A REAL TIME APPROACH FOR SECURE TEXT TRANSMISSION USING VIDEO

Jyoti Uppar,

MTech Student,

VTU Extension Centre,

UTL Technologies Ltd,

Bangalore.

Hemanth Kumar K S ,

Assistant Professor,

VTU Extension Centre,

UTL Technologies Ltd, Bangalore

Dr Siva Yellampalli,

Principal,

VTU Extension Centre,

UTL Technologies Ltd,

Bangalore

ABSTRACT

Picture and video are most simple form of transmitting the data. By using of image and video with technique of encryption it's possible to secure information safely to the network or server. Here following the basic building module of Pixel mapping method. The video are separated into frames and those frames are ordering into chronological form to store it. Those frames are organized into RED, BLUE and GREEN levels. The taken one pixel equal to 8bit means then total range of this value is 255.In this process information are placing in opposite of corner of frames. Finally arranging the frames in video, it is look same as input video only.

Key words: *Cryptography, Stenography, Pixel Mapping, Public Key*

INTRODUCTION

This frame movement can be easily identified with a help of the objects or animated things in frames [1]. But normal eye it is difficult to find out the pixel changes in frame because pixel are not visible scale and rest of pixel are constant stage [2].

If we consider any video will be same or different types of frames and binding into the single video. General calculation of each frame rate equal to the 25frames, these frames are confine into 1sec.If video is 1minute the simple calculation 1second equal 25 frames means 60seconds multiple by 25frames. By using converted video into frames can be filled the data into frame with help of Stenography. Why we considering stenography techniques why not Watermark techniques. The stenography is more accurate and efficient compare to Watermark techniques [3][4][5]. Watermark main drawback is it will consume more time following the processing steps. In given long time it convert only small amount of data. Stenography method considering the pixel mapping technique and algorithm steps are less compare to the watermark technique [7][8].

I. IMAGE TRANSMISSION USING CRYPTOGRAPHY

Cryptography algorithm steps are shown in Fig 1.The input of data is video, this video format may anything according to ng that make sure in development of extension video format.

Step 1: Upload video on application of video loading function and convert video to frames.

Step 2: Write input text data into frame in sequential order.

Step 3: If already text data is available on frame means have a option to overwrite information or keep as it is..

Step 4: Check condition if want to replace then repeat step 3 or not required to write data on already present in the frame.

Step 5: Store remaining frames into .AVI file.

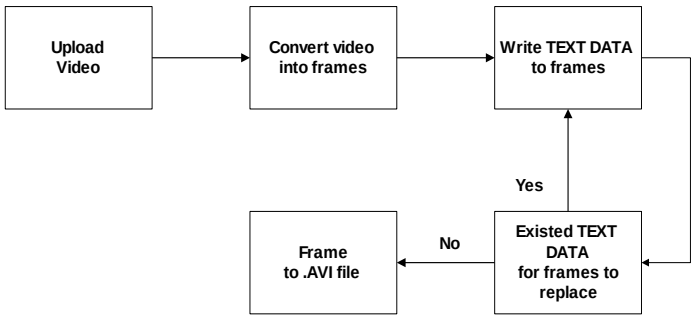

Figure 1: Block diagram of Cryptography

CRYPTOGRAPHY

Cryptography is design of high hidden the data while transforming into the other side without any issues in text data.

The entire process can be done with Matlab code for batter result. In this case encryption method and text placing into the video converted frames [9]. As shown in Fig 1, the full bundle video is converting into frames with help of video converting module in Matlab code and different dimension of frame size. The message text is inserted into frame and divided into two bits of each. Now we need to update only two pixels per image[11]. Each text is string and converted into ASCII value then sizes become a one byte or 8 bits in image. In this algorithm to signify the one character required four pixel to store particular character. If consider grassman law 2:1 weighage of green colour remaining both of colour are 41 percent in pixel requirement [12]. The green colour is constant remaining red and blue will as per the colour modification.

The rule for the writing text into the frame number of character (i) should be less then the number of frames (j).

Video encoding steps are listed below:

a) Modification of segment patter into text, here distributing group like 2, 4 or 8bits.
b) Test data insertion can implement in alternate frame to make more secure of data.
c) The text data is encoded with green, red and blue layer in systematic manner, who inserted person can only make data encoding.

Cryptography is the procedure one can share and many user can be utilizes of to share information it may be in the form of text or frame picture with safe mode. The other side user will receive data like garbage string and its highly impossible to understand the information..

The encryption key generator is used to generate the encryption key and also public key as shown in below block diagram. Thus encryption key information is encrypted with help of encryption. Finally this result is sent to the particular receiver as shown in Fig 2.

