ISSN 2347 - 3983
Volume 7, No. 9 September 2019
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter19792019.pdf
https://doi.org/10.30534/ijeter/2019/19792019

Android-based Image and Video Steganography System

Reggie C. Gustilo[1]. Ron Michael Castillo[2], Nicole Anthonnie Gonzales[3], John Gerard Raz[4], Trisha Jane Tejones[5]
Electronics & Communications Engineering Department
De La Salle University Manila, Philippines
[1]reggie.gustilo@dlsu.edu.ph
[2]ron_castillo@dlsu.edu.ph
[3]nicole_gonzales@dlsu.edu.ph
[4]john_gerard_raz@dlsu.edu.ph
[5]trisha_tejones@dlsu.edu.ph

ABSTRACT

Steganography is a form of security measure wherein confidential information is hidden within a cover media. This study aims to contribute to the security of digital information, particularly of audio data using image and video steganography. A total of six technique combinations were derived from three-pixel location strategies and spatial domain embedding in order to successfully mask and impose audio data into cover images and videos. The final prototype comes in the form of an integrated system that operates on three environments. The first platform is an android application, which serves as the input/output gateway, followed by a Matlab program which serves as the main processor, and a server that allows two-way exchange of information at both ends. The goal of the prototype is to successfully hide the audio data into the cover media with minimal to negligible visual and audible changes between the original files and output files. To evaluate the system's performance, both qualitative and quantitative bases are used. Quantitative assessment includes the MSE and PSNR of the steganography output, the BER and accuracy of the recovered audio data. Meanwhile, qualitative assessment is conducted in the form of a survey. Results from quantitative and qualitative assessment strongly verify that the proposed integrated system is verified and hereby recognized as consistent, reliable and accurate.

Keywords: Steganography, image, video, embedding

1. INTRODUCTION

In this digital age, hundreds of researchers focus on topics that take advantage of the advancements of technology and computer systems. Some of these research topics cover machine vision system [1], [2], [3], [4] and expert systems or intelligent systems [5], [6], [7], [8], [9], [10]. [11], [12]. On the other hand, all these research topics must assure that all information are secure and accurate even if this information are transmitted in public domains or unbounded media like wireless transmission such as wifi, Bluetooth and the like. The information being transmitted can be altered resulting to errors during transmission. Fortunately, there are also lots of researches that focus on how transmission of data can be improved [13], [14], [15], [16], [17], [18]. Aside from assuring that the information is accurate. There are few instances that information must be properly secured or even concealed to protect it from unauthorized access from unknown users [19].

Cryptography protects the information being sent by converting it into data that is hidden or unreadable to an unknown user. This is done to secure digital information sent over unbounded or unsecure media. A key or password is usually shared by the sender and receiver to extract and recover the information signal. Cryptography provides confidentiality, authenticity and data integrity for computer systems. However, because of the advancements in technology and computer science, cryptography based security schemes are vulnerable, at the same time cryptographic techniques are hard to decode. While messages are written in secret codes and symbols, it is apparent to other users that it is an encrypted message. The contents of the messages are hidden while the message itself is not.

A new technology called digital steganography is an alternative to cryptography. Unlike cryptography, steganography hides both the content and any signs of hidden message from information hackers. Digital steganography embeds an encrypted message in a cover media such as audio, digital image or video. It is a technique wherein the least significant components of a cover media are replaced by the hidden message. With this technique, other users are kept unaware of the existence of the message. The steganography image or video should be visually similar to the original file to avoid suspicions of having hidden messages.

Image Steganography [20] usually uses the Least Significant Bit technique in embedding the message on the images. Images typically has either 8-bit or 24-bit color matrix. The pixels are composed of a set of bits that define its color. The encrypted message or the cipher-text are embedded in the message in such a way that alterations are not distinguishable by other users. The Least Significant Bit technique alters the

LSB of a pixel that contains the bits of the hidden message. The LSB method is the most common and the simplest technique used for embedding messages in a cover media. The LSB method also allows embedding large capacity of information [4]

Video Steganography uses video files as cover media. The use of video steganography is one of the most secure type of steganography due to its capacity and complexity. The video file is converted into frames where the bits of the encrypted message are embedded. The use of the video file as the cover media, the bits of the message or information embedded is unnoticeable.

