Cryptographic Algorithms Analyzing of Different Combination with Secret and Public Key using Text and Audio Files using LabView

Divya Kshetri[1] Mr. Vaibhav Chandrakar[2]
[1]Research Scholar [2]Professor
[1,2]Department Computer Science Engineering
[1,2]Central College of Engineering, Raipur, India

Abstract— This proposed paper focuses on implementing a secure technique that enables to select one of the several text and voice signal show in waveform displayed simultaneously with a unique security key for each text with length using AES algorithm toolbox of LabVIEW and voice sound generating waveform data base. This process involves applying block based logic using of input device and output device, followed by integrating the text, key length and key(hex).AES based algorithm to generated to cipher text block (hex) to convert input text message to encrypted output message .AES based technique and encrypting the text and voice sound with Advanced Encryption Algorithm. With the hex key string specifically generated for the text and voice sound data, the original text is decrypted from multiple cipher text blocks(hex). This method is useful when access permissions need to be restricted to certain viewers and security application and fast technique for cryptography for text and sound signal of a real-time. Voice sound convert and generated to waveform using wavelet transformation frequency domain. LabView and IMAQ vision software package has been utilized to achieve the proposed method of real-time take text input and voice sound signal input for encryption. The use of LabView and AES toolbox present a complete set of text and voice signal processing and acquisition function that improve the efficiency of the project and reduce the programming effort of the user obtaining a better result in shorter time.

Keywords: RT Text and Audio File, AES Algorithms and Advance Signal Processing Tools

I. INTRODUCTION

In this method, the real-time text input and voice signal has been captured from the external device, in this work laptop from a microphone and loudspeaker has used for input of text and voice signal to be encryption, which is then converted into the text convert to cipher block(hex) and voice signal data converted to waveform. Security is the main part of an enterprise which can be achieved by using a combined cryptography algorithms. However, the main purpose of cryptography is not only used to ensure confidentiality, but also to provide solutions to problems such as: hacked integrity, authentication and non-repudiation. In cryptographic systems, the key term refers to a numerical value used by an algorithm to change the information, making that information secure and visible only to individuals who possess the appropriate key for revealing. As a result, the term of key management refers to secure management of keys for making them available to users when they need them. Currently researchers continue to find new algorithms. However, this issue is a very difficult thing because there is a need to consider many factors, such as: security, algorithm characteristics, speed and complexity.

A. Real Time text and audio signal Encryption and Decryption Technique

The paper focuses mainly on text files and audio files. Using the designed system, the text file that needs to be transformed is received as input. The characters of the data file is extracted and converted into ASCII codes. This is then subjected to FFT algorithm to obtain an encrypted file and is ready to be transmitted. The encrypted text file is received as input at decryptor module and decrypted using IFFT algorithm. The whole system is implemented in LabVIEW. In the encryptor module, characters of the data file is extracted, converted into ASCII codes. This is then subjected to FFT algorithm to obtain an encrypted file. The implementation of the DFT on a vector of encrypted samples relying on the homomorphic properties of a cryptosystem is investigated. The process of decryption is the inverse of encryption. The encrypted data is extracted and IFFT is carried out. A fast encryption method based on new fast Fourier transform representation in order to secure the sensitive information within the multimedia data, such as digital images, documents, audio, and video. An encryption-decryption module is also developed in LabVIEW for secure transmission of audio files.

The audio can be input in real time into the encryptor module. Encoding is done using FFT algorithm and the output at each sampling instant can be separately obtained when interfaced with laptop(microphone and loudspeaker). The encryption-decryption algorithms are programmed into the hardware. The output can be listened to using a loudspeaker.

