IMPROVE DATA SECURITY OVER OPEN CHANNEL WITH ROBOTIC FRAME SELECTION MODEL

Sonali Jain, M.tech. Scholar, Rajasthan Institute of Engineering & Technology, Jaipur,
sonalijain1588@gmail.com
Jyoti Khandelwal, Assistant Professor, Rajasthan Institute of Engineering & Technology Jaipur
jyoti.khandewal19@gmail.com
Vijay Kumar Sharma, Assistant Professor, Rajasthan Institute of Engineering & Technology Jaipur
cs.vijay@poornimarietjaipur.ac.in

Abstract:- Since the advent of open channel communication data security is a live and hot research field. However, much of efforts have done by different investigators to secure statistics by utilizing of various tools but still a complete secure system is a dream. In this incorporated effort a naïve technique has converse on the base of combine functionality of two admired data security mechanism into a single frame, crypto-Steganography. Typically near about all obtainable data security methods that use crypto-Steganography based schemes offer a simple procedure, after encryption process approaches takes manual elected random frame/image of cover media and try to improve the quality of frame in which data is hidden but this course of action consume much more effort and time with offering of low act, PSNR value. Sometime to secure same information other frame of elected cover media may be a best option but wrong selection of cover frame degrades the act of build procedure. The proposed approach considers such case with integration of an auto selection procedure that mechanically elects a best suited frame of cover animated file to hide cipher information.

Keywords: Cryptography, Steganography, Data Hiding, DES, AES.

I INTRODUCTION

Data security over an unprotected channel is a big dare for the researchers of relative fields. Rapid set up of innovative techniques and much exploitation of digitalized tools with its services has augment security qualms. However, each one user employs different methodology for sharing secrete data safely, protect message with code words, use firewalls, encryption techniques etc. but due to inadequacy of each approach and arrive of inventive data stealing methods in quick way the mechanisms of data security has face an assorted challenges.

On the other hand related literature of data security field has shown that each accessible scheme associates unique inadequacy and be unsuccessful to protect data in real time communication. Therefore the belongings shortage of data security field has attract an attention of researchers and make it a hot area of research.

II DATA DEFENSE WITH STEGANOGRAPHY METHODS

Steganography is another well-liked mechanism for defense of data. It increases data security to next level of cryptography methods. Where the mechanism of cryptography altered the form of information the Steganography technique conceals the existence of information into a cover media, in an image/video/audio file. The cover media which hide secrete information in it known as stego file. Sender of information transfers this stego file to its recipients using a secure channel [1]. Message receiver performs a turnaround process of file sender to obtain forwarded data. The process is known as the data decryption.

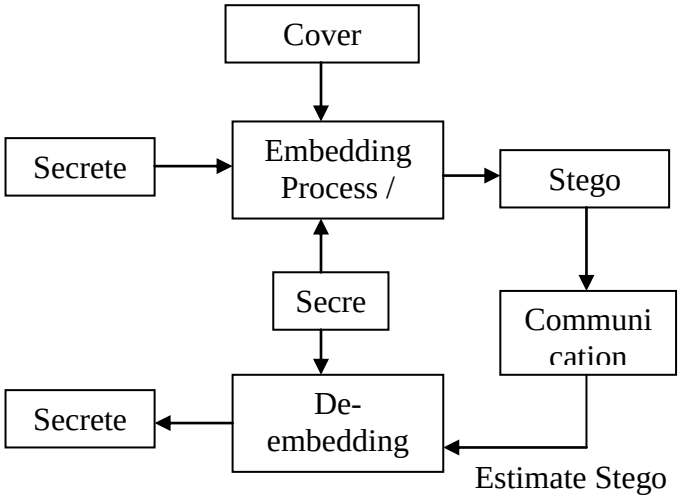


Figure 1 Basic Concept Steganography Scheme

A secrete message may be in form of plain, encrypted text or images. Cover media may be in form of other text, image or audio/video file. A key is generated and shared between communicating parties for securing data against unauthorized access. Guarding of data against detection and removal are two most objectives of Steganography scheme. The first term protection against detection is desirable in condition when someone wants to ensure that the embedded message is not detected by a third unauthorized party. Typically this term ensure the data integrity. Defense against removal make an endeavor to avoid an elimination of concealed data without making it inadequate or corrupting its quality. However, in modern era with advanced techniques the Steganography schemes support all types of digital file formats like text, image and audio/video files but always a high resolution file are more suitable for data hiding because of providing far greater accuracy for the object's use and display [2].