2. PROBLEM STATEMENT

A complex method of hiding information using audio signals was proposed using image and video steganography. Audio signal considered information signals are embedded in either an image cover media or a video cover media.

3. METHODOLOGY AND DESIGN CONSIDERATIONS

Here are the techniques and methods used in this research to fully implement an audio and video steganography.

Table 1: Elements of the Image and Video Steganography

Software/ Method used	Description
Matlab	This is used to perform most of the processing like embedding of the audio data into the cover medium, extracting audio data from previously embedded files, conversion and sampling of audio data, password generation, recovery and analysis, and technique-based identification of pixel locations.
Android Studio	This is used develop an Android Application that will serve as the input and output interface of the project.
Server	It acts as the medium between the Android Application and Matlab. Its main purpose is to store data for both the android application and Matlab.
Android Application	The Android Application developed is capable of reading audio, image, and video files from internal storage. It is used for uploading and downloading audio, image, and video files to database server.
Audio as a Secret Message	Audio files were used as the secret messages in this study.
Image as a Cover Media	Image files are used to embed audio files to cover the hidden information. The last bit of each color component of an image is used as storage for the audio message to be transmitted.
Video as a Cover Media	Images from video files are used to embed audio files to cover the hidden information and can carry larger audio data than image cover media. Mp4 format is not used due to compression done that corrupts the embedded audio message.
LSB Embedding Technique	The LSBs of the selected pixels are compared and modified in accordance to the secret message. The R, G and B components of each pixel serve as carriers of the secret message, by modifying the last 2 or 3 bits of the color values. For a single pixel, a maximum of 9 LSBs may be modified.
Selection of Pixel Location Strategies	These are methods that choose the location of the pixels that will carry the information signal or the audio signal.
Password	Password is used increase the security of the information. It consists of 10 alphanumeric and special characters that are generated in both image and video embedding. Passwords have a total length of 57 bits.

3.1 Embedding Technique Design

Six techniques were derived and implemented from the combinations of three carrier pixel location strategies and spatial- domain embedding. Table 2 below shows the bases of each technique in terms of carrier pixel location and n-bit embedding that needed to hide the information.

Table 2: Technique Details

Technique	Pixel Location Strategy	LSB
T1	Pseudo Random Technique	2
T2	Pseudo random Technique	3
T3	Pixel Intensity Based Technique	2
T4	Pixel Intensity Based Technique	3
T5	Side-most Technique	2
T6	Side-most Technique	3

3.1.1 Pseudo-Random Pixel Location Selection

Depending on the dimensions of the image, this technique produces a specific sequence of the designated carriers and all the pixels contained in the image can be used. The technique will first identify the locations of each pixel then it will rearrange the said locations using the sequence produced by the technique.

3.1.2 Pixel Intensity Based Selection

In this technique, the pixels recognized as dark are designated as the carriers of the audio data. The grayscale values of the pixel images determine the darkness or whiteness of the pixel. The dark pixels are then identified and used as carriers.

In the identifying the carrier pixel locations, the equivalent grayscale image of the original true colored image aree used as the basis for visual examination. The equation for getting the equivalent gray values are shown below.

$$\text{Gray value} = 0.299R + 0.587G + 0.114B \quad (1)$$

Where R = red pixel component value
G = green pixel component value
B = blue pixel component value

Pixels with a grayscale values ranging from 0 to 120 are assigned as carrier pixels. The maximum absolute deviation from the original pixel value is 7 due to the fact that up to the third least significant bit of the RGB values may be modified. With this, the upper range limit was extended to 127 during the extraction process. This is also done in order for the program to distinguish which are non- embedded and embedded pixels. Embedded pixels have values in the range from 121 to 127 while the non-embedded pixels are modified in such a way that its equivalent gray values become at least 128. This modification was done using the equations below used in computing the new RGB values of the pixel components.

