International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 2, Mar- Apr 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A REAL TIME APPROACH FOR SECURE TEXT TRANSMISSION USING VIDEO CRYPTOGRAPHY

BOODODA GNANANANDA, SIDDAPU NAGARAJU

Abstract:

Picture and video are the two most basic types of communicating data. With the help of Image and video encryption methods a particular arrangement of pictures or recordings can be communicated without agonizing over security. In the proposed paper a basic and ongoing algorithm, utilizing pixel planning, is utilized for the encryption of the pictures which are the basic structure blocks of any video record. In the proposed research paper the video is conveyed into the photo outlines utilizing a tangle lab code and every one of the edges are successively put away. Each such edge contains a combination of red, blue and green layers. On the off chance that we consider a pixel as a 8 digit esteem than each pixel has the worth in the scope of 0 to 255. In the proposed work for each edge two pixels arranged at the upper left and the base right corner are changed in order to embed text in each picture. After the completion of the pixel esteem changing every one of the pictures is placed in a consecutive way and then every one of the casings are cascaded for age of the first video document with encryption. This new video is practically like the first video document with no changes obvious to the unaided eye.

1. INTRODUCTION

In late computerized world, the security of interactive media data like pictures/recordings turns out to be more essential since the interchanges of sight and sound things over system happen more as frequently as could really be expected. Moreover, special and strong security away and transmission of advanced pictures/recordings is needed in various computerized applications, for instance, TV, secret video conferencing and helpful imaging structures, and so on, various encryption calculations have been proposed actually as would be reasonable responses for the assurance of the video data. Typical data, for instance, system code or content are generally less awesome to encode or disentangle. Significant volume of the picture data makes the encryption inconvenient as we need the encryption to be done continuously. The central methodology for picture encryption is to see picture data as content and scramble it using standard encryption calculations like water stepping strategy. The basic issue with these encryption calculations is that they have high encryption time making them forbidden for continuous applications.

2. TEXT TRANSMISSION

Data transmission, computerized transmission, or advanced interchanges is the physical exchange of data (a computerized bit stream or a digitized basic give) over a highlight direct or indicate multipoint Communication channel. Tests of such channels are copper wires, optical strands, far off correspondence channels, stockpiling media and PC transports. The data are addressed as an electromagnetic sign, for instance, an electrical voltage, radio wave, microwave, or infrared sign. While basic transmission is the exchange of a consistently shifting basic give up a basic channel, computerized correspondences is the exchange of discrete messages over an advanced or a straightforward channel. The messages are either addressed by a grouping of heartbeats by method for a line code (baseband transmission), or by a restricted plan of perseveringly contrasting wave structures (pass band transmission), using a computerized change strategy. The pass band change and comparing demodulation (otherwise called identification) is did by modem hardware. As indicated by the most generally recognized importance of computerized sign, both baseband and pass band signs addressing bit streams are considered as advanced transmission, while a choice definition simply considers the baseband signal as advanced, and pass band transmission of advanced data as a sort of computerized to straightforward change.

2.1 PROTOCOL LAYERS:

The field of data transmission commonly deals with the accompanying OSI model convention layers:

Layer 1, the physical layer:

- Channel coding including
- Digital guideline plans
- Line coding plans
- Forward botch revision (FEC) codes
- Bit synchronization
- Multiplexing
- Equalization
- Channel models

Layer 2, the data connection layer:

- Channel access plans, media access control (MAC)
- Packet mode correspondence and Frame synchronization

- Error identification and customized rehash demand (ARQ)
- Flow control
- Layer 6, the introduction layer:
- Source coding (digitization and data pressing factor), and information hypothesis.
- Cryptography (may happen at any layer)

3. CRYPTOGRAPHY AND PIXEL MAPPING ALGORITHM

The proposed strategy uses a blend of systems called as steganography and cryptography. This technique improves the errand of securing the crucial information from the abuse and shields it from the unwanted client. With the use of cryptography and steganography blend the information security can be expanded.

3.1 CRYPTOGRAPHY:

Cryptography (or cryptology) is the practice and examination of methods for secure correspondence in the vicinity of outcasts (called foes). Even more all things considered, it is tied in with creating and inspecting conventions that piece foes various perspectives in information security, for instance, data privacy, data respectability, confirmation, and non renouncement are indispensable to current cryptography. Cutting edge cryptography exists at the crossing point of the controls of arithmetic, computer programming, and electrical planning. Employments of cryptography incorporate ATM cards, PC passwords, and electronic exchange.

