INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Hybrid Call Security System using Encryption & Steganography

Manmeet Kaur
Assistant Professor, ECE, CEC,
Landran,
manmeetsandhuu@gmail.com

Samreen Sekhon Brar
Assistant Professor, USMS,
Rayat-Bahra University, Mohali,
samreensekhon14@gmail.com

Namrata Chopra
Assistant Professor, ECE, CEC,
Landran.
Namrata.ece@cgc.edu.in

Abstract— Most of the users use internet for various voice or video calling applications. Also many companies utilize these applications for their corporate calls (inbound/outbound business calls) with the users outside of their network. To achieve the goal of voice communication security, a number of audio security and audio processing algorithms are in use individually or in a combination to provide the effective voice security. Hacking attacks on these applications can cause great losses to the user security which can lower the number of active users and so the business popularity. In the proposed voice call security model, we have proposed a hybrid approach using compression, encryption and steganography to enable to highest level of security in the voice calling while adding the minimum possible delay in the voice packets delivery. Our proposed framework focuses on the security of voice communications, which can take place over a wired phone, cellular connection or internet. The proposed framework consists of three major components to secure the voice communications over internet or intranet i.e. band pass filter, cryptography or steganography. The voice signal would be decomposed using band pass filters, followed by application of cryptography on all of the bands. All of the signal components after decomposition and encryption would be combined and placed in another voice signal using steganography method. This framework have designed to provide multi-layer security to the sensitive voice calling channels between the VVIP, VIP and other important personal of the nation. The results have proved the effectiveness of the system. The system had been tested for its security level, possibilities of breaching attacks, accuracy, noise (WGN) reduction, compression levels, encryption levels, elapsed time and many other aspects. The proposed framework has proved to be effective in all situations related to the voice communication security.

Keywords— voice call security, encryption, steganography, cellular security, robust cryptography.

I. INTRODUCTION

With the fast growing network, many people utilize the various applications to transfer digital data which contains voice, video, image, text files and other forms of digital data. When it comes to the voice communications over the internet, security of voice communications becomes the extremely important for military, security agencies or political talks on phones or internet. Most of the users use internet for various voice or video calling applications. Also many companies utilize these applications for their corporate calls (inbound/outbound business calls) with the users outside of their network. To achieve the goal of voice communication security, a number of audio security and audio processing algorithms are in use individually or in a combination to provide the effective voice security. Hacking attacks on these applications can cause great losses to the user security which can lower the number of active users and so the business popularity. Now-a-days users access these applications from their portable devices (smart phone, tablet, etc.). To prevent the hacking attacks on those web or mobile application architectures, there is various data security mechanism for voice, image, video, and text data. These existing security mechanisms are either using encryption or steganography, or their combinations. There is various securable and perfect system of image encryption that can be well protected from unauthorized access [1]. When it comes to the image transfers over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. To achieve the goal of image security, a number of voice call security or voice encryption algorithms are in use individually or in a combination to provide the effective voice calling security. But these existing voice security mechanisms fail to provide the best voice security and sometimes proved to be breakable or hack-able.[1]

The algorithms usually used for the Voice security purpose are encryption and steganography. For the encryption of audio, we use a variety of symmetric or asymmetric algorithms like Blowfish, AES, DES, etc.[13] Symmetric key encryption uses same key to encrypt an decrypt, whereas asymmetric key algorithms uses different keys for encryption and decryption. For voice security, blowfish is considered the best encryption algorithm. It is fast and reliable and provides the security at core.[14]

Steganography is a security mechanism which is used to hide the message into another object which may be a text, audio, audio, video etc. The techniques used into the steganography are spatial domain method and Transform domain method [2][3]. Steganography comes into fashion to hide the text into text, audio into audio, text into audio, text or audio into audio, audio in to audio, audio into video, etc.

Audio compression is an additional function, which can be applied on the audio to lower their memory size. Memory size is decreased (compression) in case audio is of larger size and it becomes difficult to transfer it over the internet using an internet connection. The known and popular algorithms used for the data compression are DFT, FFT, DCT, DWT, etc.[1]

Steganography is used to hide the secret data into another data. Spatial Domain Method and Transfer domain Method are most popular steganography methods. Spatial Domain Methods embed the information directly into the cover object to create the stego object, whereas Transfer domain method embed the data based on the frequency analysis, which seems more secure and more undetectable. Spread Spectrum based Transform domain method or DWT based Transform domain methods are considered best among others. [5]