$$R_{new} = R_{old} + (128 - \text{Gray value}) \quad (2)$$
$$G_{new} = G_{old} + (128 - \text{Gray value}) \quad (3)$$
$$B_{new} = B_{old} + (128 - \text{Gray value}) \quad (4)$$

Where R_{new}, G_{new},B_{new} = new pixel component values
R_{old} , G_{old} , B_{old} = old pixel component values

The Pixel Intensity Based Selection is done by firswt converting the color images into grayscale. The grayscale values are then divided into two groups, values from 0 to 120 and values from 128 to 255. All pixel colors with an equivalent gray value of 127 and below are replaced by 0 (black) while the remaining upper range is represented by 1 (white). The coordinates of all pixels represented by zero serve as carrier pixel locations.

3.1.3 Side-most Pixel Selection

In this technique, 80 percent of the total columns in an image or frame are located and assigned as carrier pixels. Half of these columns are taken from the leftmost side and the other half from the rightmost side. The length of audio information than can be carried by the cover image or video is limited by the number of carrier pixels of the image or frame of the cover media. Multiple audio information with variable lengths are used in this research.

3.2 Password Generation

For security measures, passwords consisting of 10 alphanumeric and special characters are generated in both image and video embedding. The password's binary data comprises of a total of 57 bits which corresponds to 7 pixels (three color value RGB for each pixel, 3 bits per color value). The sampling frequency of the audio information used 18 bits of data that requires to pixels for embedding and lastly, the number of channels of the audio information that requires 2 bits and embedded in a red color data of a pixel. Table 3 below shows the bit configuration of the password for both image and video cover media.

Table 3: Bit Configuration for Passwords

Nth Character	Image password bit count	Video password bit count
1	7	3
2	3	7
3	7	4
4	4	4
5	4	7
6	7	7
7	7	4
8	4	7

3.3 Carrier Frame Selection for Video Steganography

For video steganography, the audio data is scattered throughout the video frames. The binary audio data are embedded on either every 10th frame or 2nd frame. This depends on the size of the audio data that must be embedded for every frame as well as the total number of video frames. By default, the frame interval for embedding is 10. The total number of frames in the video is used to determine how many frames, in intervals of 10 may be processed for embedding. The audio data is then divided into the number of carrier frames to determine how many audio bits must be embedded for every carrier frame.

3.4 Output File Formats

The proposed file formats after the embedding process are Portable Network Graphics (PNG) for images, Audio Video Interleaved (AVI) for videos and Waveform Audio (WAV) for the recovered audio data. It is found the in this implementation, file format MPEG- 4 (MP4) for videos is not compatible for writing the output steganographic video because it uses standard compression techniques that corrupt or alter the original data.

3.5 Systems Integration

The user interface for the system is the android based program used to load or capture the audio information to be transmitted, password generation and extraction and selection of embedding technique to be used. The basic block diagram of the system integration is shown in figure 1 below. The sender and the receiver are linked via a webhost program that overlooks the transmission and reception of the embedded signal. A server is also used to perform all the complex processing needed in the system such as embedding of the audio signal into either the image or video cover media.

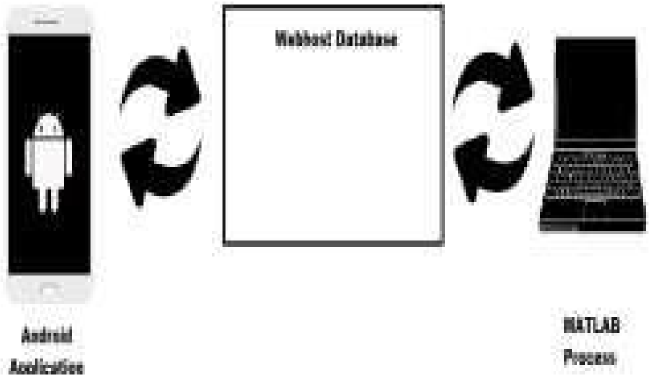


Figure 1: Integrated System Design

Transmission is done in two modes, Bluetooth and email. Steganographic video files are limited to 25MB for email transmission.