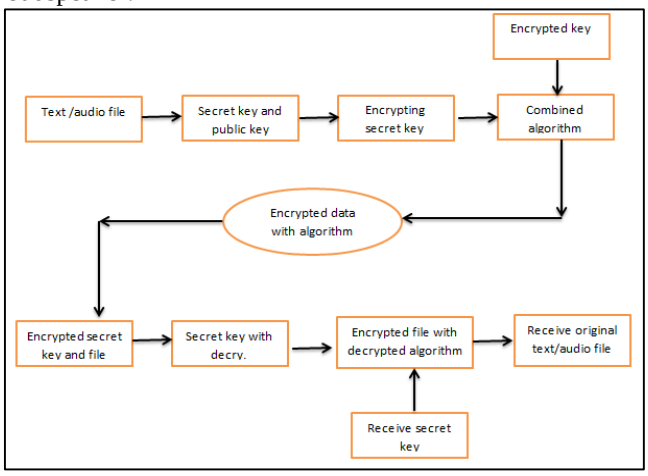

Fig. 1: Block diagram for text and audio signal cryptography

B. NI LabView

The NI LabVIEW stands for National Instrument Laboratory Virtual Engineering Workbench. LabVIEW offers a graphical coding to create an application. It offers a platform for designing a system virtually. It is also called as "G" which refers that coding is to be done in a graph form. LabVIEW

programs are called as virtual instruments because it creates the hardware design/model on software platform. LabVIEW can be categorized into two main programming: Data flow programming and Graphical programming. The components of LabVIEW consist of namely acquisition, analysis and display. The three major aspects are required to complete a VI are,

- Front panel of LabVIEW
- Block diagram of LabVIEW
- Icon/connector

Controls are inputs: they allow a user to supply information to the VI. Indicators are outputs: they indicate, or display, the results based on the inputs given to the VI. The back panel, which is a block diagram, contains the graphical source code. All of the objects placed on the front panel will appear on the back panel as terminals. The back panel also contains structures and functions which perform operations on controls and supply data to indicators. The LabVIEW files are not any text files but they use an extension called Virtual Instrument file or VI file. This VI is only executable in LabVIEW .AES algorithm. Solve the hacking and attack tracing problem of image copyright protection through embedding multiple watermarks option and decryption wavelet Transform is recently adopted technology which is more advantageous than Fourier Transform (FT), as well as Discrete Sine Transform (DST) and the Discrete Cosine Transform (DCT). Wavelet is an algorithm with the components like decomposition, thresholding and reconstruction of the original image. There are tremendous applications in the area of image denoising which are used in scientific and engineering technology fields, medical science, Security and military services

C. Fast Fourier Transform

A fast fourier transform (FFT) is a tool to compute the Discrete Fourier Transform (DFT) of a sequence. The algorithm converts the signal from time domain to frequency domain. Domain conversion enhances data security.
Let x0,…....., xN−1 be the set of N complex numbers which needs to be transformed. The DFT is defined by the formula,

$$x_n=(1/N)[\sum_{n=0}^{N-1}\left(X_k e^{i2\pi kn/N}\right)],\ n=0,1,..,N-1$$

Similarly, in case of Inverse Fast Fourier Transform (IFFT), the formula is given as follows,

$$X_k=\sum_{n=0}^{N-1}\left(x_n\, e^{-i2\pi kn/N}\right),\ k=0,1,.....N-1$$

IFFT which is employed at the decryptor side converts A Text file Encryption The basic operation in text file encryption can be illustrated as a process of encryption in the encryptor module, transmitted through a communication frequency domain back to time domain. Medium to the decryptor module and the retrieval of the original text file at the output of decryptor module. The algorithm used is that of FFT and IFFT.

The encryptor module provides the facility of encrypting a text file, i.e. converting it into a nonreadable form. The text file that has to be encrypted is first created. The location of this file is provided. Each character of the data is extracted and is further converted into ASCII codes. The codes are subjected to FFT algorithm for further encryption. A series of complex numbers are produced as the result. The output obtained after carrying out the FFT algorithm is the required encrypted output. The encrypted output is saved and stored

The Decryptor module is the other vital part of the application where the encrypted text files are received from encryptor. The decryptor module designed for the application avail the cryptographer with user friendly and security options. Initially, the user needs to provide the path or file location of the data that has been encrypted to so as to convert it intoreadable form or retrieve it back to its original form.

The next step is to extract all the coded characters from the required file. The file is then made to undergo IFFT algorithm. The output of this is the required decrypted output data. This is then displayed, saved and stored. Thus the outputs of both 8-bit and 16-bit encryption techniques can be observed. The complexity of the block diagram increases with FFT size. Thus a text file of larger size can be effectively and efficiently manipulated as and when required.

