DOI: http://dx.doi.org/10.26483/ijarcs.v9i5.6286

ISSN No. 0976-5697

Volume 9, No. 5, September-October 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

VISUAL SYMMETRIC SPEECH CRYPTOGRAPHY

Mr. Sanket Shah
G.H.Patel Institute of Engineering And Technology,Anand,Gujarat,India

Mr.Jainam Shah
Charotar University of Science and Technology, Anand, Gujarat, India

Abstract: — Today Communication is mainly depends upon digital data communication. Data is sent across internet using sequence of bits. Data integrity is major issue in such a communication. To preserve data integrity of the message sent over the internet various method of cryptography is used. Though there are two types of algorithm for encryption namely symmetric [1] and asymmetric [1], This paper is mainly concern with digital symmetric cryptography using image to replace some bits and at the receiver side this encrypted message is decrypted at the receiver side For Encryption block cipher mode [2] is used which is data is encrypted in blocks rather than individual bits. Digital encryption of data is the approach, in which the original data, say x, is first digitized into a sequence of bits, x (k) which are then embedded digitally with the chosen segments of the image file, y (k) before transmission. For this, we have utilized the MATLAB (Matrix-Laboratory) which is a multi-paradigm numerical computing environment and fourth generation programming language. Encryption is a much stronger method of protecting speech communications than any form of scrambling. The ability to securely store and transfer sensitive information has proved to be a critical factor of success in today's day and age. The secrecy as well as integrity of data during storage and transmission has been the motivating factor for us in the build up to this paper.

Keywords: cryptography; digital cryptography; speech cryptography, Block cipher; symmetric cryptography

I. INTRODUCTION

The most common way of communication for humans is through speech or plaintext. There are situations when message is intended for only authorized users. The speech signal or text message is at risk of eavesdropping. Encrypted signal prevent the unauthorized access to the signal over the internet. Encryption in modern times performed by using modern algorithms that have a key to encrypt and decrypt information. Key convert the data into some "digital gibberish" and at the decryption side, this encrypted text is converted to the actual understandable form. Generally longer key have better chance of security. This holds true because deciphering an encrypted message by brute force would require the attacker to try every possible key. For instance, 56-bit key is provide more security than 8-bit key. Cryptography can also be used for user Authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography [1], public-key (or asymmetric) cryptography [1], and hash functions [3]. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted cipher text, which will in turn (usually) be decrypted into usable plaintext [4].This paper is organized in 7 sections. Preamble is about the basics of cryptography. Next section gives Gist of Speech cryptography. Third section consists of Programming Language and functions that are used. Fourth and Fifth section is about our project workflow and results. Finally conclusion and advantages of the project.

II. CRYPTOGRAPHY

Cryptography is a method of transferring the private data onto the open network in a way that only those for whom it is intended can read and process it. It is techniques through which third party hindrance in reading private messages is avoided. Some experts argue that cryptography appeared Spontaneously sometime after writing was invented, with Applications ranging from diplomatic missives to wartime battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications.

In data and telecommunications, cryptography is necessary When communicating over any entrusted medium, which includes just about any network, particularly the Internet.

The following figure gives an idea about the basic components and processes which are an integral part of a cryptosystem.

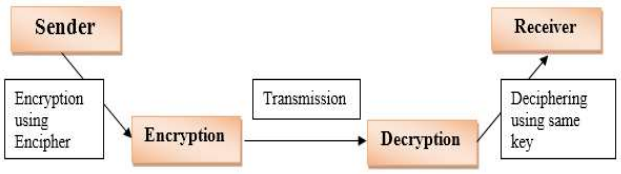


Figure-1 Key Cryptography Components

Plaintext: It is the data to be protected during transmission.
Encryption Algorithm: It is a mathematical process that produces a cipher text for any given plaintext and encryption key. A cryptographic algorithm takes plaintext and an encryption key as input and produces a cipher text.
Cipher text: It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the
Encryption key: The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
Decryption Algorithm: It is a mathematical process, that produces a unique plaintext for any given cipher text and
Decryption key: It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
Encryption Key: A value is known to the sender. The sender

inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.

Decryption Key: A value is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext. [4].

I. Types Of Cryptographic Algorithms:

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. A key is a piece of information that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into cipher text, and vice-versa for decryption algorithm.