II. **RELATED WORK**

Liebchen, Tilman, et al. (2005) have proposed the MPEG-4 audio lossless coding (ALS) standard-Technology and applications. MPEG-4 Audio Lossless Coding (ALS) is a new extension of the MPEG-4 audio coding family. The ALS core codec is based on forward-adaptive linear prediction, which offers remarkable compression together with low complexity. Khalifa, Othman O., Sering Habib Harding, and Aisha-Hassan A. Hashim (2008) have worked on Compression using Wavelet Transform. In simple words, bandwidth cost money, therefore, the transmission and storage of information becomes costly. However, if authors can use less data, both transmission and storage become cheaper. Further reduction in bit rate is an attractive proposition in applications like remote broadcast lines, studio links, satellite transmission of high quality audio and voice over internet. Cunningham, Stuart, Vic Grout, and John McGinn (2005) have proposed a framework named as Play it Again, Babbage. This Framework is used to Exploit Musical Repetition for High-Quality Audio Compression. This paper proposes new methods of compression based on the frequently fundamental compositional element of repetition within music. By exploiting the musical content of a piece of audio, data can be discarded that is perceptually redundant, without the removal of frequency components and variable rate encoding found in other compression techniques, such as MP3. Frameworks for new method of compression are presented and several techniques considered, as possible solutions to the problem of implementing an effective process of data reduction. Rivero, Cristobal, and Prabhat Mishra (2008) have conducted a case study upon Lossless Audio Compression. This paper investigates improvements to the Free Lossless Audio Codec (FLAC), one of the best lossless audio formats, by conducting tests on nineteen quality benchmarks. Eman A. Al-Hilo, Rusul Zehwar (2014) has proposed the fractal compression technique for color images. The data of the color component (R,G,B) are transformed to (YIQ) color space, to take the advantage of the existing spectral correlation to gain more compression. Also the low spatial resolution of the human vision systems to the chromatic components (I,Q) was utilized to increase the compression ratio without making significant subjective distortion. Xiangui Kang, Jiwu Huang (2003) has proposed water marking extraction technique for JPEG compression. In watermark extraction, authors at first detect the template in a possibly corrupted watermarked image to obtain the parameters of affine transform and convert the image back to its original shape. Then they have performed translation registration by using the training sequence embedded in the DWT domain and finally extract the informative watermark.

III. **DESIGN AND IMPLEMENTATION**

Our first goal in this project is the audio compression. Various compression schemes have been studied under the first objective. The major compression schemes evaluated under the preliminary study for this research are DFT (Discrete Fourier Transformation), DCT (Discrete Cosine Transformation) and DWT (Discrete Wavelet Transformation) because of their popularity and effectiveness.[10, 11] For audios, the JPEG audios are taken into account as it preferred DWT over DCT or DFT. [12, 13] In DFT, execution time is lower and it provides lower compression as compare to the other techniques. In DCT is simple compression algorithm, because computation count in this algorithm is limited, hence provides lower compression ratio. DWT on the other hand, is complex and computation count is very high and it provides higher compression ratio as compared to later two and also proven to be more effective. In wavelet transform system the entire audio is transformed and compressed as a single data object rather than block by block as in a DCT based compression system. It can provide better audio quality than DCT, especially on higher compression ratio. [10] After preliminary study of literature based on these compression techniques we evaluated that DWT with HAAR Wavelet is the best performer among all other compression techniques available in our selection in terms of compression ratio and elapsed time. Finally, the decision is made to use DWT and DCT in a combination for its effectiveness and robustness over DCT and DFT.[10, 11]

Algorithm 1: Compression Method

1. The audio is broken in smaller parts, say 8x8 pixels
2. Working from left to right, top to bottom, the DWT is applied to each block
3. Each block is compressed through quantization
4. The array of compressed blocks that constitute the audio is stored in a drastically reduced amount of space.
5. When desired, the audio is reconstructed through decompression, a process that uses the inverse discrete wavelet transform (iDWT).

To perform the encryption in the second object, blowfish encryption algorithm is used to hide the audio details of hidden object.[1,3-4,8] A significant number of research papers on the performance evaluation and work flow of encryption algorithms has been studies under the literature survey part. The AES and Blowfish algorithms were selected in the final short listing of encryption algorithms, because these two provide the best encryption security. [4, 8] Out of the two shortlisted ones, the conclusion was obtained that the blowfish encryption algorithm is considered the fastest one among the all other options. [4] Blowfish encryption algorithm is designed in a customized way to work with audios in MATLAB environment. The algorithm code is designed to perform various rounds of encryption. The encryption algorithm is used here to hide the audio details and to create a new audio with dizzy audio details. The audio details are made hidden in chaotic way to create a new audio with less number of details. The audio is not made completely unreadable because it provokes the hacker to crack into the encryption, whereas a low resolution less detail encryption can be easily mistaken as a bad audio. [3, 8]. The decryption process is the reverse process, which is used to obtain the original audio by using the reverse engineering of the cryptographic process on the receiver’s end. [3] For the decryption, user has to enter the same key as it was entered on the sender’s side while encrypting the audio. The decryption process returns the full resolution original audio from the encrypted audio once the process is complete. [8]