3.6 Extraction Process

During extraction process, the user must enter the correct password generated by the system. The system will only continue if the password entered is similar to the password generated when the steganographic image or video is produced. The password was also used to determine details for extraction, such as the technique used and the number of bits to be extracted by the system. The bits extracted were used to reconstruct the audio information that can be retrieved by the user.

3.7 Evaluation of the system

Two comparative methods were used to measure the effectiveness of the system. Quantitative analyses were done with respect to error parameters such as the BER, MSE and PSNR. The MSE and PSNR were obtained from the embedded steganographic images and videos compared to their original unembedded input files. The bit error rates were obtained by comparing the original and the recovered audio files.

Qualitative analyses were also done by examining the visual changes between the original file and the produced steganographic file. In support the qualitative method, a survey was conducted involving 85 participants by asking them to determine whether or not visual and audible changes were noticeable. The produced steganographic files were transmitted using Bluetooth or E-mail. Error checking parameters such as MSE and PSNR were computed between the embedded file and the received file.

4. DATA AND DISCUSSIONS

Image steganography and video steganography are implemented and tested using the same audio information signals.

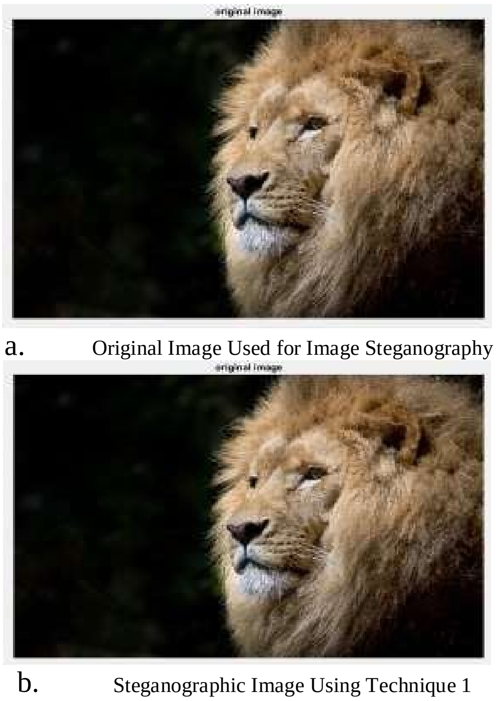
4.1 Image Steganography

The data shown to test and implement image steganography is shown in table 4 below.

Table 4: Data Used for Image Steganography

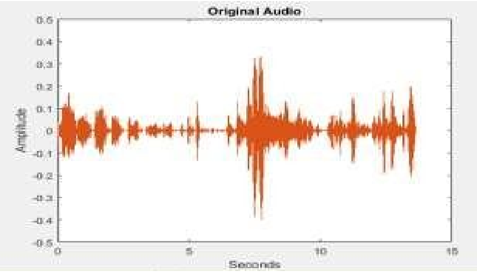
Image	Height	2835
	Width	4252
	Size	3.23MB
Audio	Row	713726
	Channel	2
	Frequency	44100
	Size	332KB

In the image steganography, the audio signal is embedded in the image using any of the six embedding techniques that is chosen by the user. The original image, image with embedded information and the original audio information is shown in figure 2.



a. Original Image Used for Image Steganography

b. Steganographic Image Using Technique 1



c. Original Audio Message

Figure 2: Original image, embedded image and audio signal used in Image steganography

Figure 2a shows the original image and the embedded image in figure 2b after using embedding technique 1 using the audio signal shown in figure 2c. there is very little or almost no difference between the original image and the embedded image using the naked eye.

The password generated during embedding and the qualitative comparison of the original image and the embedded image are shown in table 5 below.

Table 5: Qualitative Analysis using Image Steganography

Sample	Tech	Password	MSE	PSNR (dB)
1	1	D1j38v#5I|	0.7837	49.2229
2	2	D2j25y$6O+	2.2569	44.6295
3	3	D3j38v#5I|	1.2384	47.2359
4	4	D4j25y$6O+	2.5444	44.1088
5	5	D5j38v#5I|	0.7228	49.5740
6	6	D6j25y$6O+	1.9691	45.2219

From table 5, it can be seen that using image steganography, the original image and the embedded image are visually similar but qualitatively different as shown by the MSE and PSNR values that proves the difference in the pixel values of the two images.

