

Study of Encryption and Decryption of Wave File in Image Formats

Rahul R Upadhyay

Department of Mechanical Engineering, BBD National Institute of Technology and Management, Lucknow
Email: rahulrupadhyay91@gmail.com

ABSTRACT

This paper describes a novel method of encrypting wave files in popular image formats like JPEG, TIF and PNG along with retrieving them from these image files. MATLAB software is used to perform matrix manipulation to encrypt and decrypt sound files into and from image files. This method is not only a stenographic means but also a data compression technique.

Keywords -Stenography, Rasterization, Matlab, Grayscale Image.

Date of Submission: August 01, 2013

Date of Acceptance: August 30, 2013

1. INTRODUCTION

This present work puts forth a novel method to encrypt '.wav', which are basically sound files in image formats such as PNG, TIF and JPEG. The sound file is fetched and the values corresponding to the sample range is put in a column matrix which is then put in a two dimensional matrix having "double" as data-type. Using 'imwrite' function of MATLAB, this matrix defined in the class 'double' is put in a graphics file or image file having dynamic range from 0 to 1 [18].

After encryption the data is retrieved from the image file and compared with the original wave file to show the variation in encrypted and decrypted data. This methodology can not only be used as stenographic means but possibly as a technique for data compression. The illustrated method for data encryption of sensitive user information can be used as a viable method to further secure cloud computing transactions [11] [24] [27].

1.1 WAVE Bitstream Format

Waveform Audio File Format (WAVE) is an application of RIFF or Resource Interchange File Format which stores audio bit streams in "chunks". WAVE encodes the sound in LPCM format i.e. Linear Pulse Code Modulation [1] [22].

Sound is basically a pressure wave or mechanical energy having pressure variance in an elastic medium. The variance propagates as compression and rarefaction wherein compression occurs when pressure is higher than the ambient pressure and rarefaction occurs when the pressure of the propagating wave is less than the ambient pressure.

Exactly in the same manner a WAVE file just represents the sampled sound waves which happen to be above or below the equilibrium or ambient air pressure.

In this paper we will be using a "drums.wav" wave file to show the proposed algorithm of encrypting the sound file in various image formats [17] [26]. As already mentioned a wave file consists of positive and negative values over its entire range of samples. Here for the sake of simplicity we will be using only the samples having positive values. The sound file will be read and handled in MATLAB.

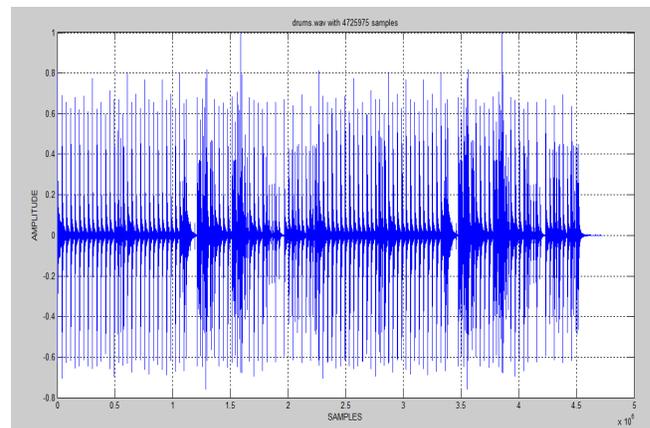


Figure 1 Graphical representation of "drums.wav" wave file in its entire sampling range.

1.1 Image Formats and Image Compression

Digital image formats are means of storing digital images in either uncompressed (e.g. TIFF), compressed (e.g. JPEG) and vector formats. On rasterization an image is converted into a grid of pixels. Basically there are two types of image file compression algorithm- lossless and lossy. In lossless compression the entire digital data is

preserved during compression thus preserving image quality. In lossy compressions, the digital data preservation takes place by compromising image quality [2]. Here we will be discussing PNG, TIFF and JPEG formats and these are the very formats in which the wave file will be encrypted into, in this paper.

