We draw an image by painter.
3- We recorded an audio file by recorder.
4- We used an innocent image file of type GIF as a cover and audio file of type MP3, according to the popular wide exchanging over the web.

5.1 Image File As Cover

We could hide the created text file, image file, and audio file within the original image and extracted them successfully. The following figures shows the original image and the resultant stego_objects respectively.

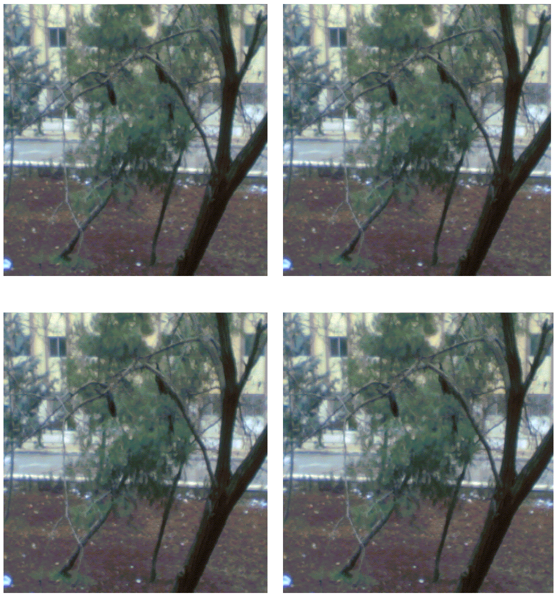


Figure 5 : cover, cover after hiding (text, image, and audio).

We used MATLAB program to plot the histogram, which represents the distribution of image pixels, for each image above where we can notice that the pixels are distributed uniformly, compared with cover image, which in turn reflects the similar appearance for each resultant images. Figure 6 illustrates this observation.

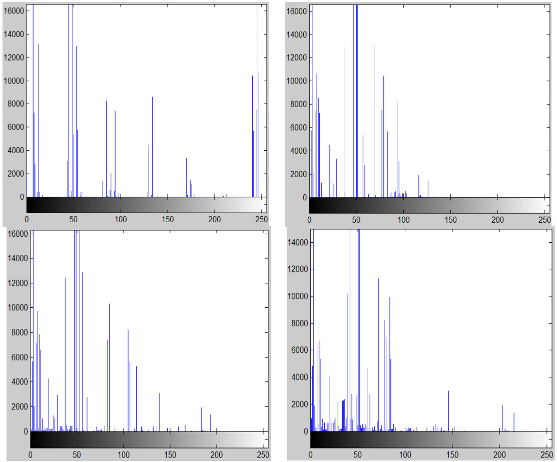


Figure 6 : Cover Histogram, Cover After Hiding (Text, Image, And Audio Histogram).

From figure 5, it could be noticed that no differences between the cover and the resultant images after hiding. This is because the hiding in LSB has the lowest distortion that could be caused which in turn reflects the success of our proposed approach for exploiting the low sensitivity of human visual system. Moreover, figure 6 supported our claim where slight change happened on the histogram after hiding.

To measure the quality of our proposed approach, we used the following metrics: Correlation [25] factor which measures the similarity between the cover and stego_object.

$$corr = \frac{numberof\_unchangedpixels}{numberof\_all\_pixels\,in\_one\_imag} \quad (4)$$

PSNR [26] which measure the Peak Signal to Noise Ratio. It needs to calculate MSE.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2$$

$$PSNRindB = 10Log_{10}\frac{L^2}{MSE} \quad (5)$$

Where,

MSE: Mean Square Error.
M,N: Row, column of original image.
f_{ij} : Pixel of cover.
g_{ij} : pixel of image after hiding.
L: Level of peak signal that equals 255.

MSSIM [27] which measures the quality of an image to evaluate the visual impact through luminance, contrast, and structure.

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (6)$$

Where,

- μ_x the average of x;
- μ_y the average of y;
- σ_x^2 the variance of x;
- σ_y^2 the variance of y;
- σ_{xy} the covariance of x and y;
- $c_1=(k_1L)^2$, $c_2=(k_2L)^2$ two variables to stabilize the division with weak denominator;
- L the dynamic range of the pixel values (typically this is $2^{\#bits\ per\ pixel}-1$);
- $k_1=0.01$ and $k_2=0.03$ by default.

Bit Error Rate which calculates the amount of noise caused by hiding.

$$BER = \frac{number\_of\_errors}{total\_number\_of\_bits\_send} \quad (7)$$

Table 2, 3 summarize our obtained results.

