Implementation of Video Encryption using Hill Cipher in Labview

K. Gnana Sushma, BVSSN Raju

Abstract: ***The video encryption is necessary to protect the information from unauthorized viewing, sharing, data breaching and theft. This paper presents video file encryption implementation in LabVIEW. Hill cipher technique is used to encrypt the video file with an asymmetric encryption. The encryption key is different from the key used for decryption since it is an asymmetric encryption. The LabVIEW Vision Acquisition Software is used to obtain images continuously and then save them to a file in AVI format. The video file is opened using IMAQ open AVI VI (Virtual Instrument) and it is separated into frames. The encryption is applied on each frame such that they convey no visual information about the original frame. The encrypted frames are combined together to form an encrypted video and then it is saved to a file. The encrypted video file can be transferred to an email from LabVIEW using Simple Mail Transfer Protocol (SMTP). If any error occurs during transmission an error message is popped. To access the original video, decryption key is applied on the encrypted video.***

Keywords— Video file encryption, Hill Cipher, Asymmetric encryption, SMTP, LabVIEW

I. INTRODUCTION

Encryption is restructuring of data into new unintelligible form controlled by a known random key to ensure privacy by hiding the data from everyone. The encrypted data can only be viewed by an authorized user who knows the decryption key. Decryption is a process for converting the encrypted data in to its original form. Video characteristics are different from the image characteristics such as large capacity with high correlation and redundancy among pixels which together make conventional encryption schemes slow for processing. Conventional encryption scheme use symmetric encryption, the same key is used for both encryption and decryption. So Hill Cipher with an asymmetric encryption technique is taken. The main aim of the Hill Cipher Encryption is to keep data hidden from all non-authorized parties (restricted availability), and the data has not been modified and viewed during transmission by non-authorized persons (Authentication). The 4*4 asymmetric key matrix is generated by a random search method. LabVIEW, which is a powerful graphical programming language, is chosen to implement the video encryption. It reduces the programming effort of the users to obtain better results in shorter time. Although it is a graphical development environment, it allows creating .m files and solves the text-based math using Math Script nodes. The internet standard that is used to send the email reliably over the internet is Simple Mail Transfer Protocol (SMTP). In LabVIEW video is saved in .avi format by using AVI functions in the function palette.

II. HILL CIPHER

The first simple polygraphic cipher grouping more than two letters is Hill cipher algorithm. It was first described by the mathematician Lester S. Hill in the journal The American Mathematical Monthly in 1929. He applied Linear algebra to polygraphic cipher. The text and image encryption using Hill cipher in LabVIEW is discussed below.

A. Text Encryption with Hill Cipher (p=97)

The computers store the textual data with the ASCII character set. In ASCII set the first 32 characters out of 128 characters are control characters and the last 128th character is another non printing character. The 95 printable characters present between the control characters containing 10 digits, 26 lower case letters, 26 upper case letters, and 32 punctuation marks including space.

The Hill Cipher key for a block with two characters is a 2*2 matrix whose entries are non negative integers among 0, 1, 2, . . ., p-1, where p is the length of the printable characters. The p has to be a prime, if it is not then modulo p does not constitute a finite field. The length of the printable characters is p = 95 which is a semi prime, so the next largest prime p = 97 is chosen to do arithmetic modulo-p.

Steps for encrypting a text using Hill cipher Algorithm in LabVIEW are:

Step1: The text encryption and decryption code is placed in a case structure. The user has to decide either to do encryption or decryption. Only one of the cases runs at any time.

Step2: The string is converted to an array with Byte array VI.

Revised Manuscript Received on June 01, 2019.

K. Gnana Sushma, Department of Electrical & Electronic Engineering, SRKR Engineering College, Bhimavaram, India.
B.V.S.S.N. Raju, Department of Electrical & Electronic Engineering, SRKR Engineering College, Bhimavaram, India.

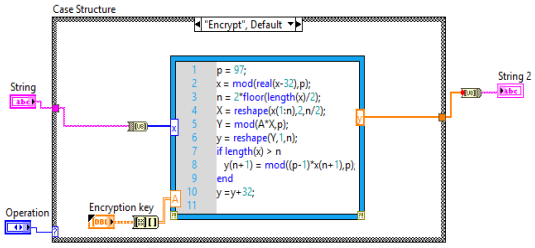


Fig. 1 Block Diagram for Text Encryption using Hill cipher in LabVIEW

Step3: In MathScript node the array is modular multiplied with the encryption key.
Step4: At the output of MathScript node the encrypted byte array is obtained and converted back to string using Byte array to string VI.
Step5: The reverse process is applied to decrypt the encrypted string, but in this process the encrypted string is modular multiplied with the inverse matrix of the encryption key.