TABLE I
 RASTER IMAGE FORMATS

Sr. no	Image Format	Description in Brief
1	JPEG	JPEG compresses image files to great extent but at the cost of image quality.
2	TIF	TIF is a lossless compression format which is considered as industry standard.
3	PNG	PNG files are smaller than TIF(LZW compression) though both are lossless although it is slower to read or write to.[3]

2. ENCRYPTION

2.1 Obtaining data of wave file in column matrix

We will be using “drums.wav” wave file in this paper whose graphical representation is provided in Fig1. The sampling length of this tone is 4725975 samples. As already mentioned, we will be using only those samples which have positive values. Following is the MATLAB code which fetches the wave file using ‘wavread’ function [4]. Amplitude values are obtained in the range of 0 and +1.

```

Command Window
>> % wavread to fetch .wav
>> b=wavread('C:\Users\Rajeeva\Desktop\drums.wav');
>> % C stores all values which are +ve
>> C=b(b>=0);
>> % D stores first 2000000 +ve values
>> D=C(1:2000000);
>> plot(D)
>> grid on
>> xlabel('Samples');
>> ylabel('Amplitude');
    
```

Figure 2 MATLAB code to fetch wave file and obtain first 2000000 positive samples.

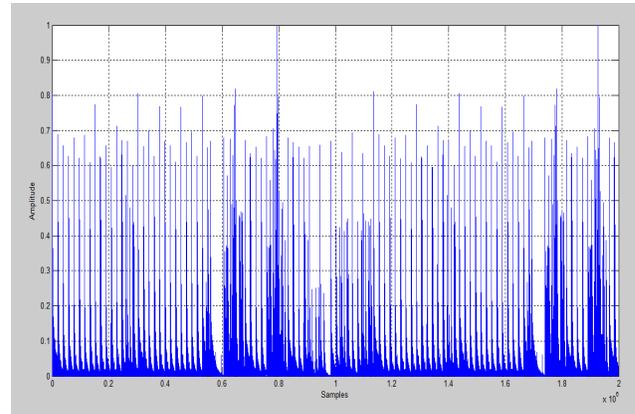


Figure 3 Graphical representation of variable ‘D’ which holds first 2000000 positive samples. Its value ranges from 0 and +1.

It is to be noted that the variable D is basically a column vector.

2.2 Converting column matrix into M x N matrix.

A ‘grayscale’ [12] image of M by N pixels is represented in MATLAB as an M X N matrix having “double” data type wherein each element of the matrix denotes a pixel within an intensity of 0 and 1. [5]. It is to be noted that the variable D is a column matrix with “double” type and intensity within 0 and 1. So to convert variable D in an image format we have to transform D into a 1000 X 2000 matrix.

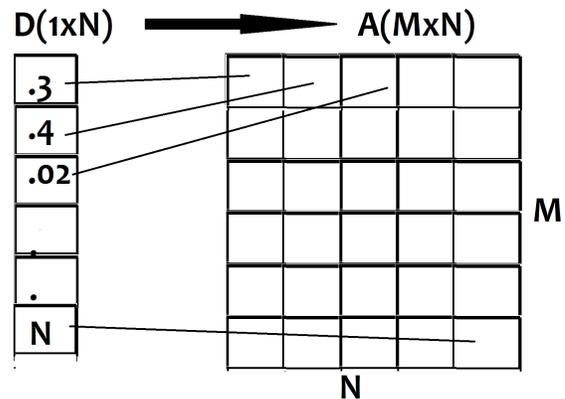


Figure 4 Converting N (1xN) matrix into A (MxN) matrix.

```

Command Window
>> x=1;
>> y=2000;
>> for i=1:1000
% All values in row i are fetched
L=D(x:y);
% Column vector L is transposed
N=L';
% Values are put in Matrix A(2000x1000)
A(i,:)=N;
x=x+2000;
y=y+2000;
end
    
```

Figure 5 MATLAB code to convert column matrix D into A (MxN) matrix.

2.3 Converting matrix into Image File.

We convert matrix A into JPEG [16], PNG and TIF formats using MATLAB function called “imwrite”.

