Secure Text Transmission by using Video Cryptography in Real Time Applications

V.Chinnapu Devi, K.Gnanaprasuna, B.Chandana, K.Leelakrishnaprasad

Assosciate Professor, Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student , Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student , Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student , Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

ABSTRACT: Picture and video are the two most fundamental types of transmitting data. With the assistance of Image and video encryption techniques a specific arrangement of pictures or recordings can be transmitted without agonizing over security. In the proposed paper an extremely basic and ongoing calculation, utilizing pixel mapping, is utilized for the encryption of the pictures which are the fundamental building squares of any video file. In the proposed research paper the video is dispersed into the photograph outlines utilizing a matlab code and every one of the edges are successively put away. Each such casing contains a mix of red, blue and green layers. On the off chance that we consider a pixel as a 8 bit esteem than every pixel has the quality in the scope of 0 to 255. In the proposed work for every edge two pixels arranged at the upper left and the base right corner are modified in order to embed content in every picture. After the finish of the pixel esteem changing every one of the pictures is put in a successive way and afterward every one of the edges are fell for era of the first video file with encryption. This new video is verging on like the first video file without any progressions noticeable to the bare eye.

KEYWORDS: Video Encryption, Lossless Water Marking , Pixel Mapping, Stegnography.

I.INTRODUCTION

For ordinary person the capacity to see the movements of other energize edges or video has been broadly concentrated on and it is demonstrated that for the developments made in the running video just the little measure of the pixels are modified and rest every one of the pixels stay static in the event that we look at the pixels of any back to back casings in a video. So by the progressions made in the littler number of pixels in a succession of pictures every one of the developments are portrayed flawlessly in a video file. This is extremely straightforward and simple strategy for picturing any procedure under study. Research demonstrates that among the back to back pictures having million quantities of pixels just couple of hundred pixels are modified for showcasing the developments happening in the specific video.

Any video is fundamentally a blend of various edges and every one of the casings constituting a video has a fixed outline rate. By and large the casing rate is 25 so we can say that 25 edges are caught inside of one second time. For the efficient and fruitful execution of this specific calculation there is a necessity that the video should be divided. For a specific case on the off chance that we assume that the video is of 5 minutes length of time than this video significantly contains 7500 edges in it. These edges are crucial building hinder for the video and in addition for video encryption process.

We can embed what's more, send the content alongside the casing by utilizing different accessible watermarking methods. There are different distinctive watermarking systems accessible like visual watermarking, discrete cosine change, discrete Fourier change and misfortune less watermarking technique. All the watermarking systems as of late accessible have certain downsides furthermore these strategies are a tiny bit tedious. Likewise the watermarking procedures can be modified utilizing more propelled methods for picture handling. To get over the disadvantages of the watermarking strategies stenography technique can be utilized for the encryption of the video files.

Stenography is for the most part valuable regarding efficient and precise information handling for the instance of the constant applications. In the proposed work likewise the stenography system can be produced by utilizing a pixel mapping calculation. Additionally the stenography system is quicker and efficient as far as time required for denoting the specific arrangement of pictures.

II. . LITERATURE SURVEY

Cryptography is a specialty of transforming so as to ensure the data it into a garbled and untraceable arrangement known as figure content. Just the individual who have the mystery key can translate or we can say unscramble the message into the first frame. Cryptography is the method by which one can send and share the data in a mystery way. Due the cryptography the data is by all accounts seeming like a refuse worth and it is dependably practically difficult to find the data content lying under the picture or a video file.
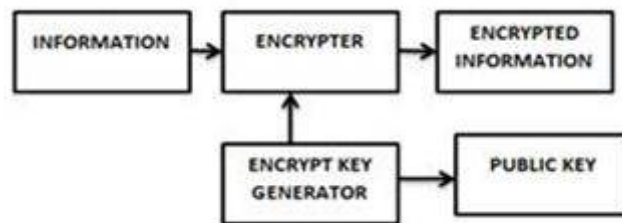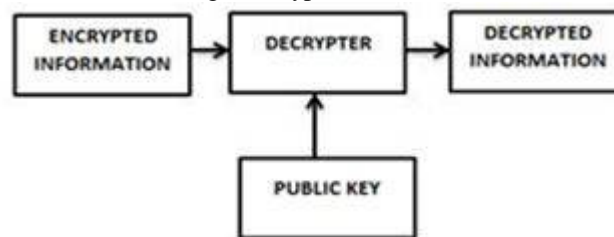