D. Audio Encryption

Audio encryption-decryption processes are also carried out in Figs 6 and 7 by employing FFT-IFFT techniques respectively. Audio is acquired in realtime by making use of the microphone of the computer. It is encrypted using FFT and send to myRIO via Wi-Fi hosted by it. The decryptor block programmed into the device will receive the encrypted audio and decrypts it. The output can be listened using a headset attached to myRIO. myRIO can be interfaced either by connecting directly to the computer using a USB connector cable or by connecting laptop device(loudspeaker, mircophone)encryption and decryption using FFT and IFFT algorithm is implemented in LabVIEW. Both 8-bit as well as 16-bit FFT-IFFT algorithms are carried out and outputs are verified. The domain conversions provide more security. Thus any text file can be efficiently encrypted and decrypted using this technique.

Protection of audio from eavesdroppers play a critical task for the technologist. In this project, audio input is taken in real time. The encryption and decryption mechanism is implemented using in myRIO-1900.The decrypted output can be listened to, from the audio output pin of myRIO-1900 using a headset. Thus the real time audio input can be directly Processed.

II. LITERATURE SURVEY

FlorimIdrizi,et al, proposed a Security is the main part of an enterprise which can be achieved by using a combined cryptography algorithms. However, the main purpose of cryptography is not only used to ensure confidentiality, but also to provide solutions to problems such as: hacked integrity, authentication and non-repudiation. In cryptographic systems, the key term refers to a numerical value used by an algorithm to change the information, making that information secure and visible only to individuals who possess the appropriate key for revealing. As a result, the term of key management refers to secure management of keys for making them available to users when they need them. Currently researchers continue to find new algorithms.

However, this issue is a very difficult thing because there is a need to consider many factors, such as: security, algorithm characteristics, speed and complexity. [1]

Hardjono, et al RC4 stream cipher most preferred Stream cipher algorithm. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process of algorithm, mean RC4 basically two stages process. In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext andcipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage.[2]

Sudha Rani. K, et al. proposed" Text file encryption using FFT technique in Lab VIEW 8.6" In the proposed method, , The advantage of asymmetric over symmetric key encryption, where the same key is used to encrypt and decrypt a message, is that secure messages can be sent between two parties over a non-secure communication channel without initially sharing secret information. The disadvantages are that encryption and decryption is slow, and cipher text potentially may be hacked by a cryptographer given enough computing time and power. One very important feature of a good encryption scheme is the ability to specify a 'key' or 'password' of some kind, and have the encryption method alter itself such that each 'key' or 'password' produces a unique encrypted output, one that also requires a unique 'key' or 'password' to decrypt. This can either be a symmetric or asymmetric key[3]

SRUTHI S et.al proposed a data encryption is employed to provide security to confidential data which thereby denies any unauthorized access. In this project, an efficient design is implemented to encrypt any text file and decrypt it using FFT and IFFT algorithms respectively. The design is implemented in LabVIEW software. The basic operations include encryption in encryptor module, transmission through a communication medium to the decryptor module and the retrieval of original text file at the output of decryptor module. A similar encryption-decryption module is also developed for secure transmission of audio files in a realtime scenario by interfacing myRIO hardware.[4]

paper is to discuss on the Shuhaimi bin Shamsuddin, et. Al proposedaimplementation of cryptographic security algorithms forradio telemetry using graphical programming software from National Instruments known as LabVIEW. The telemetry system consists of a remote telemetry station (RTS) and base telemetry station (BTS) for acquiring and monitoring environmental conditions respectively. RTS setup includes a desktop computer integrated with data acquisition system, 1200 bps modem and GP300 Motorola walkie talkie. Meanwhile, BTS is having the same setup as RTS except that it does not have a data acquisition system. The walkie-talkie operating frequency is 477.1 MHz with FM transmission. A combination of One Time Pad (OTP) and Caesar Ciphercryptographic algorithms will be implemented in order to safeguard the information from the eavesdroppers OTP was chosen because it is suitable for low bit rate data.[5]