Imwrite (A,'../filename.xyz'); [6]

The above syntax stores matrix A in the file path mentioned. We also save column matrix D in a new wave file using “wavwrite” function.

```
>> % converting MxN matrix in PNG, JPEG and TIF
>> imwrite(A, 'C:\Users\Rajeeva\Desktop\Aa.jpg');
>> imwrite(A, 'C:\Users\Rajeeva\Desktop\Aa.png');
>> imwrite(A, 'C:\Users\Rajeeva\Desktop\Aa.tif');
>> wavwrite(D,42100,'C:\Users\Rajeeva\Desktop\Aa.wav');
```

Figure 6 MATLAB code to convert column matrix A in image formats and array D into .wav file.

TABLE II
 SIZE OF WAVE FILE AND VARIOUS IMAGE FORMATS IN WHICH THE FILE IS ENCRYPTED INTO

S.no	NAME	TYPE	SIZE
1	Aa	.wav (WAVE)	3.81 MB
2	Aa.jpg	JPEG	293 KB
3	Aa.tif	TIFF	1.61 MB
4	Aa.png	PNG	734 KB

It can be clearly seen that JPEG stores the wave file of 3.81 MB into merely 293 KB whereas TIFF stores the same file in 1.61 MB. These images will be studied further in the paper.

Figure 7 Snapshot of how the wave file appears in JPEG format (this is a cropped image as the actual file is far bigger).

3. DECRYPTION OF WAVE FROM IMAGE

(STEGANALYSIS)[13][23] [14]

This method is just the opposite of encryption with minor variations. When the image is created during encryption it is basically an MxN matrix with “double” data type, however on fetching the same image back to MATLAB we get an MxN matrix with datatype “uint8” i.e. unsigned integer of 8 bits [20].

Thus we need to first convert all elements of matrix obtained into double precision [7].

Decryption can be basically understood as a data mining method to fetch, audit and understand the pattern of data stored in the encrypted file[9] [19] .

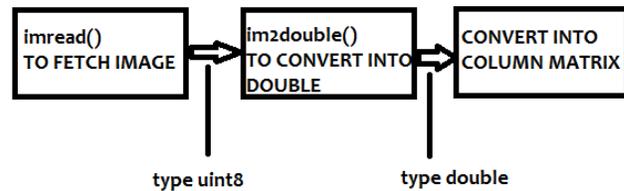


Figure 8 Figure showing the necessary conversion of datatype.

3.1 Datatype conversion[7]

“im2double” function of MATLAB takes an image as input and converts it into another image or matrix having all elements with type double. As already stated, the image files retrieved by MATLAB are in unsigned integer form and before they are put in column matrix representing a WAVE file, it has to be converted into datatype of double precision [21].

```
Command Window
>> %Fetch image file
>> AaJPG=imread('C:\Users\Rajeeva\Desktop\Aa.jpg');
>> AaTIF=imread('C:\Users\Rajeeva\Desktop\Aa.tif');
>> AaPNG=imread('C:\Users\Rajeeva\Desktop\Aa.png');
>> %CONVERT THE ABOVE MATRICES INTO DOUBLE PRECISION
>> AaJPG=im2double(AaJPG);
>> AaTIF=im2double(AaTIF);
>> AaPNG=im2double(AaPNG);
>>
```

Figure 9 MATLAB code to convert datatype of matrices.

3.2 ALGORITHM TO CONVERT IMAGE MATRIX INTO COLUMN MATRIX AND HENCE .WAV.[8]

“wavwrite(X, FS, ‘../filename.wav’);”

The above function is used to save X column vector in the given ‘filename’ (say DivyaSharma or Shumo) with a desired frequency ‘FS’. The column vector X is obtained by converting image matrix of double precision into column matrix. The method is explained in the following programming code of MATLAB.

```

Command Window

>> % defining column matrices
>> JPEG=[:];
>> TIF=[:];
>> PNG=[:];
>> %converting JPG into sound file
>> for i=1:1000
w=AaJPG(i,:);
%transpose of w
m=w';
JPEG=vertcat(JPEG,m);
end
>> i=1;
>> %converting PNG into sound file
for i=1:1000
w=AaPNG(i,:);
%transpose of w
m=w';
PNG=vertcat(PNG,m);
end
>> i=1;
>> %converting TIF into sound file
for i=1:1000
w=AaTIF(i,:);
%transpose of w
m=w';
TIF=vertcat(TIF,m);
end
fx >>
    
```

Figure 20 MATLAB Code to convert all image files into Column Matrix/Wave File.