B. Image Encryption with Hill Cipher

An 8-bit image is made up of pixels. Each pixel has intensity value ranging from 0-255. First the image is split into similar non-overlapping blocks D of size M*M. The key matrix M of the size 4*4 is formed by taking entries from 0, 1, 2, 3, . . . , p-1 where p = 256 is total no of gray levels in an image. In this paper D is chosen to be a 4*4 matrix.

The encryption equation is,

$$E = DM \pmod{256}.$$

The decryption equation is,

$$D = EM^{-1}(mod256).$$

Steps for encrypting an image using Hill cipher algorithm using LabVIEW are:

Step1: Acquire an image into LabVIEW through image acquisition device, Camera or load an image from the computer.
Step2: IMAQ create VI automatically allocates the memory space required to store the image data.
Step3: Read the image through IMAQ Read file VI to open and read data from a computer in to the IMAQ reference.
Step4: With the display image control the loaded image is displayed on the panel. It is located on the vision control palette.
Step5: The image grayscale distribution is analyzed with the IMAQ Histogram and Histograph VI'S. The image quality and saturation contrast is analyzed using Histogram plot.

a) The Concentration of peaks on the left side of histogram, if the image is underexposed and the pixels in the image have low intensity values.
b) The Concentration of peaks on the right side of histogram, if the image is overexposed and the pixels in the image have high intensity values.
c) The distinct regions of pixel concentration in the histogram, if the image has appropriate contrast and brightness.

Step6: The image is converted to 2D array by IMAQ Image to array VI. It is given as input to the Math Script node. In this each 4*4 group of pixels is modular multiplied with the 4*4 encryption cipher.
Step7: The encrypted groups of pixels are modular multiplied with the 4*4 inverse of encryption cipher to obtain the original image. Array of pixels are converted to image by using array to image VI at the output of MathScript node. Encrypted and decrypted images are displayed on the front panel with image display control. The histograms are plotted using IMAQ HISTOGRAM VI.
Step8: The correlation coefficient is used to compute the correlation between two vertical, horizontal and diagonally adjacent pixels of both original and encrypted images. For two random variables *u* and *v*, the correlation coefficient is given below where COV (*u*, *v*) is co-variance.

$$r_{uv} = \frac{Cova(u,v)}{\sqrt{\text{var}(u)}\sqrt{\text{var}(v)}}$$

$$\text{cov}(u,v) = E\left(u - E\left(u\right)\right)\left(x - E\left(x\right)\right)$$

III. SMTP PROTOCOL

The encrypted or decrypted video is transferred to email using SMTP Protocol. It is a user-level client mail application so SMTP only sends the message. If Transport Layer Security (TLS) is enabled then with the port 587 the outgoing emails are submitted by Mail clients to mail server or with port 465 if TLS is disabled. On the receiver side Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP) has to enable in email settings to receive the emails.

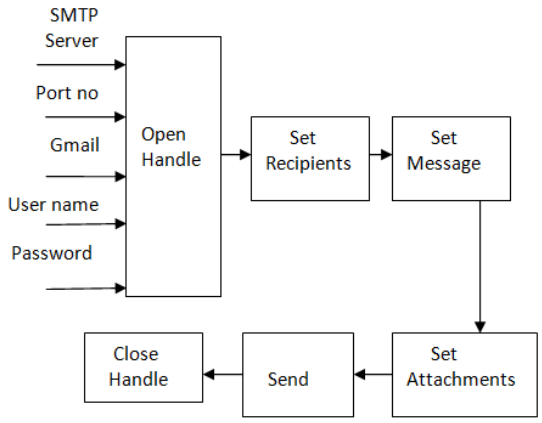


Fig. 2 Block Diagram for sending a video file to email using SMTP in LabVIEW

Steps for sending the encrypted or decrypted video along with a message from LabVIEW to email are:

Step1: Open the send email.vi
Step2: Fill in the SMTP server in the outgoing mail server i.e. Smtp.gmail.com. Gmail and its port number are available by default.

Step3: Specify sender email address, username & password and receivers email address along with the message and video attachment to be sent.
Step4: In case if the message cannot be delivered an error report is popped up on the screen.

IV. MATHSCRIPT NODE

MathScript node is designed to add script programs to the graphical programming environment and to visualize data plots. The MathScript node supports C, C++, JAVA, PYTHON and MATLAB script languages. The Hill cipher technique programmed in MATLAB is used to encrypt the video file in LabVIEW. Video encryption program has been developed by combining both script language MATLAB and visual programming LabVIEW. MathScript node runs almost all the commands of MATLAB without showing error but for some commands, the syntax has to change according to LabVIEW rules.

Advantages with the MathScript Window: It saves time by reusing existing .m files developed in MATLAB Software; it is easy to deploy .m files so there will be no extra code generation steps; Develop .m files with an interactive command line interface in MathScript Window.