Cryptology related development has raised different legitimate issues. In the United Kingdom, increments to the Regulation of Investigatory Powers Act 2000 require a suspected criminal to hand over his or her unscrambling key whenever asked by law execution. For the most part the client will confront a criminal accusation. The Electronic Frontier Foundation (EFF) was included for a circumstance in the United States which tended to whether requiring suspected culprits to give their unscrambling keys to law authorization is illicit. The EFF contended this is an encroachment of the advantage of not being compelled to implicate oneself, as given in the Fifth Amendment.

3.2 MODERN CRYPTOGRAPHY:

Modern cryptography includes use of various types of algorithms based on the kind of the key utilized. The key assumes an indispensable part in cryptography encryption and decryption techniques.

3.2.1 SYMMETRIC-KEY ALGORITHM:

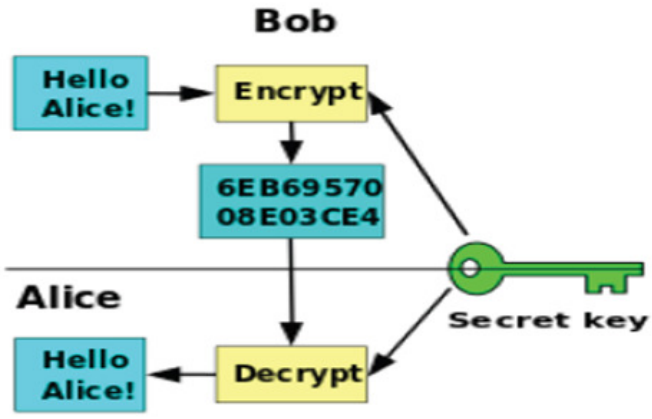

Fig:1 Symmetric key cryptography

Symmetric key cryptography alludes to encryption systems in which both the sender and beneficiary have the same key(or, less normally, in which their keys are distinctive, however related in an effortlessly processable way). This was the main sort of encryption openly known until June 1976.

Symmetric key figures are executed as either square figures or stream figures. A square figure enciphers data in pieces of plaintext rather than individual characters,, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are square figure outlines which have been assigned cryptography models by the US government (however DES's assignment was at last pulled back after the AES was adopted).Despite its expostulation as an official standard, DES (particularly its still affirmed and considerably more secure triple DES variation) remains entirely popular; it is utilized over an extensive variety of uses, from ATM encryption to email protection and secure remote access. Numerous other square figures have been outlined and discharged, with significant variety in quality. Numerous have been altogether broken, for example, FEAL.