KundankumarRameshwarSarafet al. proposed Text and Image Encryption Decryption Using Advanced Encryption Standard Due to increasing use of computers, now a day security of digital information is most important issue. Intruder is an unwanted person who reads and changes the information while transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to some formats that is unreadable by an unauthorized person. AES is mainly advance version of data encryption standard (DES). The input (block size Nb, also known as plaintext) of the AES algorithm is converted into a 4 x 4 array, called a state. Four transformations, AddRoundKey, SubBytes, ShiftRows and MixColumns, perform various operations on the state to calculate the output state (the final cipher text). Except for AddRoundKeyeach of these operations are invertible. InvMethod(Method(a)) = a (2) If AddRoundKeyoperates on a variable twice, the variable itself is returned. [6]

Sudha Rani. K,et al. proposed TEXT FILE ENCRYPTION USING FFT TECHNIQUE IN Lab VIEW 8.6Encryption has always been a very important part of military communications. Here we deal with digital transmission technique. Digital transmission is always much more efficient than analog transmission, and it is much easier for digital encryption techniques to achieve a very high degree of security. Of course, this type of technique is still not quite compatible with today's technical environment, i.e. most of the telephone systems are still analog instead of digital; most practical digitizers still require a relatively high bit rate which cannot be transmitted via standard analog telephone channels; and low bit rate speech digitizers still imply relatively high complexity and poor quality. Digital transmission adopts "Scrambling" technique. Scrambling methods are considered as important methods that provide the communication systems a specified degree of security, depending on the used technique to implement the scrambling method. There are many traditional scrambling methods used in single dimension such as time or frequency domain scrambling.[7]

Israa H. Latif1,etal.software implementation of the hybrid cryptosystem which consists of the Symmetric-key algorithm AES-256 and the secure hash algorithm SHA-2 256 is presented using the VI LabVIEW environment toolkit. The idea of the proposed Hybrid Cryptosystem is to use the SHA-256 bit as a key generation for AES-256 in order to improve the data security to a greater extent because it provides higher security in terms of complexity. The proposed hybrid cryptosystem is implemented using LabVIEW 2013, and from the simulation results obtained, we see the simplicity in modeling AES-256,SHA-256 and the complete hybrid cryptosystem, the results show two cases, the first case is how we can use the same input messages(plain text of AES-256 is the same as the input message to SHA-256), and the second case with different input messages (plain text of AES-256 is not the same as the input message to SHA-256). And from these results we see that the output results

will be the same for the compelete hybrid cryptosystem in the two cases.[8]

Shelveenpandeyet al. Different image encryption and decryption technique and KA image cryptography. It additionally focuses on the functionality of Image encryption and decryption techniques and a KA encryption technique. KA Image cryptography is new approach in image cryptography which will be very helpful to improve image encryption. KA Technique Encrypt the image in two steps. First apply different operation on image rows and column wise pixels. And then divide whole image in Different parts and then apply different operation[9]

Davis et al proposed a paper for data security is an essential part of an organization; it can be achieved by the using various methods. In order to maintain and upgrade the model still efforts are required and increase the marginally overheads. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. The information about the key is present in the encrypt data which solves the problem of secure transport of keys from the transmitter to receiver In case of practical system encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format cipher text with the help of key [10].

RinkiPakshwar, et al. A Survey on Different Image Encryption and Decryption Techniques. New image encryption technique based on a new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rossler chaotic system. From Experimental analysis, they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first, a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image. [11].

Kaladharan N et al. Unique Key Using Encryption and Decryption of Image. Encryption and decryption attain by single key is the previous finest technique of image security. Single key assigned for image encryption and it is encoded. Then the key is sent via secure way for decryption purpose. Subsequently, the key is safely received and apply the decryption process and obtain the original image. The encrypted part is used to conceal the information of the image. This instant no individual can perceive the information. Decrypt part is utilized the secret information to unlock and a layup as an original image.[12]

Tejaswini B. et.al. a proposed method "A Survey on Different Image encryption techniques" proposed an Image Encryption Using Block-Based Transformation Algorithm. Here a block-based transformation algorithm and Blowfish algorithm was used for encryption and decryption. First, the original image was divided into blocks; it is then rearranged into a transformed image using a transformation algorithm and then the Blowfish algorithm was used for encryption. It was observed that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. Experimental results showed that a direct relationship between a number of blocks and entropy and an inverse relationship exists between the number of blocks and correlation.[12]

III. PROBLEM IDENTIFICATION

Cryptography algorithms to secure management of keys for making them available to users when they need them. Currently researchers continue to find new algorithms. However, this issue is a very difficult thing because there is a need to consider many factors, such as: security, algorithm characteristics, speed and complexity.