After the extraction and recovery of the audio information signal, the BER during transmission is measured to check if the images are altered during the wireless transfer. Afterwards, the original audio data and the recovered audio data are compared by evaluating the accuracy of the recovered audio data. Table 6 shows the error checking of the audio signal.

Table 6: Audio Error Checking

Sample	Tech	BER	Accuracy
1	1	0	99.99998741
2	2	0	99.99998741
3	3	0	99.99998741
4	4	0	99.99998741
5	5	0	99.99998741
6	6	0	99.99998741

4.2 Video Steganography

The details of the data used for video steganography is shown in table 7 below.

Table 7: Input Details for Video Steganography

Video	Height	1080
	Width	1920
	Total Frames	97
	Frame Rate	24
	Duration	4.046
	Size	1.55 MB
Audio **Audio**	Row	1764352
	Channel	2
	Frequency	44100
	Size	621KB

In video steganography, the six embedding techniques are used to test the performance of the system. Table 8 shows the password generated by each technique.

Table 8: Technique and Password Details

Technique	Password
1	1j03z&4H~E
2	2j03z&4H~E
3	3j03z&4H~E
4	4j03z&4H~E
5	5j03z&4H~E
6	6j03z&4H~E

The embedded videos are transmitted wirelessly using Bluetooth and email. The average performance of the transmission is shown in table 9.

Table 9: Average Transmission Performance for Video Steganography

Technique	MSE	PSNR (dB)
1	0.1176	57.4609
2	0.3351	52.9128
3	0.1429	56.6133
4	0.3588	52.6167
5	0.1168	57.4903
6	0.3344	52.9216

Lastly, the original audio messages were compared to the recovered audio messages and were tested for accuracy. Table 10 shows the average accuracy of the recovered audio messages.

Table 10: Audio Error Measurements

Technique	BER	Accuracy
1	0	99.5656
2	0	99.5656
3	0	99.5656
4	0	99.5656
5	0	99.5656
6	0	99.5656

5. CONCLUSION

A complex android driven system was developed to implement image and video Steganography. The user interface was driven an android application that was able to load or record the audio signal to be transmitted, choose the type of embedding technique to be used and generate the password for added security during transmission. On the receiver side, this android application can extract and recover the embedded audio signal with at least 99.99% accuracy. The length of the audio signal is variable and the duration depends on the size of the image cover media or the video cover media.

Matlab is used to perform all the complex tasks such as the actual embedding, extraction and recovery of the audio signal. The android program and the Matlab program are linked using a webhost and a server that process and saves all the data of the system.

The embedded images and videos are transmitted wirelessly via Bluetooth and email. BER and PSNR are used to quantify the performance of the system during the transmission stage.

Experiment results show that the presented steganography methods are proven to be efficient and effective way of concealing audio information inside images or videos.