Fig1:Encryption

Fig2:Decryption

The data looks like covered up inside the picture or the video file. The encryption key generator is utilized to produce the encryption key and in addition the general population key as appeared in the square graph underneath. By utilizing the encryption key the data substance to be sent gets encoded by the encryptor. The encoded data is then transmitted to the specific collector. At the recipient end the Cryptography Decryptor is utilized which removes the first data content mapped onto the picture or a video file with the assistance of an open key gave by the transmitter area.

So by the utilization of the cryptography strategy just the recipient which has the learning of people in general key can recover the first data content from the picture or a video file. So regardless of the fact that any undesirable individual or a source gets the picture or a video file with data content covered up in it, it can't be separated without appropriate open key. So open key assumes a key part in the entire cryptography process.Threshold Secret Sharing Schemes.In secret sharing schemes, the number of the participants in the reconstruction phase is important for recovering the secret. Such schemes have been referred to as threshold secret sharing schemes.

III. . PROPOSED METHOD

Stenography is the specialty of embedding so as to conceal data message inside of one another. It works by supplanting the extremely futile bits by the data substance to be transmitted. It works by concealing data inside a spread. The spread might be a picture file or a video file according to the client necessity. Despite the fact that the spread looks extremely basic and unaltered however it has data contained in it.
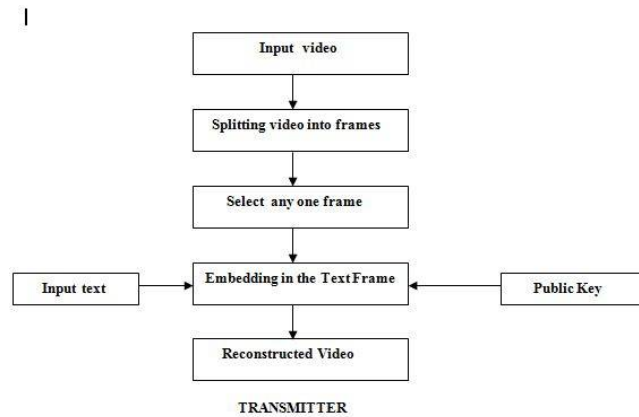
First all the video files convert into equal frames.The data content which is to be transmitted by mapping onto the video file is conveyed into little parcel contingent upon the span of the casings in the video file. From every edge a littler district is modified relying on the private key. Because of this the chose bunches looks extremely arbitrary to the outsider who does not have the private key with them.

The chose pixels are then changed over into the recurrence space with the assistance of the discrete cosine change. Generally a predefined segment of the pixels such as we say the last a few bits are then supplanted by the spilled message bit and afterward the pixel bit is again changed over once more into the spatial space. The change from the recurrence area to the spatial space is finished with the assistance of backwards DCT. At that point that gathering of pixels is set again into the specific casing. This procedure is taken after until the end of the entire data content. The casings are then orchestrated into a consecutive way and the video is built from it.

Presently this video contains the data which gets transmitted alongside the transmission of the video file.