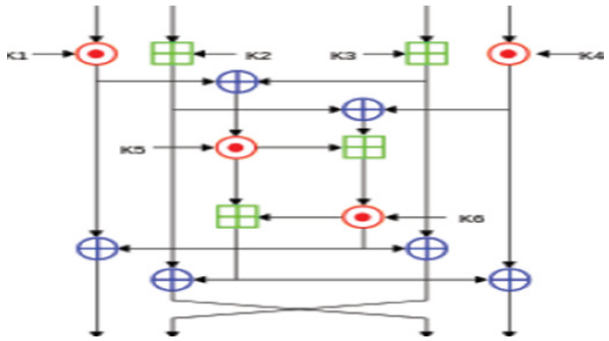

Fig.2:One round (out of 8.5) of the IDEA cipher

4. RESULTS & DISCUSSION

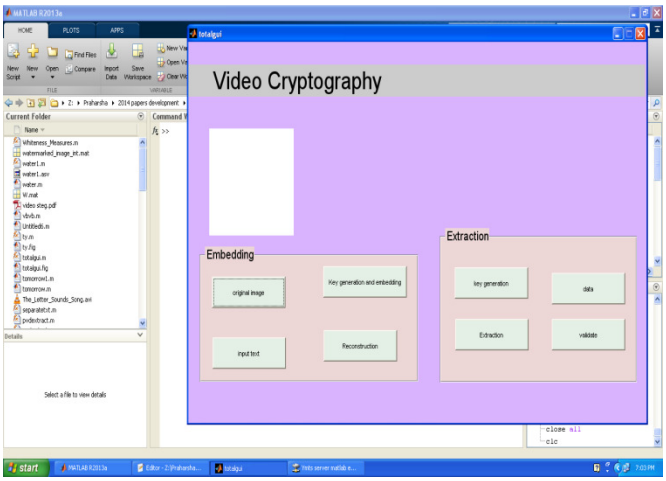

Fig.6.1: Running the program

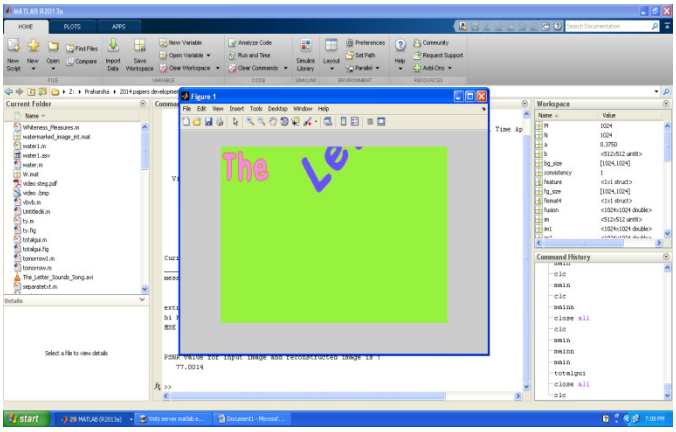

Fig 6.2: Frames in a sequential order (frame 1)

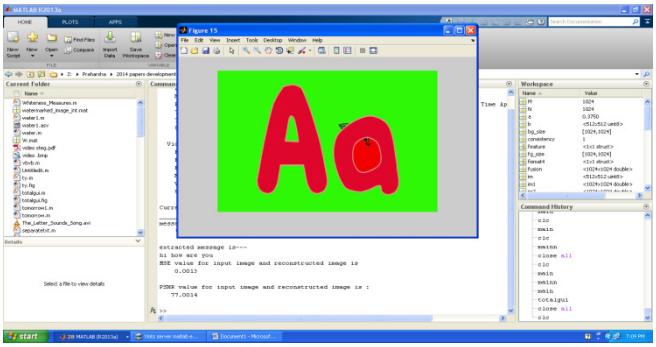

Fig 6.3: Frames in a sequential order (up to frame 15)