V.IMPLEMENTATION OF VIDEO FILE ENCRYPTION

Video encryption using Hill cipher is an extension of image encryption discussed in above section [II (*B*)]. For any video either grayscale or color video, first step is to split video into frames. For grayscale frames the encryption process is same as image encryption. For color frames, first RGB components are separated using IMAQ Extract color planes VI and then each frame is encrypted similar to image encryption. Finally processed RGB components are merged together with IMAQ Replace color planes VI.

The steps for video file encryption are given below and the block diagram for encryption process is shown in fig 3.
Step1: Acquire video from camera or load the video file from storage and open the avi video file using Open AVI VI then read the video one frame at a time and write each frame to a file and save the file in a disk.
Step2: Open the images file with Open folder VI then create an image reference using IMAQ create function.
Step3: Encryption and Decryption process is same as discussed above.
Step4: With AVI VI's the encrypted and decrypted frames are concatenated to form a video file.
Step5: The video file is transferred to email using SMTP, if the video size exceeds 25 Mb the error message will popped on the screen.

The color images slow down the encryption speed especially for high resolution images. So it is better to use grayscale images for efficiency unless color is required for the application.

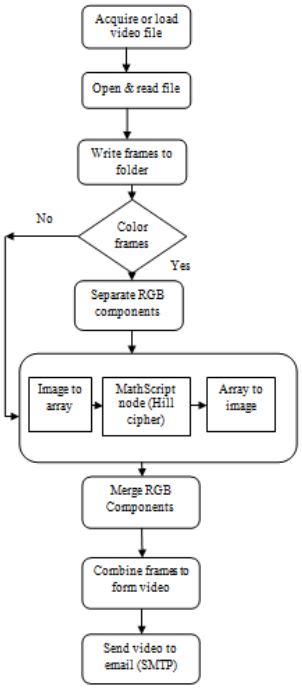


Fig. 3 Flow chart for video file encryption

VI. RESULTS

The proposed video file encryption method with Hill cipher is implemented in LabVIEW 2017. The correlations between pixels in an image and Histogram for an image and test video frames are shown in the results.

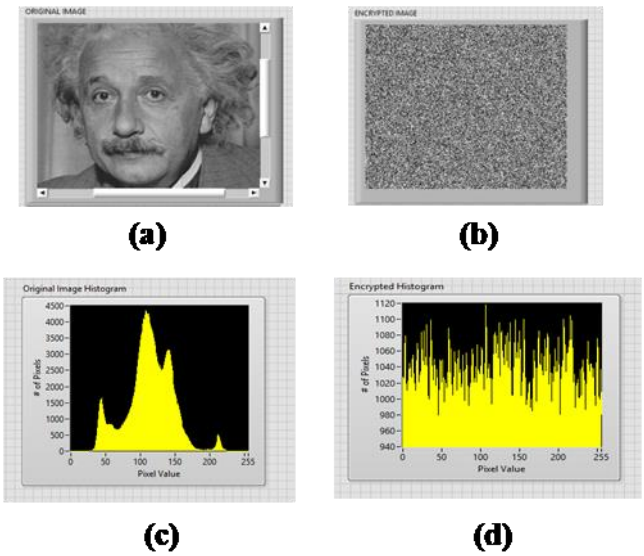


Fig. 4 (a) Einstein image, (b) Encrypted Einstein image,
(c) Einstein histogram, (d) Encrypted histogram

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

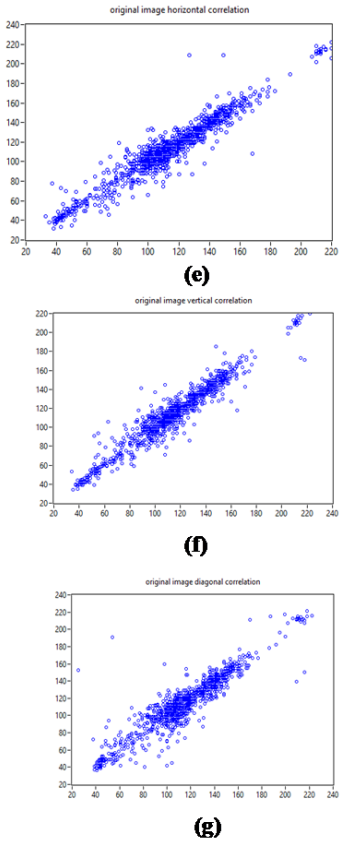


Fig. 5 (e, f, g) Einstein image horizontal, vertical & diagonal correlation plots.