They can be categorized into Symmetric (secret) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key. DES uses one 64-bits key. Triple DES uses three 64-bits keys while AES uses various 128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys. The most common classification of encryption techniques.

Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simply because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput. However, Hill cipher succumbs to a known plaintext attack and can be easily broken with such attacks. This paper suggests efficient methods for generating a self-invertible matrix for Hill Cipher algorithm. These methods encompass less computational complexity as an inverse of the matrix is not required while decrypting in Hill Cipher. This proposed method for generating self-invertible matrix can also be used in other algorithms where matrix inversion is required. Although the algorithm presented in this project aims at image encryption and decryption, it is not just limited to this area and can be widely applied in other information security fields such as text and audio encryption. This provides the security against the different attacks like brute-force attacks. Proposed Advance Hill algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm. A Brute Force Attack requires 27+8*(n / 2)2 number of key generations; where n is the order of key matrix. Advance Hill is a fast encryption technique which can provide satisfactory results against the normal hill cipher technique. The proposed scheme is resistant against known

plaintext attacks. So the image encryption with Advance Hill cipher is quick response encryption scheme.

This purpose, the application of cryptographic methods represents the main condition to enable a secure business communication. Due to the massive electronic communication the importance of cryptography is significant: sending sensitive data, and distance access to various information systems. On one hand, our analysis prove that secret key algorithms (AES) are faster than public key algorithms.

IV. METHODOLOGY

The proposed methodology of this paper based on digital signal processing tools and an advanced encryption standard algorithm based. Presented in this section is performed by a tab control. A tab control text window using a input message text format using AES algorithm key length(128,256) and key format alphanumerical and generated to cipher text block for hex codes to convert to output message. Second tab control report generation window using real time audio signal to convert waveform and save to data to graph form and save real time sound to data file

Third tab control is sample read is reading to output signal and wave from and send to webpage. The http file send to server side and send to data to receiver end .

A. Text Control Window

The basic operation in text file encryption can be illustrated as a process of encryption in the encryptor module, transmitted through a communication medium to the decryptor module and the retrieval of the original text file at the output of decryptor module. The algorithm used is that of AES algorithm to text file converting to the using of key(hex) and key length(128,256) to convert cipher text block (hex) convert input message to output message.