4. GRAPHICAL ANALYSIS.

During encryption we used “wavwrite” to store the sample wave file that we used in the paper. We fetch the same wave file and compare it graphically with the sound files that we obtained during decryption.

```

Command Window

>> ORIGINAL=wavread('C:\Users\Rajeeva\Desktop\Aa.wav');
fx >>
    
```

Figure 11 Storing the original wave file in variable ORIGINAL.

4.1 ORIGINAL WAVE FILE vs. SOUND MATRIX OBTAINED FROM JPEG FILE.

We plot original file with decrypted sound file.

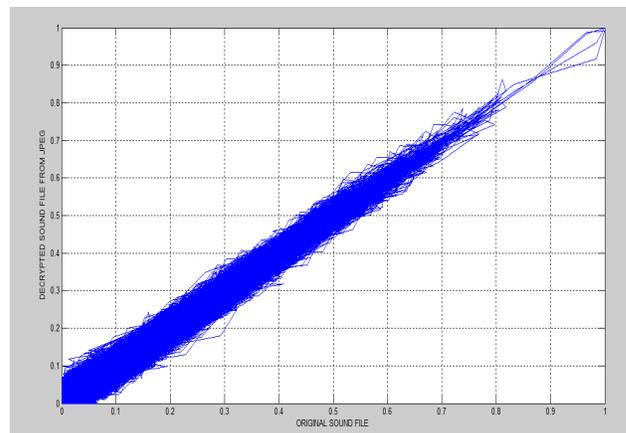


Figure32 Plot of the original sound file vs. the decrypted sound file.

The graph shows that the image file decrypted using JPEG has decent variation from the actual WAVE file. This variation can be represented by another 1000x2000 matrix called ERROR such that [25]

$$\text{ERROR} = \text{ORIGINAL} - \text{JPEG (Equation A)}$$

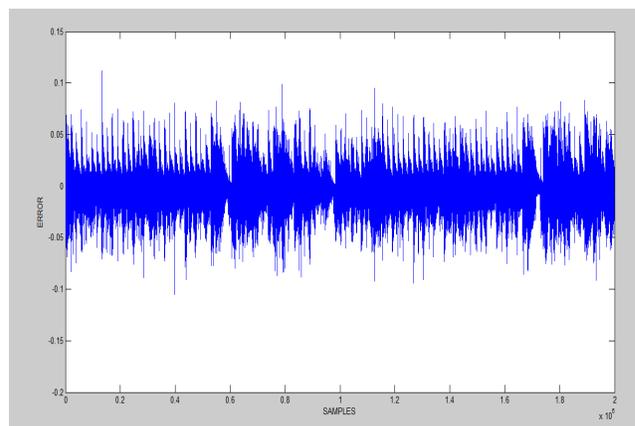


Figure43 Plot of ERROR vs. SAMPLES.

Error in case of JPEG decrypted wave file varies from -.01 to +.01.

4.2 ORIGINAL WAVE FILE Vs. SOUND MATRIX OBTAINED FROM TIF FILE.

Column matrix obtained from TIF file is plotted against original wave file matrix using plot () function.