The Stegnography encoder needs to keep some control message into the video file by which the collector can comprehend the information position, method for concealing the data content, sort of encryption done and so forth. This is known as the tenet rundown for a specific stegnography process. This principle rundown is created and for the most part it is set in the first casing of the video file. This tenet rundown goes about as a kind of perspective for a specific craved recipient. Without standard rundown the recipient will be unable to comprehend and recover the first data content covered up inside of the got video file. So the standard rundown assumes a fundamental part at the collector side.
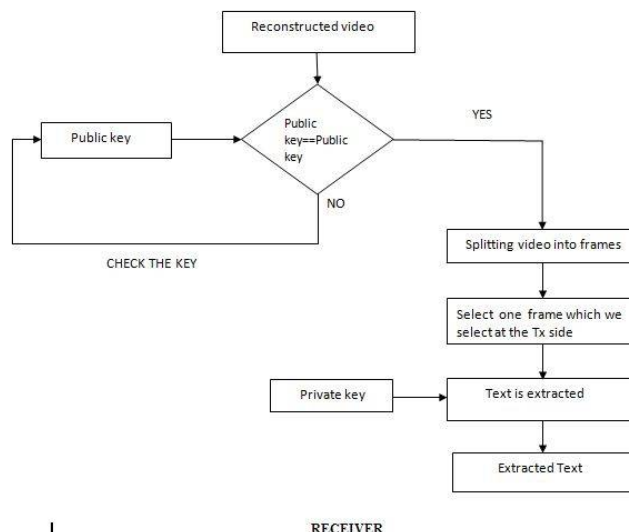
The primary squares in a Stegnography Decryptor it is clear that if the private key is not known not is difficult to extricate the first data content in the got video file. There are sure techniques like some steganalysis apparatuses by

which the data can be identified without the utilization of the private key moreover. This is by all accounts the significant disadvantage of the basic Stegnography strategy. Stegnography technique can be modified for changes so that without private key the data may not get extricated effortlessly.

IV. SECURE TEXT TRANSMISSION BY USING VIDEO CRYPTOGRAPHY

Depicts the flowchart demonstrating the grouping of ventures to be executed for producing the scrambled video file for secured content information transmission.The calculation is briefly portrayed regarding flowchart for the better comprehension of the entire procedure. The complete calculation is coded in a Matlab code demonstrating the itemized process included in the video encryption and the content insertion in the video file for secured transmission.

The complete video is fragmented into number of pictures utilizing a little Matlab code module and after the preparing of the video by the Matlab code module the video gets partitioned into various edges of same size. At that point the content string which is to be embedded among the pictures is divided into the gathering of two bits each. As we have to change just two pixels for every picture so we partition the content information into the gathering of two bits. Every character in the content information can be spoken to by a specific ASCI esteem so each of the character involves 1 byte or 8 bits in a picture.

In this specific calculation each of the picture must be modified by two pixel esteem and that additionally just the last two bits so each of the character in the content information to be embedded is spoken to by its ASCI esteem in line. After this each of the characters spoke to into the gathering of 8 bits is subdivided into the gatherings of 2 bits as it were. So now we have four gatherings for each of the character in the content information to be embedded into the pictures. In this calculation to speak to one specific character we require four pixels to store one specific character. According to the grassman law significance of three fundamental hues which are red, blue and green are distinctive.

According to grassman law the significance of the green layer is the most on the grounds that it contains 59% weightage to produce any shading in a specific pixel according to the necessity. Because of this in this specific calculation just the estimation of the red and the blue layers are changed for preparing the picture to hold the first shade in the edge. The green layer in each of the pictures is unaltered. Just the blue and red layers pixels are modified in each of the picture outlines

Presently we have outlines and in addition exceptionally all around circulated content information accessible so the following stride to be taken after is to encode or delineate content information into the pixels of individual casings till the end of the content information. In the proposed work we are going to store one character into one edge so there is a prerequisite of n number of edges for putting away n number of characters in the content information. For a specific picture outline by adjusting just two pixels at top and base of the picture file does not roll out any significant improvements in the visual impacts of the edge so they are not unmistakable to the human eye.

Next stride to be taken after according to the flowchart is to choose the first outline from the succession of the edges and recognize the red layer of the first pixel and overwrite the last two bits with the first two bits of the character in the content information. So also likewise over compose the last two bits of the blue layer pixel by the comparing next two bits of the character. Same procedure is to be defeated the pixels present in the base area of the picture. By along these lines we can force   one character into one casing and the same procedure is to be taken after for every one of the characters present in the content information with successive distinctive edges.