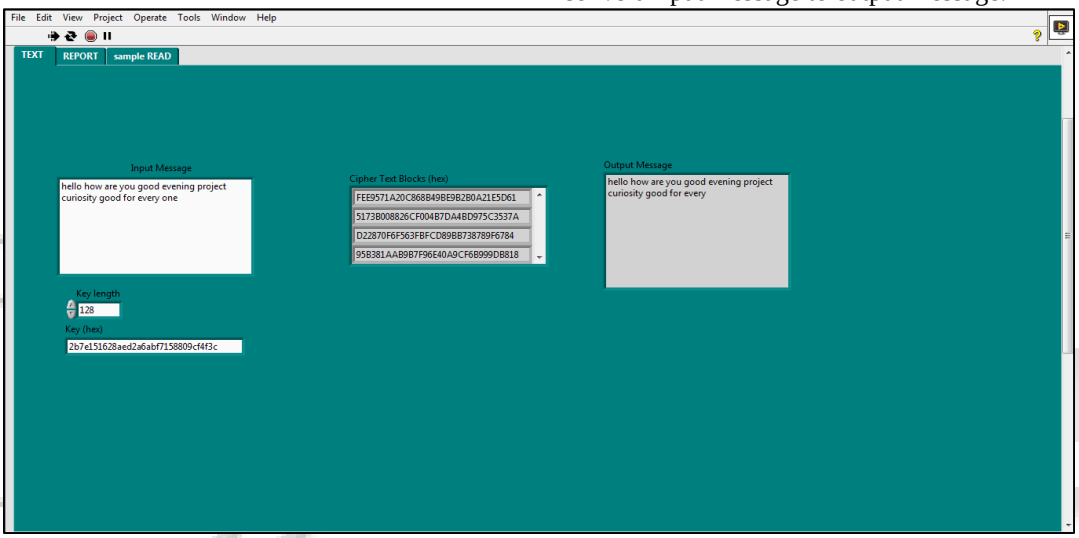

Fig. 2: Front panel of text file windows

Showing the front panel of text file encryption and decryption window, where message is entre in text for mate which define the key (128, 256 bit) and alpha numeric key will generate using AES algorithm. Here cipher text block (hex) will be create and the encrypted message will be sent to receiver end as output message.

B. Report Generation Windows

External sound is given as input which is converted to wave form as shown in the figure 3 and this will be transfer as ecrypted data to receiver end. The first graph shows input audio signal which could be taken from the mic input of laptop or any other input device and the second graph shows show the receiver end signal.

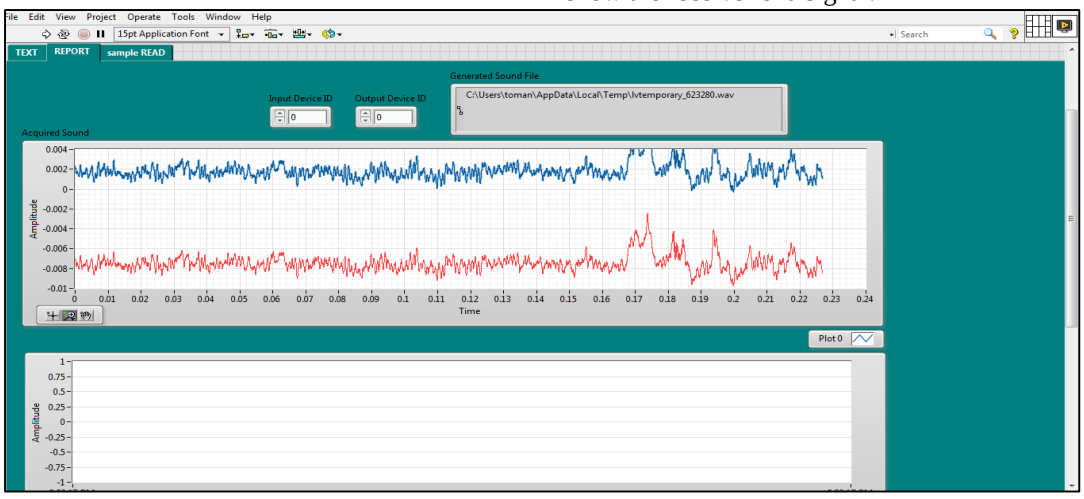

Fig. 3: Front panel Audio signal waveform generation

Therefore, it seems necessary to develop a complete library of functions, programs and tools tailored to specific programming environments, which would give the application or system developer the opportunity to design and simulate secure and safe distributed measurement system in an easy and intuitive way. These additives should help to ensure safe transmission of data in any communication infrastructure and the creation of mechanisms for authentication and integrity of both measurement and control data. In the previous work, the authors have analyzed the LabVIEW environment capabilities for efficient implementation of cryptographic algorithms .The next phase of the work, described in this paper, is to develop new mathematical tool for LabVIEW environment - a Large Number library (also known as Big Integer or arbitrary length integer library). This library allows for the computation on numbers with arbitrary (within the limits of available memory) number of decimal digits, far exceeding the typical representation in computer systems (32 or 64bit). Large numbers are widely used in many popular cryptographic algorithms, including RSA, Rabin or ElGamalpublic-key encryption systems, used for both, data encryption and the generation of secure digital signatures. The LN library in addition to basic arithmetic operation includes operation modulo N in the suitable rings or finite bodies, functions for calculating the opposite element in such algebras and primality test algorithms.