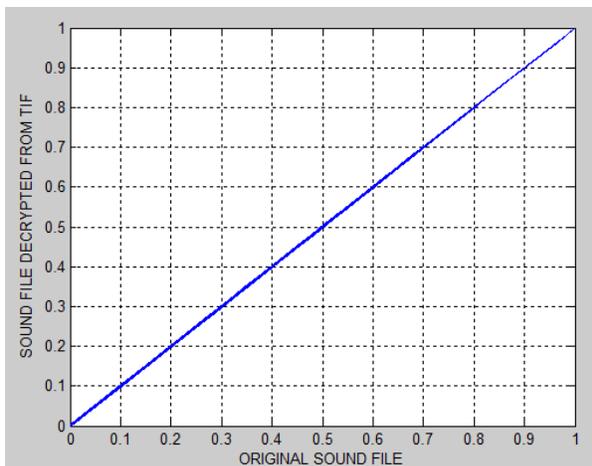


Figure 54 Plot of TIF decrypted sound file and original sound file.

The graph obtained is a straight line of type $y=mx$ such that $m=1$. This implies that the sound file is exactly similar to the one obtained from TIF file format [15]. Using Equation A, we find that the error in this case is within a range of .0002 to -.0002.

Figure 65 Range of error lies from -.0002 to .0002.

Thus TIF images encrypt sound files without compressing or hampering the data in them.

4.3 ORIGINAL WAVE FILE Vs. SOUND MATRIX OBTAINED FROM PNGFILE.

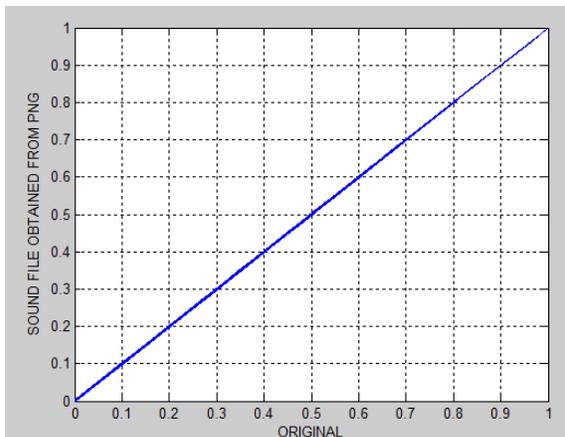


Figure 76 Plot of PNG decrypted sound file and original sound file.

Column matrix obtained from PNG file is plotted against original wave file matrix using plot () function. Error in this case is same as that in TIF decrypted sound.

5. DISCUSSION AND CONCLUSION

Following table summarises the results obtained in this paper.

TABLE III

	Image Type	Range of Error	Discussion
1	JPEG	-.05 to +.05	JPEG file stores a sound file of 3.81 MB in less than 300kb but the sound quality is badly deteriorated. If sound quality can be compromised then JPEG can do best wave compression
2	TIF	-.0002 to .0002	TIF format stores a 3.81 MB long wave file in around 1.6 MB with negligible error and the sound quality is perfect.
3	PNG	-.0002 to .0002	PNG just like TIF stores data with negligible error however the space occupied by it is far less as compared to TIF. It stores sound files without hampering the sound quality to a significant extent.

This method can be used for secured data transfer over networks wherein the entire image file containing the encrypted sound file would be arranged in a haphazard manner (or puzzled) and the retrieving end could be provided with the algorithm to extract and the sound file from the complex array [10].

REFERENCES

- [1] Definition of WAVE file format. Available At: <http://en.wikipedia.org/wiki/WAV>
- [2] Description of various image formats and compression methods. Available at: http://en.wikipedia.org/wiki/Image_file_formats
- [3] Overview of compression losses in various file formats. Available at: <http://www.scantips.com/basics09.html>
- [4] MATLAB syntax definition for reading WAVE file formats. Available: <http://cens.ioc.ee/local/man/matlab/techdoc/ref/wavread.html>
- [5] Elaborate description of grayscale and RGB images and their handling in MATLAB. At: <http://www.getreuer.info/tutorials/matlabimaging>
- [6] MATLAB syntax definition for writing image files. Available: <http://www.mathworks.in/help/matlab/ref/imwrite.html>
- [7] Description of conversion of matrices into “double” datatype: <http://www.mathworks.in/help/images/ref/im2double.html>