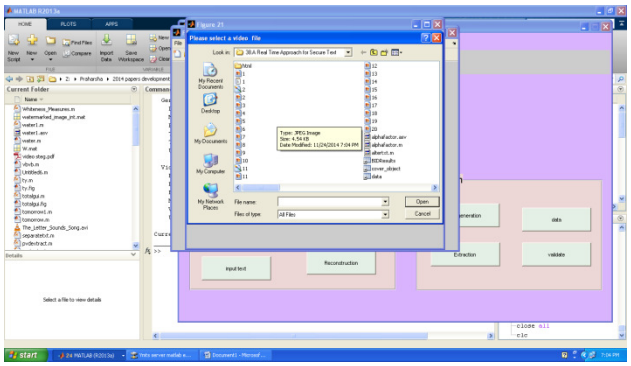

Fig 6.4: Selection of video file

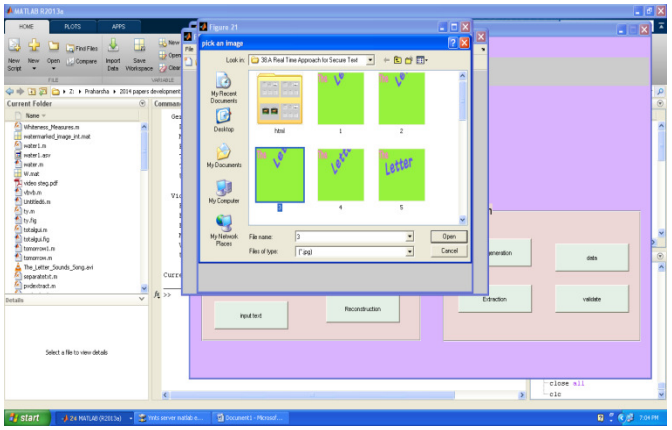

Fig 6.5: Selection of input frame

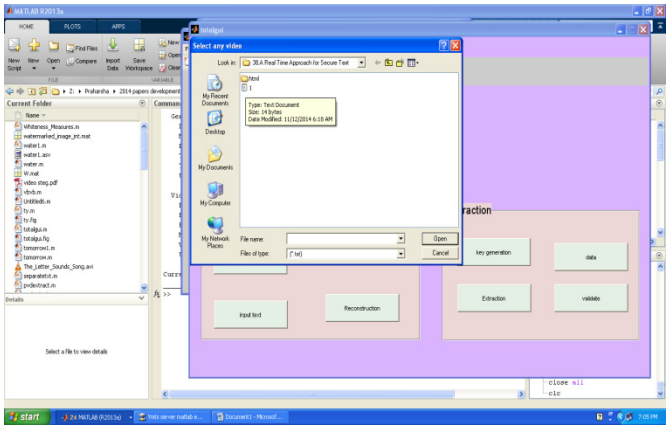

Fig 6.6: Select any text from a text documents

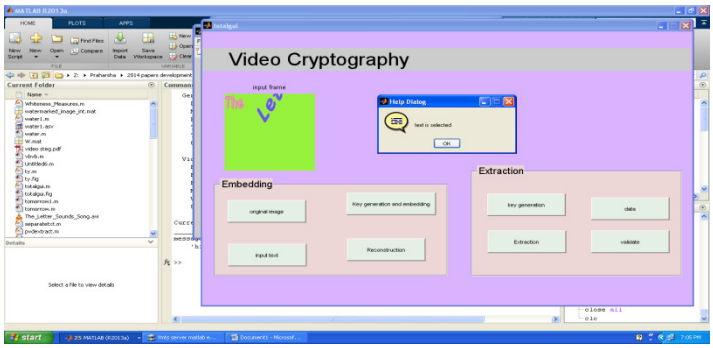

Fig 6.7: Text is selected

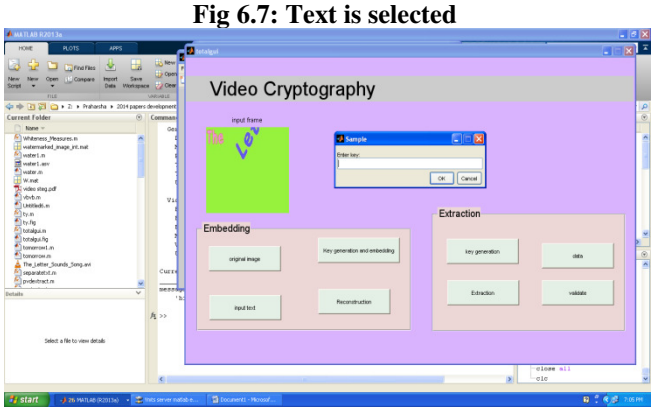

Fig 6.8: Input dialog box to enter a key

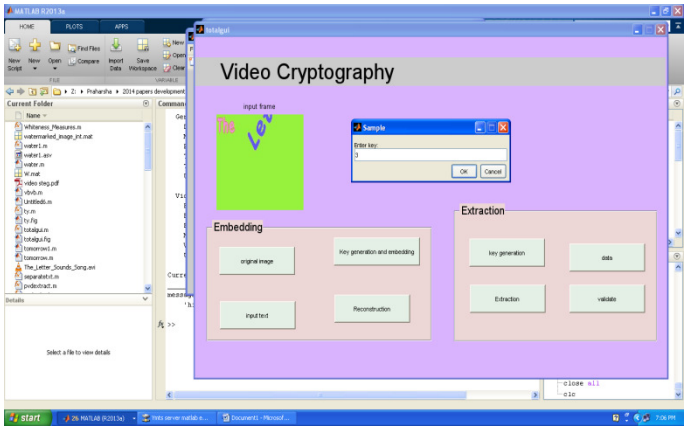

Fig 6.9: Key is entered in a dialog box

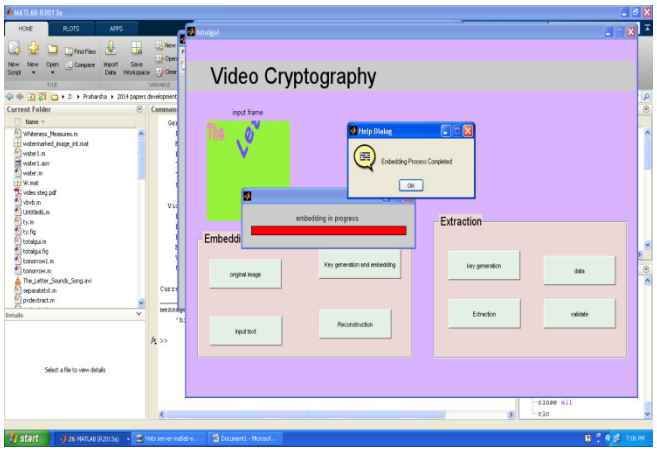

Fig 6.10: Embedding process is completed

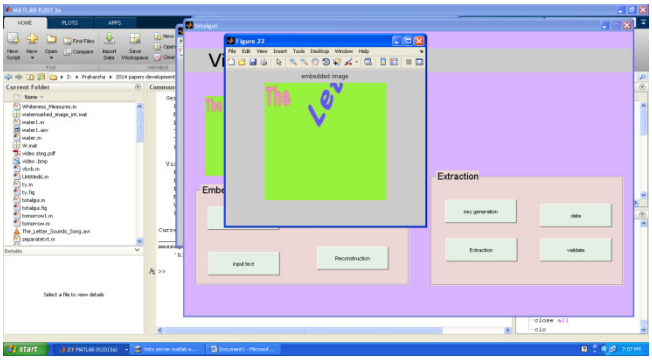

Fig 6.11: Embedded image

Fig 6.12: Enter a key in extraction process

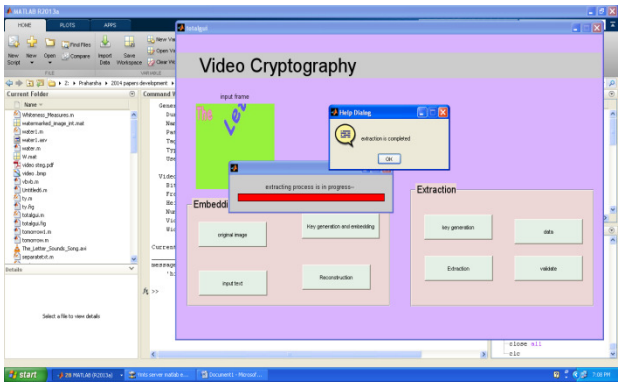

Fig 6.13: Extraction process is completed

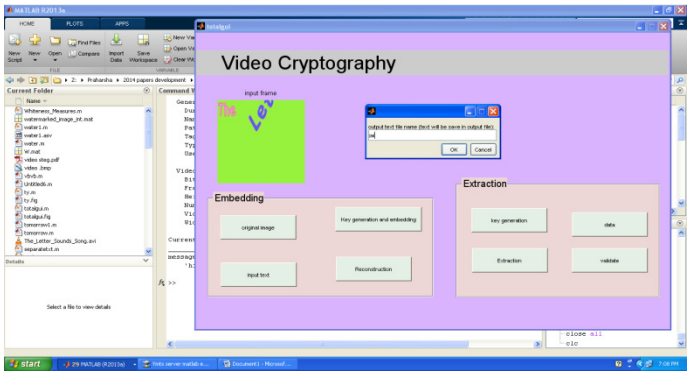

Fig 6.14:Enter output image name

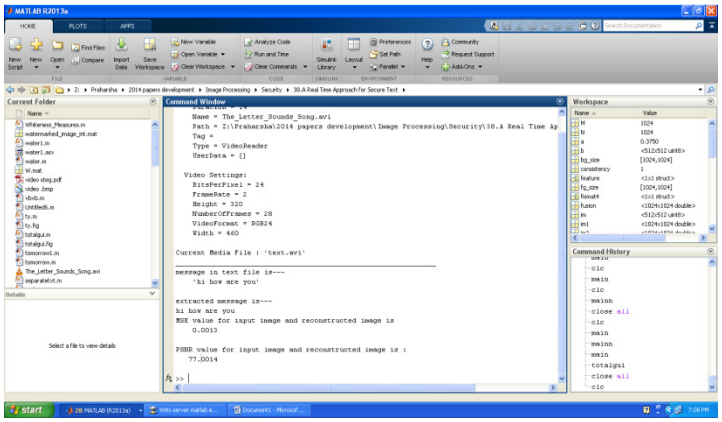

Fig 6.2:Extracted message

6.1 MSE:

$$\mathbf{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}.\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2$$

m and n are the number of rows and columns in the input images

6.2 PSNR:

$$\mathbf{PSNR}=10.\log\left(I^2/MSE\right)$$

I is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then I is 1. If it has an 8-bit unsigned integer data type, I is 255,etc.

6.3CONCLUSION

One of the important features of the proposed work is it plays a vital role in transmitting the information mapped on an either image or a video file very effectively and efficiently. The information underlying the image or a video is not visible to the naked eye.

6.4 FUTURE WORK:

The person having the private key and the rule list can identify and decode the original information into its original form & no other third party person cannot decode the original content.

REFERENCES

1.http://en. wikipedia. org/wiki/Time-lapse.

2.Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.

Google Scholar

3.Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.

Google Scholar

4.R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.

Google Scholar

5.Adnan M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. On Image Processing, vol. 13, no. 8, Aug, 2004.

View Article Full Text: PDF (1879KB) Google Scholar

6.Avcibas, N. Memon, and B. Sankur Steganalysis using image quality metrics, IEEE Trans. IP, VOL. 12, PP. 221-229, Feb. 2003.

AUTHORS

1. BOODIDA GNANANANDA
M.Tech Scholar
Dept. of Computer Science,
SSSISE, VADIYAMPET
Anantapur.

2. SIDDAPU NAGARAJU
Assistant Professor,
Dept. of Computer Science,
SSSISE, VADIYAMPET
Anantapur.