Algorithm 2: Blowfish encryption

Blowfish has 16 rounds.

```
1. The input is a 64-bit data element, x.
2. Divide x into two 32-bit halves: xL, xR.
3. Then, for i = 1 to 16:
4. xL = xL XOR Pi
5. xR = F(xL) XOR xR
6. Swap xL and xR
7. After the sixteenth round, swap xL and xR again to undo the last swap.
8. Then, xR = xR XOR P17 and xL = xL XOR P18.
9. Finally, recombine xL and xR to get the ciphertext.
```

To perform the steganography in the third objective, which is used to embed audio(secret object) into audio (cover object), A number of papers have studied for the selection of best steganography technique for the development of our security model.[5, 6] Steganography is a security mechanism which is used to hide the message into another object which may be a text, audio, audio, video etc. 1-D discrete wavelet transform has been used to perform the decomposition of the audio matrix up to two level decomposition. DB1 or HAAR wavelet is used for the decomposition to compute the 1-D DWT decomposition for steganography.[5, 6] This decomposition will produce four decomposed matrices which include CA (Absolute Coefficient) and CD (Detailed Coefficient) in the first level decomposition.

After applying the compression on the hidden object audio, the very next step is to hide it inside the decomposed cover object. [1, 5-7] The hidden object is hid inside the decomposition matrix of cover object using Transform domain based steganography method. For steganalysis or audio extraction, the stego object undergoes the decomposition using the HAAR wavelet using the similar decomposition process used on the embedding step. [5] The program applies the reverse engineering to extract the audio data from decomposed stego object.

Algorithm 3: Steganography Method

A. At Sender side:

```
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DWT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
```

B. At Receiver side:

Algorithm to retrieve text message:-

```
Step 1: Read stego image
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DWT is applied to each block.
Step5: Each block is compressed through quantization table.
Step6: Calculate LSB of each DWT coefficient.
```

The fourth objective is yet partially achieved by implementing the code for compression and steganography in MATLAB using normal coding in Matlab and Audio Processing Tool Box. The compression module is completed by using 1-D HAAR wavelet for decomposition of audio matrix using Haar wavelet based low pass and high pass filter and results in Approximation Coefficient Matrix and Detailed Coefficient Matrix. Then built-in Matlab function for calculation of threshold using Birge-Massart Algorithm based on 1-D wavelet. This function returns level-dependent thresholds THR and numbers of coefficients to be kept NKEEP, for de-noising or compression. THR is obtained using a wavelet coefficients selection rule based on the threshold average calculation. [14] In next step, the threshold value will been used to perform the compression on the audio matrix. This step returns a de-noised or compressed version of 1-D audio matrix from input audio matrix obtained by wavelet packets coefficients thresholding, again based on HAAR wavelet.

IV. RESULT ANALYSIS

In this research project, our major objective is to improve the voice communication security for the voice communication over internet. To achieve the objective, we have proposed the use of various technologies together with a new and robust compression method. To achieve the objective of voice communication security, we are undergoing implementation of the component techniques in MATLAB environment. We have implemented almost 55% of our research project by implementing the general voice signal compression and almost more than half of the steganography technique. For the compression module, we are using 2-D HAAR wavelet for the voice matrix decomposition and compression on the basis of Birge-Massart Method to find the threshold. The compression algorithm implemented by us has produced good results for compression. We have achieved almost 50% compression ration by implementing the compression.

The above figure is the snapshot of the source being used in the MATLAB software for the proposed research project. The source code has been written in the traditional MATLAB programming language. The built-in functions from MATLAB's signal processing toolbox and statistics toolbox has been used to develop the proposed architecture. Steganography is used to hide the secret data into another data. Spatial Domain Method and Transfer domain Method are most popular steganography methods. Spatial Domain Methods embed the information directly into the cover object to create the stego object, whereas Transfer domain method embed the data based on the frequency analysis, which seems more secure and more undetectable. Spread Spectrum based Transform domain method or DWT based Transform domain methods are considered best among others.