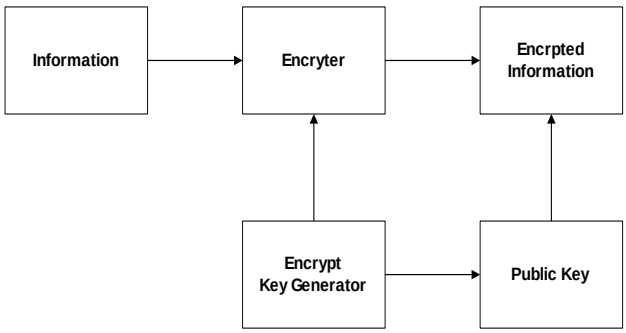

Figure 2: Cryptography Encryption

If, consider the receiver end of the Cryptography Decryption is used to brief the original information compare to the video file by using public key ,this processor will held on transmitter side. If any other user wants to extract the information then they must have the proper public key for particular video file information content. Otherwise it won't be able to get real information so here public key if working as an effective operation as shown in Fig 3.

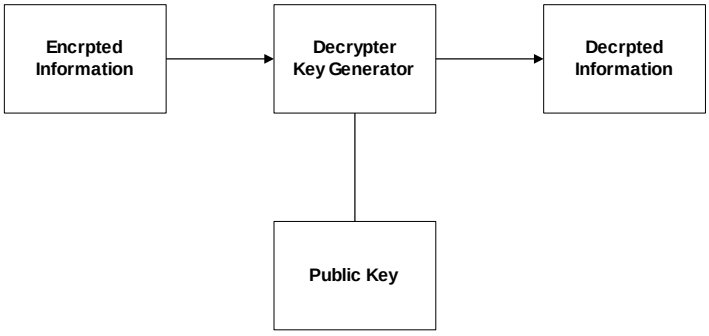

Figure 3: Cryptography Decryption

STEGANOGRAPHY

The steganography expression adapted by Greek dictionary in steganos, it says that disclose and graphy means representation like diagram or plotting .The most advantage of steganography is hidden the data thought out the network communication without any leakage of data [4].

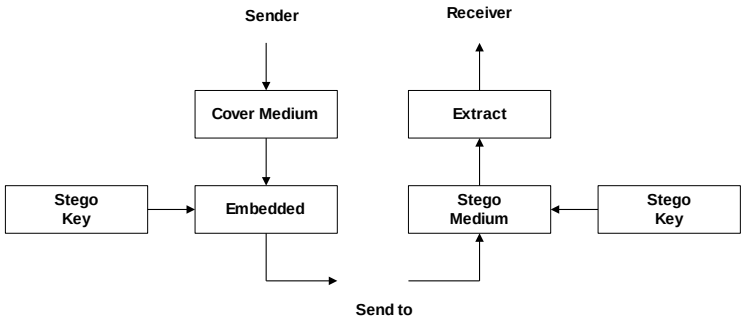

Figure 4: Block diagram of steganography

Steganography algorithm will change the given input text characteristics structure so that it cannot be possible to re-collect the normal eye into original text format. This steganography consists of three main processing steps Text data, embedded technique and Stego key, but here considering RSA algorithm .The block diagram for steganography as shown in Fig 4. The aspects of steganography are classified into different type's capacity, defense and robustness and it's required to achieve quality of model. Capacity represent the total amount of text is in secured, Defense – this means not capable to detect the original information with full safe. Robustness - is the quantity of changes the stego standard can hold out before a detector can destroy the secreted information.

The difference between cryptography and steganography is a significant one, and is detailed in below table.

Table 1: Cryptography Vs Steganography

Techniques	**Steganography**	**Cryptography**
Definition	Steganography defines cover text	Focuses on keeping contents of a message secret.
Key	Optional	Necessary
Carrier	Any digital media	Usually text based
Visibility	Never	Always
Security Services Offered	Confidentiality, authentication	Confidentiality, availability, data integrity, non-repudiation
Attacks	It is broken when attacker detects the steganography has been used known as Steganalysis	It is broken when attacker can read the secret message known as Cryptanalysis
Result	Stego file	Cipher text

RIVEST SHAMIR ADLEMAN FOR PUBLIC KEY ENCRYPTION

The RSA algorithm is also called secure public key generation technique or asymmetric cryptography algorithm and most popular method. Basically

RSA is used for encrypt and decrypt text data.

Keys are classified into two types:

a) Public Key

b) Private Key

Public Key – is known as asymmetric Key algorithm.
Private Key – is called as a Secrete Key.
Step 1: Select value for example p = 3 and q = 11
Step 2: Calculate n = p * q = 3 * 11 = 33
Step 3: Calculate ϕ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
Step 4: Select e such that 1 < e < ϕ(n) and e and ϕ (n) are co-prime. Let e = 7
Step 5: Calculate a value for d is (d * e) % ϕ(n) = 1.
One solution is d = 3 [(3 * 7) % 20 = 1]
Step 6: Public key is (e, n) => (7, 33)
Step 7: Private Key is (d, n) => (3, 33)
Step 8: The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
Step 9: The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$.

We have evaluated video encryption scheme with respect to three parameters: security level, encryption speed, and encrypted MPEG stream size. In Table 2 the comparative results of the encryption algorithms is done that is DES, AES and RSA. The speed of all three algorithms is high. Whereas the security level of the RSA and AES is high as compared to the DES.