The three type of algorithms:

Symmetric-Key Cryptography: Symmetric-key cryptography uses a single key for both encryption and decryption. Encryption and decryption algorithm are inverse of each other [2].

Asymmetric-Key cryptography: It is also called public key cryptography. In public key cryptography, two keys: a private key and a public key is used. Encryption is done through the public key and decryption through private key. Receiver creates both the keys and is responsible for distributing its public key to the communication community [2].

Hash Function (One-way Cryptography): Hash functions have no key since the plaintext is not recoverable from the cipher text. Hash functions are useful to prove message integrity. One can hash the message and display its hash somewhere publicly. When the recipient receives the message they can calculate its hash, compare it with the public one and verify that the message has not been changed.

II. Speech Cryptography:

Secure voice, alternatively known as secure speech or ciphony is a term in cryptography [5] [8] for the encryption of voice communication over a range of communication types such as Radio, Telephone or IP. [6]

Speech encryption is the paramount to any secret speech messages. Speech encryption is performed by analog encryption or digital encryption. Analog encryption is used for enhancing the secure voice signal transmission. It can be incorporated into television, satellite or mobile communication. Whereas digital cryptography. [7][8] Is uses complex techniques for encryption and it is providing greater security.

Speech cryptography can be achieved by many ways. We have used one image to encrypt the block of speech, which is also called block ciphers [1] and same image is used as a decryption key to decode the cryptic message in order to retrieve the actual message. M X N matrices of image will be converted into 1 X (M*N) [10] matrices as we want to use it to compare with ".wav file" for encryption. Image and speech signal, this two binary data streams are now given to the 2-bit encryption algorithm, which will change 12th and 13th bit of '.wav' binary elements. Some important MATLAB functions are presented to better understand the process.

III. SOFTWARE

a) Getting started with MATLAB

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. Typical uses include:

1. Math and computation
2. Algorithm development
3. Modelling, simulation, and prototyping
4. Data analysis, exploration, and visualization
5. Scientific and engineering graphics
6. Application development, including Graphical User Interface building

b) The MATLAB Application Program Interface (API):

This is a library that allows you to write C and FORTRAN programs that interact with MATLAB. It include facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for reading and writing MAT-files.

MATLAB:

- A function is a group of statements that together perform a task. In MATLAB, functions are defined in separate files. The name of the file and of the function should be the same.
- Functions operate on variables within their own workspace, which is also called the local workspace, separate from the workspace you access at the MATLAB command prompt which is called the base

Workspace.

Functions can accept more than one input arguments and may return more than one output arguments.

The following functions have been widely used during the implementation of this project. [9]

Wavered:

Read WAVE (.wav) sound file

dec2bin:

Convert decimal to binary number in string.

Typecast:

Convert data types without changing underlying data.

Single:

Convert to single precision.

Size:

Size of triangulation connectivity list.

Sz = size(TR) return.

Length:

Length of vector or largest array dimension.

Imread:

Read image from graphics file.

elseif:

Execute statements if condition is true.

reshape:

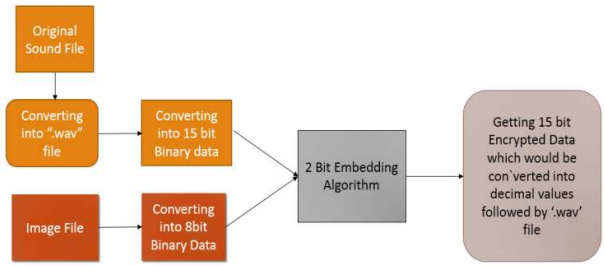
Reshape array.

bin2dec:

Convert binary number string to decimal numberP

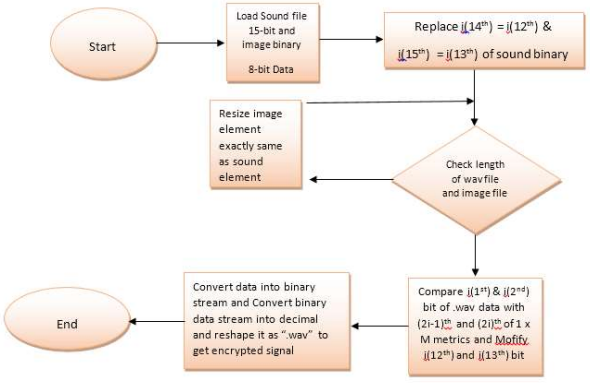
IV. CRYPTOGRAPHY SCHEMES

A. Encryption Work Flow



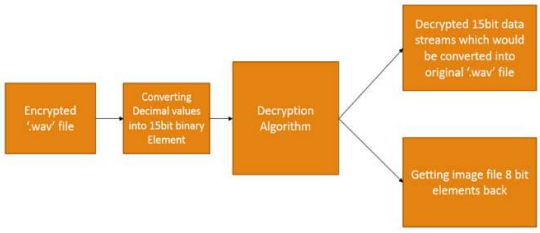
Workflow Chart. 1 Encryption using Image

Block diagram shown above describes briefly how encryption process will be done. First sound file will be fed as an input. Next, A grayscale image file will be taken as encryption key (which plays a vital role to encrypt).Sound file will be now converted to binary elements by using a MATLAB functions. As we are converting it with 15-bit data stream (15 x 1 Metrics). At the same time we are converting gray scale image file into matrices format and then into binary stream. As we are using grayscale image we will be having 2-D matrices (M X N). [8]Now, M X N matrices will be converted into 1 X (M*N) matrices [10] as we want to use it to compare with ".wav file" for encryption. This two binary data streams are now given to the 2-bit encryption algorithm, which will change 12^{th} and 13^{th} bit of '.wav' binary elements. And then we are having 15 bit encrypted data stream which values decimally different from the original '.wav' file and reshaped as a '.wav' file which is to be transmitted.In addition, this encrypted file now can be transmitted and none can decipher it until it matches the decryption table and our sound file is now secured with 2-bit encryption algorithm. And can be aired anywhere into the world without any fear of getting information stolen.



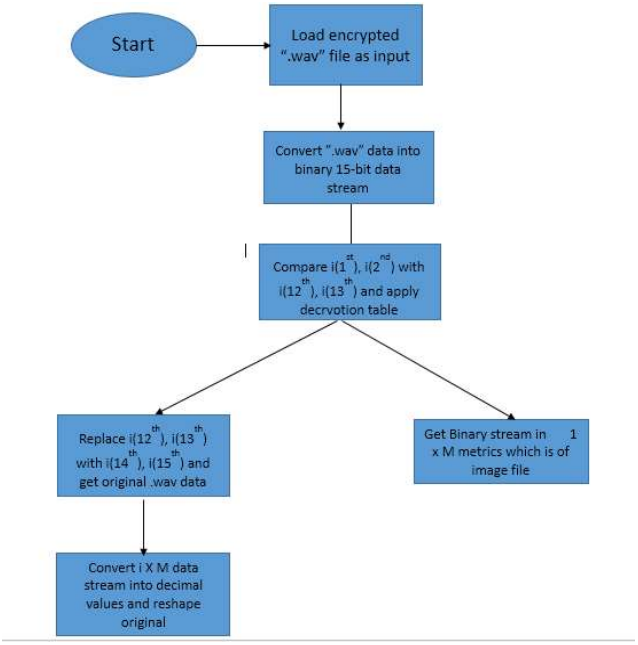
Flowchart .1 Encryption using 2-bit algorithm

B. Decryption Work flow



Workflow chart .2 Decryption process

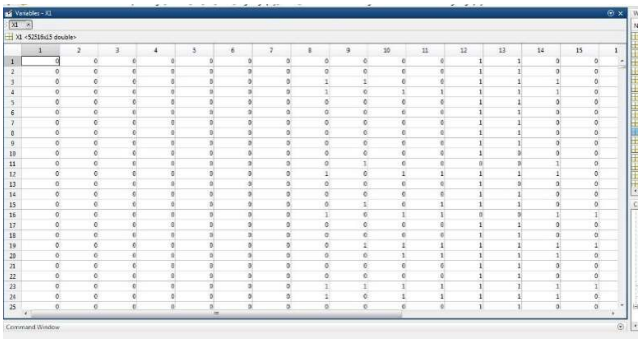
In the Decryption Process, Received encrypted signal now will be taken as an input for a decryption. First, get the element's decimal values of the signal than convert it to binary data streams of 15-bit (15 x I matrices).Apply to the decryption algorithm and we will get image data stream in the form of 1 x M matrices. [9][10].And same time we get the .wav data stream. Convert it to decimal values, reshape it and we can get the original sound file at last. Here, consider LSB of 15-bit data stream is now changed but we are not taking it into account as there is no major change in decimal element value of signal. However, as far as noise is concerned we are getting little bit noise in signal.