Compression ratio is a parameter, which shows the memory size difference before and after the compression. The compression techniques are used to minimize the memory size of the digital data, which can be used for quick transfers over networks or take less space on local memory of the system. Every program uses a number of variables during the programming cycle. In this research, most of the variables are in numeric form. These variables are used to store the values which undergo various mathematical operations to compute the result. In the above snapshot, all of variables being used in the simulation are displayed.

Index value of signal	**Amplitude Values of various index points in signal vector**			
	Before Compression	**DWT Compressed**	**DCT Compressed**	**After De-compression**
1	**-0.000518**	**-0.000518**	**-0.0294**	**-0.000518**
2500	**-0.000518**	**0.0054**	**0.0091**	**-0.000518**
4000	**0.0170**	**0.0005**	**0.000518**	**0.0171**
4500	**0.0634**	**0.2422**	**0.2422**	**0.0634**
5000	**-0.0986**	**-0.4630**	**-0.4630**	**-0.0986**
5500	**0.0190**	**0.0332**	**0.0332**	**0.0190**
6000	**0.0903**	**-0.0010**	**-0.0009**	**0.0903**
6500	**0.0015**	**0.0000**	**-5.0133**	**0.0015**
7000	**-0.0342**	**0**	**8.3511**	**-0.0342**
7500	**0.2911**	**0**	**3.6027**	**0.2911**
8000	**-0.0513**	**0**	**3.4830**	**-0.0513**
8500	**-0.1846**	**0**	**1.0275**	**-0.1846**
10000	**0.0015**	**0**	**0.0682**	**0.0015**
12000	**0.0009**	**0**	**-0.0222**	**0.0009**

Table 1: The mathematical representation of the signal values in above and below snapshot

The above snapshot is showing the decomposition in clearer picture. We can easily see the original signal, approximation coefficient, detailed coefficient and reconstructed signal. The reconstructed signal and the original signal plotting has been similar visually, which shows the accuracy and effectivity of the steganography module.

Property Names	**Value**
Elapsed Time (Encryption)	0.01211
Elapsed Time (Compression)	0.592924
Elapsed Time (Steganography/Embedding)	0.064531
Elapsed Time (Matrix Reshaping)	0.041362
Elapsed Time (Extraction)	0.013648
Elapsed Time (Decompression)	0.006163
Elapsed Time (Decryption)	0.013695
Total Elapsed Time	0.744433
Peak Signal to Noise Ratio (PSNR)	79.40624
Mean Square Error (MSE)	0.000746

Table 2: The results of proposed algorithm on 1 second data

Property Names	**Value**

Elapsed Time (Encryption)	1.145844
Elapsed Time (Compression)	0.012341
Elapsed Time (Steganography/Embedding)	0.145544
Elapsed Time (Matrix Reshaping)	0.162306
Elapsed Time (Extraction)	0.011133
Elapsed Time (Decompression)	0.036448
Elapsed Time (Decryption)	0.049965
Total Elapsed Time	0.824144
Peak Signal to Noise Ratio (PSNR)	86.071806
Mean Square Error (MSE)	0.000161

Table 3: The results of proposed algorithm on 11 second data

Property Names	**Value**
Elapsed Time (Encryption)	0.012156
Elapsed Time (Compression)	0.656803
Elapsed Time (Steganography/Embedding)	0.074417
Elapsed Time (Matrix Reshaping)	0.045601
Elapsed Time (Extraction)	0.017099
Elapsed Time (Decompression)	0.006630
Elapsed Time (Decryption)	0.014021
Total Elapsed Time	0.826727
Peak Signal to Noise Ratio (PSNR)	91.267163
Mean Square Error (MSE)	0.000049

Table 4: The results of proposed algorithm on 21 second data

Property Names	**Proposed System**	**Proposed System**
Peak Signal to Noise Ratio (PSNR)	79.40624	63.18
Mean Square Error (MSE)	0.000746	1.54

Table 5: Comparison with the Base paper

The comparison with base paper has shown that the proposed system is performing better than the existing system in the base paper. The comparison has been shown on the basis of Mean squared error and peak signal to noise ratio.