- [8] MATLAB syntax definition for creating WAVE files. <http://www.mathworks.in/help/matlab/ref/wavwrite.html>
- [9] Abraham A., Jain R., Sanyal Sugata. and Han S.Y, SCIDS: A Soft Computing Intrusion Detection System, 6th International Workshop on Distributed Computing (IWDC 2004), A. Sen et al. (Eds.) Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326. pp. 252-267, 2004.
- [10] R. A. Vasudevan, A. Abraham, Sugata Sanyal, D.P. Agarwal, "Jigsaw-based secure data transfer over computer networks", Int. Conference on Information Technology: Coding and Computing, pp. 2-6, vol.1, April, 2004.
- [11] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", Annals of Faculty Engineering Hunedoara International Journal of Engineering; scheduled for publication in Vol. 10, Issue 1, February, 2012. ISSN: 1584-2665.
- [12] Description of conversion of RGB images into grayscale image. <http://www.mathworks.in/help/images/ref/rgb2gray.html>
- [13] Animesh Kr Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal and Sugata Sanyal, RISM - Reputation Based Intrusion Detection System for Mobile Ad hoc Networks, Third International Conference on Computers and Devices for Communications, CODEC-06, pp. 234-237. Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006, Kolkata, India
- [14] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications.
- [15] Che-Wei Lee and Wen-Hsiang Tsai, "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme", Pattern Recognition and Machine Vision, River Publishers, Aalborg, Denmark, pp. 1-14.
- [16] R. Poornima and R. J. Iswarya, "An Overview of Digital Image Steganography." *International Journal of Computer Science & Engineering* (2013), pp. 23-31.
- [17] Nosrati Masoud, Ronak Karimi, Hamed Nosrati, Ali Nosrati, "Taking a Brief look at steganography: Methods and Approaches", *Journal of American Science*, vol.7, Issue 6, 2011, pp. 84-88.
- [18] Dastoor, Sarosh K. "Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices", (WICT), 2011 World Congress on Information and Communication Technologies. IEEE, 2011, pp. 279-284.
- [19] Shital C. Patil, R. R. Keole, "Cryptography, Steganography & Network Securities", "International Journal of Pure and Applied Research in Engineering and Technology", 2012; Volume 1(8): pp. 9-15
- [20] Elis Horowitz, Sartaj Sahni, Dinish Mehta: Fundamentals of Data Structures in C++, 2nd ed. Silicon Press, 2006.
- [21] Nick Nabavian, CPSC 350 Data Structures Image Steganography, 2007, <http://www1.chapman.edu/~nabav100/ImgStegano/download/ImageSteganography.pdf>
- [22] Dey, Sandipan, Ajith Abraham, and Sugata Sanyal. "An LSB Data Hiding Technique Using Natural Number Decomposition", *IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007. IHHMSP 2007*, vol.2. 2007, pp. 473-476.
- [23] Animesh Kr Trivedi, Rajan Arora, Rishi Kapoor, Sudip Sanyal, Sugata Sanyal, "A Semi-distributed Reputation Based Intrusion Detection System for Mobile Adhoc Networks", *arXiv preprint arXiv:1006.1956*(2010).
- [24] Bhadauria, Rohit, and Sugata Sanyal. "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques." *arXiv preprint arXiv:1204.0764* (2012).
- [25] Cui, Zhihua, Chunxia Yang, and Sugata Sanyal. "Training artificial neural networks using APPM", *International Journal of Wireless and Mobile Computing* 5.2 (2012): 168-174
- [26] Dey, Sandipan, et al. "Data Hiding Techniques Using Prime and Natural Numbers." *arXiv preprint arXiv:1003.3672* (2010).
- [27] Bibhash Roy, Suman Banik, Parthi Dey, Sugata Sanyal, Nabendu Chaki, "Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services", *Journal of Emerging Trends in Computing & Information Sciences* vol. 3, issue 1, 2012

Author Biography



Rahul R Upadhyay is a B.Tech student of Department of Mechanical engineering, BBD National Institute of Technology and Management. He has an interdisciplinary research interest in topics varying from embedded electronics, network security, fluid mechanics and thermodynamics. He has published papers in National as well as International Journals and participated and won several technical awards in national level competitions and conferences.