Flowchart .2 Getting Original File Using Decryption

V. RESULTS

A. Data Stream after Encryption

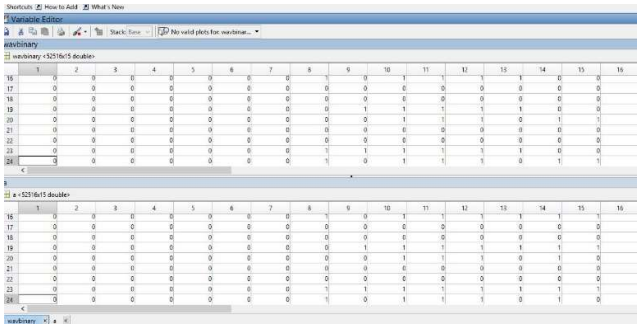


Output Image.1 Encrypted Data Stream

This snapshot shows the embedment of '.wav' file and image file, which would be the encrypted data. 12th and 13th bit of X1 is bit generated after applying algorithm.

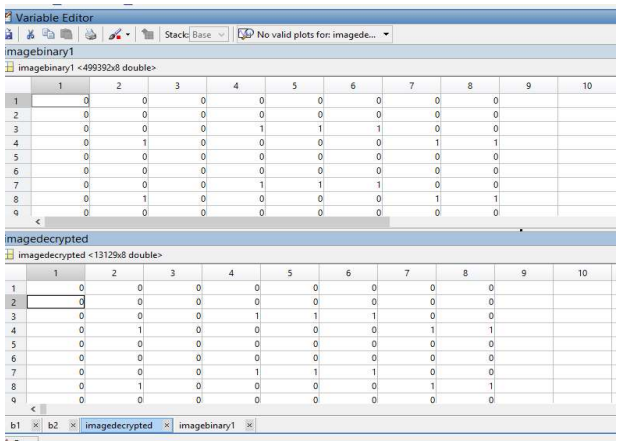
B. Input and Output Data Stream Of '.Wav' File

'Input wavbinary' and 'a' shown in below snapshot is binary data stream of input '.wav' file and output of decrypted file. All elements of 'a' are as same as 'wavbinary' except 14th and 15th bit of stream because Image we have used that bits to hide image data.

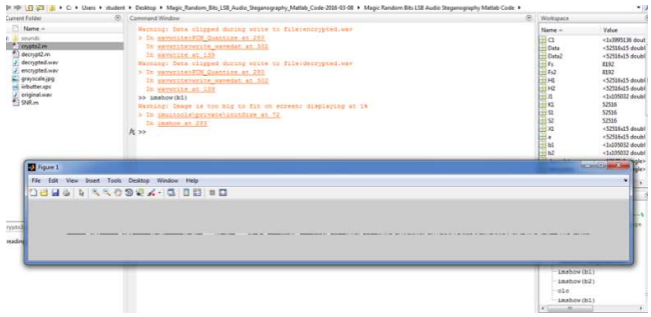


Output image.2 Input/output .wav data stream

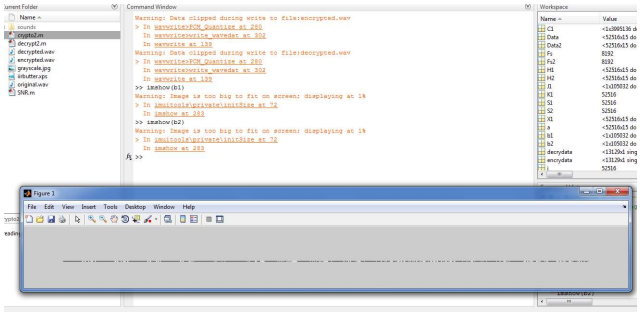
C. Output Data Stream



Output Image.3 Input/output Image Data Stream



Output Image.4 Input Image Elements



Output Image.5 Output Decrypted Image File

'imagebinary1' is a data stream of image file. 'Image decrypted' is a data stream, which we get after decryption.