In this table shows comparison of the video encryption design. We have to figure out based on these three parameters.

Table 2: Comparison of DES, ASE and RSA algorithm

	Com Plex ity	**Mem ory cons traint**	**Key Type**	**Key Len gth (in bits)**	**Key Spa ce Size (in bits)**	**Secu rity level**
DES	Com Plex ity	NA	Priva te Kay	56 bits (sub key -48 bits)	2^{56}	Low
AES	Comp lexity	Very Low	Priva te Kay	128 bits (sub key - 196bits)	2^{128} , 2^{192} , 2^{256}	High
RSA	Simple	NA	Pub	Variable	Vari	High

			lic Kay		able	

PERFORMANCE AND RESULTS

The main performance of this work is representing the design and implementation of the module. Since the Steganography is more complex part in the individual steganography. Hence this operates at high speed inserting into frames and reduce the lossless data.

The below figure represent the main GUI page. This represent the input video into number of frames and given input making into to not understandable text data is called as embedded of text and finally showing the encrypted message but destination side video is same as original video but size of video and text data inserted into frames.

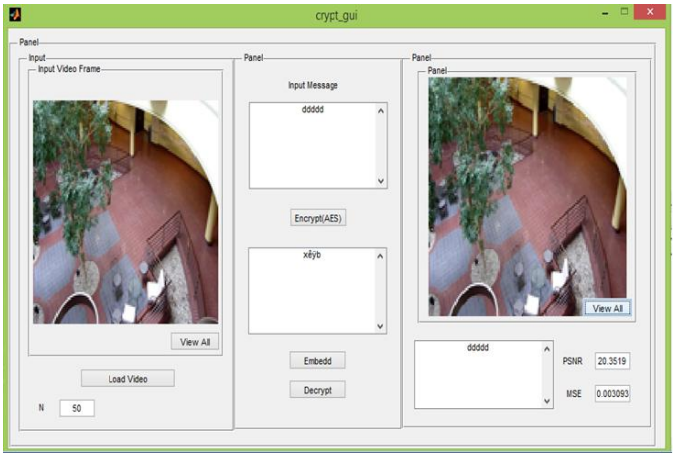

Figure 5: Result of video file processing by using RSA algorithm

CONCLUSION

The most important feature of this project proposed work is, a crucial role of transmitting the information in image or video file with effectively and efficiently. Another important characteristic is not visible to normal human eye. Only such case can be view original message, if person had a private key and list of rule explained above with decrypt technique. This method present the securing the information, misuse of data and protect from unknown persons. With combination of RSA, cryptography and steganography method will make safer and top secure.

REFERENCES

1. Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.
2. "A real time approach for secure text transmission using video cryptography" by Viral Metaliya, Dipak Jain and Ravin Sardhara in
3. conference on Communication Systems and Network Technologies (CSNT) ISBN 978-1-4799-3069-2.
4. [NeetuSettia. "Cryptanalysis of modern Cryptography Algorithms". International Journal of Computer Science and Technology. December 2010.

5. Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography",International Journal of Computers & Technology, ISSN: 22773061, Vol.9, July 2013, pp. 976-984.
6. Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Vol.2, April 2012, pp. 143-146.
7. "A real time approach for secure text transmission using video cryptography" by Viral Metaliya, Dipak Jain and Ravin Sardhara in
8. conference on Communication Systems and Network Technologies (CSNT) ISBN 978-1-4799-3069-2.
9. Mihir H Rajyaguru, "Crystography - Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.
10. H.Al-Barhmtoshy, E.Osman and M.Ezzaand, "A Novel Security Model Combining Cryptography and Steganography", Technical Report, 2004, pp. 483-490.
11. S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography:
12. 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. [10] Avcibas, N. Memon, and B. Sankur " Steganalysis using image quality metrics", IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003
13. Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani hiding using cryptography and steganography" ISSN: 2277-1581
14. A. Joseph Raphael, Dr. V.Sundaram, "Cryptography and Steganography-A Survey, International Journal of Computer and Technology Applications", ISSN: 2229-6093, Vol.2 (3), 2010, pp. 626-630.
15. Niu Jiping, "Image encryption algorithm based on rijndael S-boxes" in IEEE applied International conference on computational intelligence and security 978-0-7695-3508-1\08, 2008.
16. Punita Meelu ,"AES Asymmetric key cryptographic system" in international journal of information technology andknowledge management, volume 4, 113-117, 2011.
17. N.V Rao, J.TL Philjon, "Metamorphic Crypto-A Paradox between Cryptography and Steganography using Dynamic
18. Encryption", IEEE Xplore International Conference on Recent Trends in Information Technology, June 2011, pp. 217-222.
19. Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", International Journal of Advanced
20. Science and Technology, Vol. 54, 2013, pp. 113-124.
21. B. Subramanan, "Image encryption based on AES key expansion" in IEEE applied second international conference
22. on emerging application of information technology, 978-0-7695-4329-1/11, 2011.
23. Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and their Applications (IJNCAA), ISSN: 2220-9085, Vol. 1(1), 2011.