V. CONCLUSIONS

In this research we have worked upon the voice communication security model. We have put our effort to create a more robust and faster voice communication security model than the existing ones. This model will add minimum delay in the voice communications to perform various security algorithms on voice data which includes compression, encryption and steganography. We have successfully developed the audio compression module which is able to compress the voice data with 50 percent compression ratio. In addition, we have used the wavelet transform to decompose the voice signal matrix for the steganography purposes. Further development will include the encryption module and completion of steganography module. The new scheme has been proposed for the audio data security using the multi-layer security architecture. The proposed security framework is applying a new technique of compression developed with a combination of discrete cosine transform and discrete wavelet transform. The combination of these two techniques has produced the better results than the existing discrete wavelet transform. The proposed framework performs the blowfish encryption after the image compression. The compression creates a matrix of smaller size than its actual size, whereas the encryption scheme when performed on the compressed signal returns a signal with hidden details, i.e. unreadable or non-detailed. Then the encrypted audio signal is embedded into another audio signal on the basis of transform domain based steganography for another layer of protection. The three layer image security model is capable of providing a robust, strong and uncrack able secure audio. The proposed scheme can be used to ensure the audio security of useful for the important telephonic calls between the top political authorities, top level management, national security personnel and other very important personnel. The proposed algorithm can be embedded at the sender and receiver nodes or in middleware in case of controlled call management architecture. The results of proposed compression technique have been compared with the existing technique on the basis of PSNR and MSE. The proposed technique has been proved better than the existing one. The PSNR value of the compressed audio signal when compared to the original audio signal is recorded higher than the existing system and MSE has been recorded lower than the existing system. This means the proposed system is performing better than the existing system in terms of compression. The proposed system has also been proved quicker and stronger using the various parameters. The major concern of the proposed system was to ensure the security of the system by adding the minimum delay. The objective has been achieved using the unique combination of three security mechanisms (compression, encryption and steganography).

VI. FUTURE WORK

In the future, the technique can be enhanced to produce quick results than the proposed algorithm. Also the proposed technique can be improved to add more security to the important audio call security mechanism. The performance of the proposed technique can be evaluated by comparing it with the other existing audio security mechanisms.

ACKNOWLEDGMENT

All of us are very thankful to the seniors and the people who provide the online solutions for the implementation of this research paper. We are thankful to the colleagues and the specialists on the topic of information security and communications at CEC Landran, Rayat Bahra University and XNS Global, Mohali.

REFERENCES

[1] IngYannSoon, FengZhou, ZhenLi, HaijunLei, Baiying Lei, A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition, Signal Processing, vol. 92, pp. 1985-2001, Science Direct, 2012

[2] Gopalan., “Audio steganography using bit modification”, International conference on Acoustic, Speech and Signal Processing page(s):, vol. 2, 421 -429, IEEE, 2003.

[3] Muhammad Asad, Junaid Gilani, Adnan Khalid “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”, international conference on Computer Networks and Information Technology (ICCNIT), vol. 1, pages 143-147, IEEE, 2011.

[4]Sasan Adibi, A low overhead scaled equalized harmonic-based voice authentication system, Telematics and Informatics, vol. 31, pp. 137-152, Science Direct, 2013.

[5] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions, vol. 1, pp. 1 – 6, IEEE, 2006.

[6] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, vol. 1, pp. 1 – 5, IEEE, 2009.

[7] Raja K B, Chowdary C R, Venugopal K R, Patnaik L M “A Secure Image Steganography using LSB DCT and Compression Techniques on Raw Images”, International conference on session B-image signal processing, vol. 1, pp. 1012-1020, IEEE, 2005.

[8] Hossein Malekmohamadi and Shahrokh Ghaemmaghami, “Reduced Complexity Enhancement of Steganalysis of LSB-matching Image Steganography”, AICCSA, vol. 1, pp. 1013-1017, IEEE, 2009.

[9] Balagi R, Naveen G“Secure Data Transmission Using Video Steganography”, EIT, vol. 1, pp. 1-5, IEEE, 2011.

[10] Andrew D. Ker, “Steganalysis of Embedding in Two Least-Significant Bits”, transactions on information forensics and security, vol. 2, issue 1, pp. 46-54, IEEE, 2007.

[11] S. Suma Christal Mary, “Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream,” International Journal on Computer Science and Engineering, Vol. 02, issue 03, IEEE, 2010

[12] Andreas Westfeld and Gritta Wolf,” Steganography in a Video Conferencing System”, LNCS 1525, pp. 32-47, 1998. Springer, 1998.

[13] Gary C.Kessler, “ An Overview of Cryptography: Cryptographic”, *Handbook on Local Area Network,* ***vol. 1,*** 1999-2014.

[14] Milind Mathur, Ayush Kesarwani, "COMPARISON BETWEEN DES, 3DES, RC2, RC6, BLOWFISH AND AES", NHINT, pp. 143-148, IEEE, 2013.

[15] Katzenbeisser, Stefan and Fabien A.P. Petitcolas (eds). Information Hiding: Techniques for Steganography and Digital Watermarking. Boston,:Artech House, 2000.