Table 2 : Evaluation Values For Image File Cover.

Stego_object	Original image		
	MSE	PSNR	SSIM
Stego_T	105.074	64.278	0.854
Setgo_G	95.423	65.242	0.798
Stego_A	97.190	65.058	0.749

Table 3 : Similarity And Error Ratio For Image File Cover.

Stego_object	Original image	
	Correlation	Bit error rate
Stego_T	0.97	0.3672
Setgo_G	0.91	0.4367
Stego_A	0.88	0.4471

From table 2 and 3, it is clear that the amount of distortion caused by hiding is very low according to the high PSNR values where its value differ according the type of hidden data. This is because the amount of data that represents any type of data is originally differ when it stored in digital form. Moreover, high values of SSIM reflect the positive results under the term of human eye sensitivity to the luminance. This means that the hidden data is invisible by an attacker at all. Furthermore, the high values of correlation means that the resultant stego_object is very similar to the cover, unlike to bit error rate that gives low results since the hiding is done in the LSB.

5.2 Audio File As Cover

We used an audio file for Surat Al-Fateha (from the Holy Quran) to represent the cover. We also used PSNR, correlation, and bit error rate as metrics to measure the quality of our proposed approach. Table 4 provides our obtained results. Figure 7 illustrates this support.

Table 4 : Evaluation Values For Audio File Cover.

Stego_object	Original audio		
	PSNR	Correlation	Bit error rate
Stego_T	60.582	98.52	0.453
Setgo_G	59.988	82.68	0.789
Stego_A	59.246	66.98	0.851

In general, comparing with the results obtained under image cover, the audio cover performs less. This is because the ear of human beings is more sensitive than the eye. But, the values of correlation related to hide text file refer to a high quality comparing to the hiding of image or audio. This means that our approach performs better if a person have a text file as a secret information to be hidden against attacks. To prove our claim we duplicate the amount of data included in the text file four times. Table 5 summarizes our results.

Table 5: Evaluation Values With Duplicated File Text Size.

Text file order	Size in byte	PSNR	Correlation	Bit error rate
1	150	60.582	98.52	0.453
2	300	58.989	98.11	0.389
3	450	57.658	95.26	0.352
4	600	56.472	94.89	0.324

According to the low differences values in PSNR, correlation, and bit error rate, our approach is the best way to hide and protect a secret text message with a high level of security.

Under waveform term, we can infer the differences among cover and resultant stego_objects which in turn reflects the strong of our approach using text file as a secret information, as it is shown in figure 7.

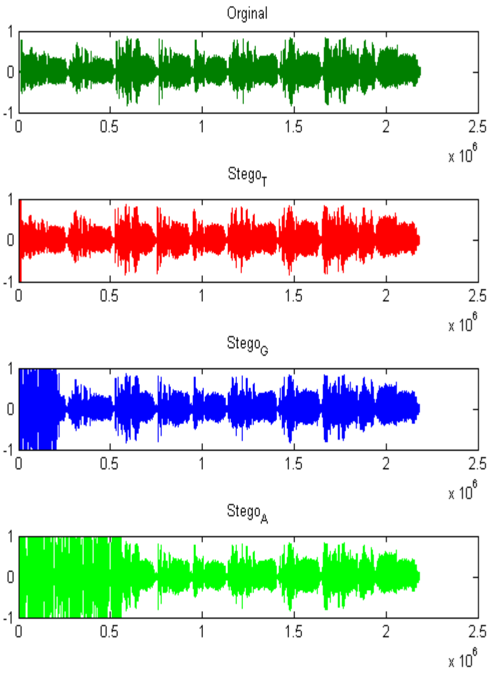


Figure 7 : Differences Among Waveforms.

6. CONCLUSION AND FUTURE WORK

In this paper, we showed a new technique for hiding a message within an image or audio file that can suit many types of data. We also showed how we can build an application that handles different expected problems with high level of security and demonstrated a brief implementation issues. Hiding and extracting a secret message was done successfully so that distortion is invisible, in spite of this, distortion is noticed in the histograms. On the other hand, a cover that can contain the secret information when it is image or audio file must be chosen. Finally, we presented practical example to measure the quality of hiding with output results.

Our proposed model could be extended to include video file as a live cover. Moreover, we will enhance our approach dealing with wavelet transform since it is considered more robust against attacks such as Gaussian noise, filtering, and compression.

REFRENCES:

[1] Sellars, Duncan. "An introduction to steganography." cs. uct. ac. za/courses/CS400W/NIS/papers99/dsellars/stego. html (1999).