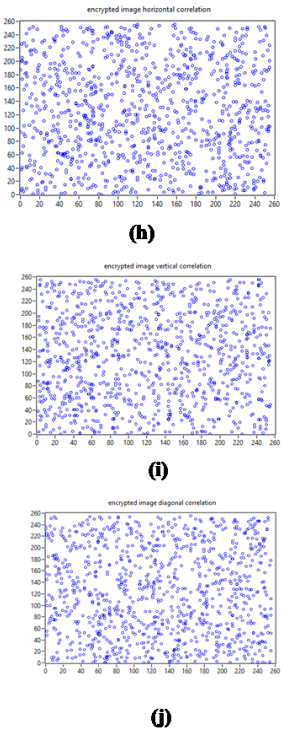


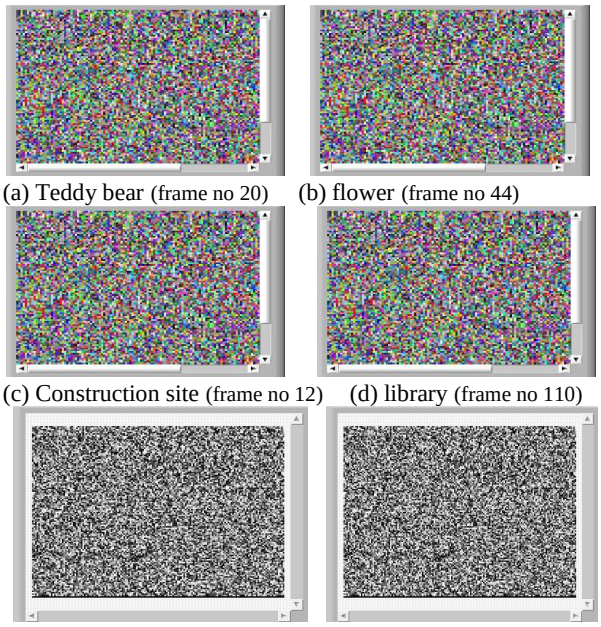
Fig. 6 (h, i, j) Einstein encrypted image horizontal, vertical & diagonal correlation plots.

(a) Teddy bear (frame no 20) (b) Flower (frame no 44)

(c) Construction site (frame no 12) (d) Library (frame no 110)

(e) Computer lab (frame no 8) (f) car (frame no 56)

Fig.7 Example frames of test videos with frame numbers a, b, c, d (color frames), e, f (gray scale frames).



(a) Teddy bear (frame no 20) (b) flower (frame no 44)

(c) Construction site (frame no 12) (d) library (frame no 110)

(e) Computer lab (frame no 8) (f) car (frame no 56)

Fig. 8 Encrypted frames of test videos with frame numbers a, b, c, d (encrypted color frames), e, f (encrypted gray scale frames)

(a) Teddy bear (frame no 20) (b) Flower (frame no 44)

(c) Construction site (frame no 12) (d) Library (frame no 110)

(e) Computer lab (frame no 8) (f) Car (frame no 56)

Fig. 9 Decrypted frames of test video with frame numbers a, b, c, d (decrypted color frames), e, f (decrypted gray scale frames)

VII. CONCLUSION AND FUTURE SCOPE

Encrypting a video file with Hill Cipher and transferring to an email using SMTP is a protective way for the security of a user. The video file encryption is implemented in LabVIEW 2017 using Hill cipher. Encryption is done quickly with the Hill cipher technique. For further extension of this project it can be deployed in NI hardware myRIO to run as a standalone application.

REFERENCES

1. V Praveena, Dr. BVSSN Raju "A project work done on "Image encryption using Hill cipher & scan patterns," unpublished.
2. Christopher G. Relf, "Image Acquisition and Processing with LabVIEW" 1st Edition, 2003.
3. Thomas Klinger, "Image Processing with LabVIEW and IMAQ Vision (National Instruments Virtual Instrumentation Series)".
4. Vipula Singh, **"**Digital Image Processing with MATLAB & LabVIEW".
5. Prerna, Urooj, Meena kumari, Jitendra Nath shrivastava, "Image Encryption and Decryption using Modified Hill Cipher Technique," ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1895-1901.
6. William Stallings, "Cryptography and Network Security", 2005, 4th Edition, Prentice Hall.

AUTHORS PROFILE

K. Gnana Sushma has completed her B.Tech from SRKR Engineering College, Bhimavaram, Andhra Pradesh in the year 2017. She is currently pursuing her M.Tech at SRKR Engineering College, Bhimavaram. Her research work includes Image processing in LabVIEW.

Prof. BVSSN Raju has completed his ME in Control Systems from Andhra University Vishakhapatnam, Andhra Pradesh in the year 1997 and PhD from Osmania University, Hyderabad in the year 2014. He is currently working as a Professor of ECE department in SRKR Engineering College, Bhimavaram. His research interests span the general areas of Signal Processing and Communications. He is member of IEEE.