VI. ADVANTAGES

This research could see widespread utility in military operations. The military as well as government organizations are always interested in cryptography, as it is a secure method of protecting data as well as government secrets. It is also useful on the ground when at war, as it does not leave communication open. Thus by leaving it encrypted, the enemy cannot listen in. One of the first uses of cryptography for military use was the Enigma machine. It was used by the German military force in World War II. It could also find wide usage with various mobile companies. These mobile companies are obligated to keep the information of their users secure and hence need this mechanism in order to ensure the same. Companies such as Blackberry and Apple are prominent examples, which have been in the news for this particular reason. Furthermore, we have employed Symmetric key Cryptography here. So it further adds to the feasibility of this project. As we know, it is also known as shared-key, single-key, secret-key, and private-key and one-key encryption. It has its own benefits. It is relatively fast and simple. It uses less of computer resources.

VII. CONCLUSION

In this research, we tried and tested our hands on sending voice messages efficiently and more importantly, securely. Emerging computer and communications technologies are radically altering the ways in which we communicate and exchange information. Along with the speed, efficiency, and cost-saving benefits of the "digital revolution" come new challenges to the security and privacy of communications and information traversing the global communications infrastructure. In response to these challenges, the security mechanisms of traditional paper-based communications

media, envelopes and locked filing cabinets, are being replaced by cryptographic security techniques. We developed an algorithm of our own for the same and conducted several experiments to check the robustness and efficiency of the cryptosystem, which we had made. Our approach cultivates an innovative idea in embedding different sound files with images. This approach is never explored in the literature, and its advantages are clear and significant. The effectiveness of this scheme is verified through a number of experiments.

VIII. REFERENCES

[1] W Diffie, M Hellman .New Directions in cryptography. IEEE Transactions on Information Theory,IT-22:644-654,1976

[2] Tang Songsheng, Ma Xianzhen, "Research of Typical block cipher algorithm", IEEE national conference, vol. 1, pp. 319-321, Aug. 2010.

[3] Bart Preneel "Cryptographic Hash Functions: Theory and Practices" Springer INDOCRYPT vol. 6498, pp. 115-117, 2010,

[4] Stallings. William, "Cryptography and network security Principles and Practice Second Edition [M]", Beijing: Publishing House of Electronics Industry, 2004.

[5] M. Rajeswara Rao, R.K. Sharma, "FPGA implementation of combined AES-128",IEEE Computing Communication and Networking Technologies(ICCCNT) 2017 8th International Conference on, pp-1-6 , May 2017

[6] Like Zhang, Sheng Liu." Secret Telephone Technology based on information Hiding and Encryption", presented at IEEE International conference on information Acquisition, Weihai, China, Aug. 2003

[7] Pahlavan Tafti A.,Janosepah S.(2011) Digital Images Encryption in Frequency Domain Based on DCT and One Dimensional Cellular Automata. In: Abd Manaf A, Zeki A., Zamani M., Chuprat S.,EI-Qawasmeh E.(eds) Informatics Engineering and Information Science, ICIEIS, 2011. Communications in Computer and Information Science, vol 251. Springer, Berlin, Heidelberg.

[8] A. Kulkarni, Sheetal & B. Patil, Shubhangi, "A Robust encryption method for speech data hiding in digital images for optimized security",Presented at International Conference on Pervasive Computing(ICPC), January, 2015

[9] Bradley, "Programming for Engineers", [Online] Available: https://www.springer.com/in/book/9783652233029

[10] Konstantin Melikhov, Feng Tian,Jie Qiu,Quan Chen, Hock Soon Seah., "DBSC-Based Grayscale Line Image Vectorization.", Journal Of computer science and technology, Volume 1,Issue 2, pp 244-248, , Springer March 2006.

Authors:

Sanket A. Shah was born in Anand City, Gujarat, India in 1997. He is currently pursuing his computer engineering at G.H. PATEL INSTITUTE OF ENGINEERING AND TECHNOLOGY, Bakrol, Gujarat, India. He has attended the national conference, RACST held at his institute in 2016. He worked on testing part of 2-bit encryption algorithm using image. In addition, he has helped in designing the algorithm for visual cryptography using image.

Jainam A. Shah was born in Anand, Gujarat, India in 1995. He received B.Tech degree in Electronics and Communication Engineering from Charotar University Of science and technology, Changa, in 2016.
He is working as a System Engineer at TCS (Tata Consultancy Services), since 2016. He has worked on algorithm design for visual cryptography,also contributed in coding part of the research.