V. RESULT OF REAL-TIME TEXT AND AUDIO SIGNAL CRYPTOGRAPHY

The proposed AES algorithm is applied to a sample real- time text and audio signal enter and recode text and audio signal which has been taken from laptop device 0&1(microphone and loudspeaker) itself in .txt file and .wav file. The proposed algorithm shows a good secret key encryption ability since the original sample text and audio signal its corresponding encryption and decryption process for cryptography looks quite identical. The performance of the proposed algorithm is used to hiding/encrypted the defense data with high security.

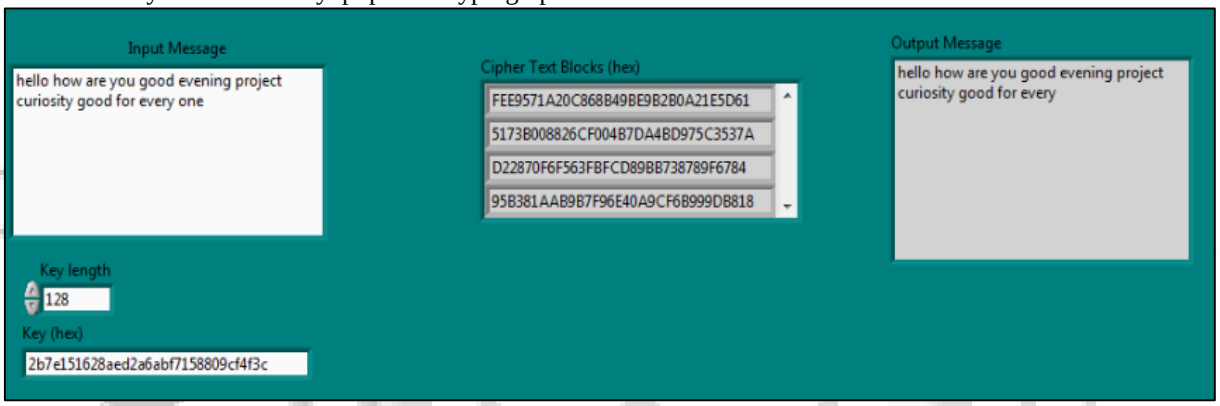

Fig. 4: Labview program front panel (GUI) Using text key

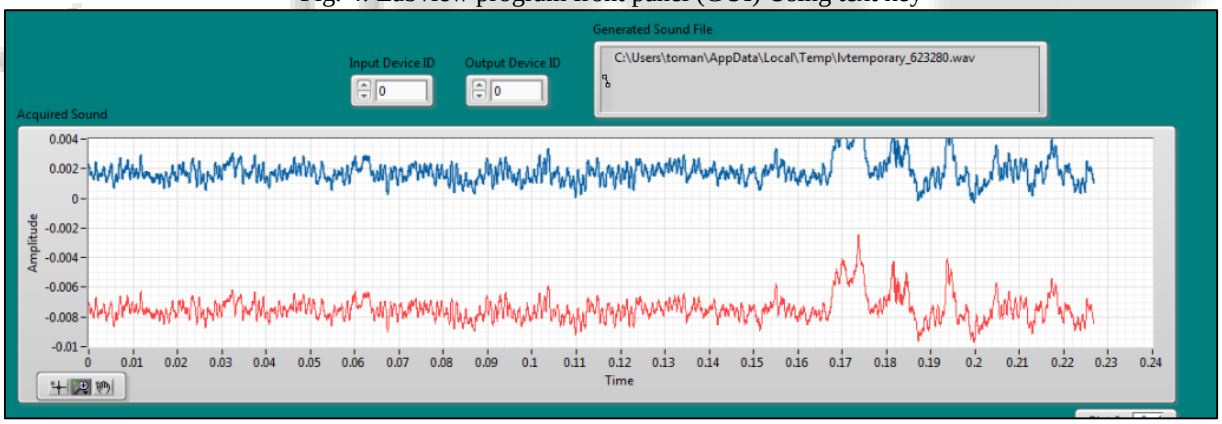

Fig. 5: Labview program front panel (GUI) select File device

Algorithm	Key Size (bits)	Block Size	Type	Features
RSA	1024	128	Block Cipher	Asymmetric algorithm, speed is low
Blowfish	32- 448	64	Block Cipher	Excellent Security
AES	128	128	Block Cipher	Replacement for DES, Excellent Security
DES	64	64	Block Cipher	Most common, Not Strong Enough
Triple DES	192	64	Block Cipher	Modification of DES, Adequate Security

Table 1: Comparison of various encryption algorithms on the basis of Key size and Block size, Type and Features

From the above results, it can be found that the proposed method of AES algorithm for cryptography encryption as performed well as compare to propose in others all algorithm. The encryption time has taken for comparison and it has been found that time taken value is lesser in this proposed method and showing excellent security.