As said before we can force m number of characters in a content information into n number of casings yet the main condition is m ought to be less or equivalent to n. Diverse variations of the video encoding can be created as portrayed underneath :

Case 1: By altering the division example of the content information we can aggregate the character bits into the gathering of 2, 4 or 8 bits. By this the quantity of casings to be modified can be expanded or diminished by prerequisites.

Case 2: The content information insertion should be possible into the substitute casings for boosting the information transmission security.

Case 3: One can transmit the points of interest of the casings modified in type of an exhibit in a casing. After that content information insertion should be possible for giving the most noteworthy information security and wellbeing.

Case 4 : One more modification should be possible by changing the calculation one might say that the successive characters in the content information are encoded into all the three shading layers in a specific manner so that just the individual who knows this example can decode the first content information.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

V. RESULTS

The chose outlines which have changes according to the al-gorithm are put away in the final video file. While catching the edges for the video file, the date and time at which that specific edge has been caught turns out to be all that much imperative in comprehension the finer subtle elements of the subject under concentrate, for example, plant developing or area of the stars in the sky and so forth.

For these date and time stamping a lossless visual watermarking technique is utilized. Here the date and time of the framework with which the casing catching gadget is associated while execution is thought to be as the reference time. The stamping technique results into the numeric characters that are spoken to with the assistance of the parallel representation.Time-stamping utilizing Visual lossless Watermark-ing.With the assistance of the lossless watermarking calculation the example for every character to be stamped if found.

Original Image

Embedded Image

2015

Reconstructed Image

Figure 6 demonstrates the first, run through stamped and recouped picture. The numbers are put away as twofold digits having exhibit of 20x18 characters. The numbers which are signified by 0 are highlighted and it speaks to the character to be shown. With the assistance of a MATLAB based calculation time stamping is defeated the recorded pictures. The areas where the time stamp is to be done are fixed inside of the pixel values extending from 1:20 x 1:144 for date stamping and 21:40 x 1:144 for timestamping.

VI. CONCLUSION AND FUTURESCOPE

One of the critical components of the proposed work is it assumes an essential part in transmitting the data mapped on an either picture or a video file successfully and efficiently. The data hidden the picture or a video is not unmistakable to the bare eye. Just the individual having the private key and the guideline rundown can distinguish and unravel the first data into its unique structure. This strategy simplifies the assignment of securing the imperative data from the abuse and shields it from the undesirable client. With the utilization of the cryptography and stegnography mix the data security can be expanded. To transmit more than 5 mb data by using this video cryptography

REFERENCES

[1]   Adnan M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. On ImageProcessing, vol. 13, no.8, Aug, 2004.
[2] Avcibas, N. Memon, and B. Sankur Steganalysis using image quality metrics, IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003.
[3] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani,Dual layer data hiding using cryptography and steganography in IJSET volume 1,issue4,ISSN:2277-1581
 [4] http://en.wikipedia.org/wiki/Time-lapse.
 [5] Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.
[6] Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.
[7] R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.

BIOGRAPHY

Smt.V.Chinnapu Devi has pursued her B.E from SLN college of engineering, Raichur. and MTech from G.Pullareddy college of engineering, Kurnool. Presently she is working as Associate Professor in Brindavan Institute of Technology & Sceince, Kurnool. She has published 4 International Journals . Her research areas of interest are Digital image processing and communication.

K. Gnana Prasuna is pursuing her B.Tech in Electronics and communication Engineering from Brindavan Institute of Technology & science, Kurnool.

B.Chandana is pursuing her B.Tech in Electronics and communication Engineering from Brindavan Institute of Technology & science, Kurnool.

K.Leelakrishna Prasad is pursuing his B.Tech in Electronics and communication engineering from Brindavan Institute of Technology & Science, Kurnool.