[2] Al-Mualla, Mohammed, and Hussain Al-Ahmad. "Information hiding: steganography and watermarking." Proceedings of the IEEE (2008).

[3] Alla, Kalavathi, and R. Prasad. "An evolution of Hindi text steganography. "Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on. IEEE, 2009.

[4] Shirali-Shahreza, M. Hassan, and Mohammad Shirali-Shahreza. "A new approach to Persian/Arabic text steganography. " Computer and Information Science, 2006 and 2006 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on. IEEE, 2006.

[5] Bhattacharyya, Souvik, Indradip Banerjee, and Gautam Sanyal. "A novel approach of secure text based steganography model using word mapping method (WMM). " International Journal of Computer and Information Engineering 4.2 (2010): 96-103.

[6] Gutub, Adnan, et al. "Pixel indicator high capacity technique for RGB image based Steganography. " WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications. 2008.

[7] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." VISAPP (1). 2007.

[8] Chen, Po-Yueh, and Hung-Ju Lin. "A DWT based approach for image steganography." International Journal of Applied Science and Engineering4.3 (2006): 275-290.

[9] Verma, Tanmaiy G., Zohaib Hasan, and Dr Girish Verma. "A Unique Approach for Data Hiding Using Audio Steganography." International Journal of Modern Engineering Research (IJMER) www. ijmer. com 3.4 (2013).

[10] Kumar, Samir, B. Barnali, and G. Banik. "LSB modification and phase encoding technique of audio steganography revisited." International Journal of Advanced Research in Computer and Communication Engineering 1.4 (2012): 1-4.

[11] Sinha, Nishith, Anirban Bhowmick, and B. Kishore. "Encrypted Information Hiding using Audio Steganography and Audio Cryptography. " International Journal of Computer Applications 112.5 (2015).

[12] Ramesh, Vikash, Kaushik Narayanan, and Premalatha Pandian. "Steganography in Audio Signals using Variable Bit Replacement Method in DCT Domain." International Journal of Engineering Research and Technology. Vol. 3. No. 4 (April-2014). ESRSA Publications, 2014.

[13] Nissar, Arooj, and A. H. Mir. "Classification of steganalysis techniques: A study. " Digital Signal Processing 20.6 (2010): 1758-1770.

[14] Banerjee, Indradip. "Text Steganography using Article Mapping Technique (AMT) and SSCE." Journal of Global Research in Computer Science 2.4 (2011).

[15] T. Moerland, "Steganography and Steganalysis", Ma 15, 2003.

[16] Singh, Prem, Rajat Chaudhary, and Ambika Agarwal. "A Novel Approach of Text Steganography based on null spaces." IOSR Journal of Computer Engineering 3.4 (2012): 11-17.

[17] Jain, Nitin, Sachin Meshram, and Shikha Dubey. "Image Steganography Using LSB and Edge–Detection Technique." International Journal of Soft Computing and Engineering (IJSCE) ISSN 223 (2012).

[18] Gupta, Shilpa, Geeta Gujral, and Neha Aggarwal. "Enhanced Least Significant Bit algorithm For Image Steganography." IJCEM International Journal of Computational Engineering & Management 15.4 (2012): 40-42.

[19] Adhiya, K. P., and Swati A. Patil. "Hiding Text in Audio Using LSBBased Steganography, " Information & Knowledge Management (2224-896 X) 2.3 (2012), Vol 2, No.3, 2012.

[20] Salleh, Mazleena, Subariah Ibrahim, and Ismail Fauzi Isnin. "Image encryption algorithm based on chaotic mapping." Jurnal Teknologi 39.1 (2012): 1-12.

[21] Cheng, Lipin B., and Ren Jye Yeh. "Trial encoding algorithms ensemble."SpringerPlus 2.1 (2013): 316.

[22] Kiesling, Elmar, et al. "Evolving secure information systems through attack simulation." System Sciences (HICSS), 2014 47th Hawaii International Conference on. IEEE, 2014.

[23] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." IJRCCT 1.4 (2012): 143-146.

[24] Kurniawan, Budi. Java: A Beginner's Tutorial. Brainy Software Inc, 2015.

[25] Jacobs, David. "Correlation and Convolution." Class Notes for CMSC 426 (2005).

[26] Hore, Alain, and Djemel Ziou. "Image quality metrics: PSNR vs. SSIM."Pattern Recognition (ICPR), 2010 20th International Conference on. IEEE, 2010.