VI. CONCLUSION

The proposed algorithm in all papers is applied to a sample text and audio signal which has been taken from laptop(loudspeaker and microphone). The proposed algorithm shows a good cryptography ability since the original sample text and audio and its corresponding encryption and decryption text and audio looks quite identical. The performance of the proposed algorithm is used to hiding/encrypted the defense data with high security. The application designed provides a very high security in transmission of a text file. This application can be used as an effective technique in programming scenarios to secure vital codes and secure transmission in research departments. The application possesses immense scope for further development.

The development relies on the factors providing transmission security. The application can be further designed for word documents and other types of text files (pdf, word document, etc).Text file encryption and decryption for 8-bit and 16-bit is carried out and their respective outputs are verified. The audio input is taken in real time whose encryption-decryption process is carried out and final audio output

REFERENCES

[1] Florim Idrizi1, Fisnik Dalipi2, Ejup Rustemi3 "Analyzing the speed of combined cryptographic algorithms with secret and public key" International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.comVolume 8, Issue 3 (August 2013), PP. 45-51

[2] Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005.

[3] KundankumarRameshwar Saraf1 , Vishal Prakash Jagtap2 , Amit Kumar Mishra3 "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014 ISSN 2278-6856.

[4] SRUTHI S, ATHIRA VIJAY, SHEJO JOSE, ATHIRA V "Encryption & Decryption of Text file and Audio using LabVIEW" 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum

[5] Shuhaimi bin Shamsuddin, Dr. MohdDani bin Baba, Dr. Deepak K. Ghodgaonkar ".IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS FOR RADIO TELEMETRY USING LABVIEW" International Symposium on Signal Processing and its Applications (ISSPA)). Kuala Lumpur. Malaysia, 13 - I6 August, 2001. Organized by the Dept. of Microelectronics and Computer Engineering, UTM, Malaysia and Signal Processing Research Centre, QW, Australia

[6] Ajay Kakkar, M. L. Singh, P.K. Bansal, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[7] Sudha Rani. K1, T. C. Sarma2, K. Satya Prasad3 "TEXT FILE ENCRYPTION USING FFT TECHNIQUE IN Lab VIEW 8.6"IJRET: International Journal of Research in Engineering and Technology ISSN: 2319-1163

[8] Phillip L. Reu, William Sweatt, Timothy Miller, and Darryn Fleming, "Camera system resolution and its influence on digital image correlation" SAND2013-8737J.

[9] Mohit Kumar, AkshatAggarwal, AnkitGarg "A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications (0975 – 8887) Volume 96– No.13, June 2014.

[10] Israa H. Latif1, Ergun Erçelebi2 "Implementation of Hybrid Cryptosystem using AES-256 and SHA-2 256 by LabVIEW" International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 1, January 2017

[11] ShelveenPandey, Mohammed Farik "Best Symmetric Key Encryption - A Review", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06, JUNE 2017, ISSN 2277-8616

[12] Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9.

[13] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

[14] KRISHAN GUPTA "DIFFERENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES AND KA IMAGE CRYPTOGRAPHY" International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-10, Dec-2013.

[15] Public Key Infrastructure Overview, By JoelWeise - SunPSSM Global Security Practice, Sun BluePrints™ On Line - August 2001

[16] "Cryptography Basics" available at weblink: http://media.wiley.com/product_data/excerpt/94/07645487/0764548794.pdf.

[17] A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY

[18] Public Key Cryptography - Applications Algorithms and Mathematical Explanations

[19] International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-54207

[20] "Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," Federal Register, v. 56, n. 169, 30 Aug 1991, pp. 42980-42982.

[21] www.ni.com\manual