REFERENCES

1. Gustilo, R.C., Dadios, E.P., **Machine vision support system for monitoring water quality in a small scale tiger prawn aquaculture**, *Journal of Advanced Computational Intelligence and Intelligent Informatics,* 20(1), pp. 111-116, 2016 https://doi.org/10.20965/jaciii.2016.p0111
2. Gustilo, R.C., Dadios, E.P., **Behavioural response analysis using vision engineering (BRAVENet)**, *Journal of Advanced Computational Intelligence and Intelligent Informatics*, 21(2), pp. 211-220, 2017 https://doi.org/10.20965/jaciii.2017.p0211
3. E. Mohammadi, E. P. Dadios, L. A. G. Lim, M. K. Cabatuan, R. N. G. Naguib, J. M. C. Avila, and A. Oikonomou, **Real-Time Evaluation of Breast Self-Examination Using Computer Vision,** *International Journal of Biomedical Imaging*, vol. 2014, pp. 1–12, 2014.
4. R. A. A. Masilang, M. K. Cabatuan, and E. P. Dadios, **Hand initialization and tracking using a modified KLT tracker for a computer vision-based breast self-examination system,** *2014 International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*, 2014.
5. M. K. Cabatuan, E. P. Dadios, R. N. Naguib, and A. Oikonomu **Computer vision-based breast self-examination palpation pressure level classification using artificial neural networks and wavelet transforms,** *TENCON 2012 IEEE Region 10 Conference*, 2012. https://doi.org/10.1109/TENCON.2012.6412282
6. J. A. C. Jose, M. K. Cabatuan, E. P. Dadios, and L. A. G. Lim, **Stroke position classification in breast self-examination using parallel neural network and wavelet transform**, *TENCON 2014 - 2014 IEEE Region 10 Conference*, 2014.
7. R. A. A. Masilang, M. K. Cabatuan, E. P. Dadios, and L. G. Lim, **Computer-aided BSE torso tracking algorithm using neural networks, contours, and edge features**, *TENCON 2014 - 2014 IEEE Region 10 Conference*, 2014.
8. Del Espiritu, J., Rolluqui, G.,Gustilo, R.C., **Neural network based partial fingerprint recognition as support for forensics**, *8th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management, HNICEM* 2015
9. Abinoja, D.D., Roque, M.A., Atienza, R., Materum, L., **Landmark-based audio fingerprinting algorithm for a transmitter-less alert recognition device for the hearing-impaired**, *8th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management,* HNICEM 2015, .
10. A. Africa, **A Rough Set Based Solar Powered Flood Water Purification System with a Fuzzy Logic Model.** *ARPN Journal of Engineering and Applied Sciences.* Vol. 12, No. 3, pp.638-647, 2017
11. A. Africa and J. Velasco, **Development of a Urine Strip Analyzer using Artificial Neural Network using an Android Phone.** *ARPN Journal of Engineering and Applied Sciences.* Vol. 12, No. 6, pp. 1706-1712, 2017
12. S. Brucal, A. Africa, and E. Dadios, **Female Voice Recognition using Artificial Neural Networks and MATLAB Voicebox Toolbox.** *Journal of Telecommunication, Electronic and Computer Engineering.* Vol. 10, Nos. 1-4, pp. 133-138, 2018.
13. Villanueva, L., Gustilo, R.C., **Artificial neural network based antenna sensitivity assignments for chaotic Internet Service Provider network architecture,** *International Journal of Engineering and Technology (UAE)*, 7(2), pp. 14-17, 2018
14. Dulay, A., Sze, R., Tan, A., Yap, R., Materum, L., **Development of a wideband PLC channel emulator with random noise scenarios**, *Journal of Telecommunication, Electronic and Computer Engineering,* 2018
15. Hanpinitsak, P., Saito, K., Takada, J.-I., Kim, M., Materum, L., **Multipath clustering and cluster tracking for geometry-based stochastic channel modeling**, *IEEE Transactions on Antennas and Propagation, 2017* https://doi.org/10.1109/TAP.2017.2754417
16. Abinoja, D.D.N., Materum, L.Y., **BIC-based optimization of the identification of multipath propagation clusters in MIMO wireless systems**, *ISAP 2016 - International Symposium on Antennas and Propagation,* 2016
17. Dulay, A.E., Yap, R., Materum, L., **Hardware Modelling of a PLC Multipath Channel Transfer Function**, *Journal of Telecommunication, Electronic and Computer Engineering,* 2017
18. Materum, L., **Stochastic tapped delay line based one-sided beamformed channel impulse response models**

of LoS and reflected waves at 62.5 GHz in a conference room environment, *Journal of Telecommunication, Electronic and Computer Engineering,* 2017

19. Monica Thomas and Dr. Varghese S Chooralil, **Security and Privacy via Optimised Blockchain**, *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No. 3, 2019 https://doi.org/10.30534/ijatcse/2019/14832019
20. Kaushik H. Raviya, Dr. Dwivedi Ved Vyas and Dr. Ashish M. Kothari, **SVD Based Performance Improvement in Hiding a Message Behind an Image**, *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No. 2, 2019 https://doi.org/10.30534/ijatcse/2019/12822019