III STEGANOGRAPHY VERSUS CRYPTOGRAPHY

Literature of data defense has shown that both methods are widely accepted and are being used by investigators to secure message from access of unwanted or unauthorized persons. Due to different working methodology of data defense these schemes cannot be evaluate on the parameter that which is most efficient. However both methodologies can judge on the base of services and efficient security of data.

However, in practical no one standalone system is enough to provide the facility of a complete secure system but the concepts of combining the cryptography with Steganography technique can provide two layer of security, where in case of failing the Steganography system the secrete message remain safe because of encoding technique. Thus the proposed approach of this investigation has combined the advantages of both techniques into a single form, use both of technique in a layer form to enhance the security of secrete message. Additionally an integrated method for improving the picture quality of stego file, (video frame) enhances the performance of proposed method in comparison of existing methods

S.no.	Context	Steganography	Cryptography
1	Support File Format	Image, Audio, Text, etc.	Mostly Text Files
2	Message Type can Hidden	Image, Audio, Text, etc.	Mostly Text Files
3	Outcome	Stego File	Cipher Text
4	Attack against Technique	Steganalysis	Cryptanalysis
5	Objectives	Keeping the existence of a message secret	Keeping the contents of a message secret
6	Function	Used for securing information against potential eavesdroppers	Used for Text Securing information against potential eavesdroppers
7	Security services offered	Confidentiality Identification Authentication	Confidentiality a Integrity Identification and authentication Non-repudiation
8	Technology-specific problems	Steganalysis y distribution (except with keyless steganography	Key distribution Law enforcement Cryptanalysis

Table 1.1 Steganography V/s Cryptography

IV Literature Review

Jun Zhang et. al. 2003 [3] have offered an information security method by employing digital watermarking. The authors use different images for depict the performance of their proposed method. Typically the presented approach utilize chaotic map for watermarking and after it hide the information by modifying the appropriate sub band in the wavelet domain.

S. M. Ashar et. al. 2003 [4] intended a hybrid approach for security of an information by engaged the functionality of crypto and steagnography into a single framework. For build an efficient security model the authors have employed compression, cryptographic and hash module.

Typically the implemented approach was derivative of **Yeuan-Kuen Lee and Ling-Hwei Chen** approach **[5]**. The approach perform a encryption of secrete message at first phase and then encrypted message conceal into a 24 bits flue color image. Additionally for improve the act of proposed method the investigators has employ three ladder at embedding time. At the beginning stage the approach estimate embedding capability of opted image and stretch the data while data amount is lesser from embedding capacity.

Hamid Izadinia et. al. 2009 [6] made an endeavor to secure information by apply Steganography mechanism on the base of analytical coding. Typically the authors have conceal the existence of information into amount of quantization error by using Quantization Index Modulation (QIM). They have use different type and size of images to show the effectiveness of proposed mechanism.

Subba Rao Y.V et. al. 2011 [7] use related method of above discussed approach for conceal message into picked cover image file. The authors have randomized the message bits with Linear Feedback Shift Register and have elected the proper set which shows bordering of opted image. The experimental outcomes depicts that intended approach has produced more powerful results in comparison to other obtainable methods.

Daphney Jerly Dsouza and Girish S. 2017 [8] made an endeavor to secure information by employ steganography scheme with QR code. Additionally they have apply AES and LSB mechanism to enhance the level of data security. For safety in key exchanging process they take account of Diffie-Hellman algorithms with the objective of removing middle attack.

V Proposed Approach

Proposed apprach has motivated from the restraints and inadequacies of obtainale data security process which has point up by related literature. As illustrate in previous chapter the connected literature of data security mechanism has shown that huge investigators have made numerous endeavor with different mechansim to secure and enhance safety of secrete information but each and every build algorithm has their unique restraints, employ standalone data security methods to secure information which is not an effective and efficient methodology in real time framework as stated by numerous investigators in literature.

On the other hand most of proposed hybrid mechanism have not provide good quality for stego file which arrouse the attention of attackers and be unsuccessful in real time framework.

Typically proposed approach has gives more focus on pick up an elevation of data protection with preserving good quality of stego file even conceal huge amount of data. With proposed tactic secrete data has remain safe even security mechanism of one phase has crack by somebody

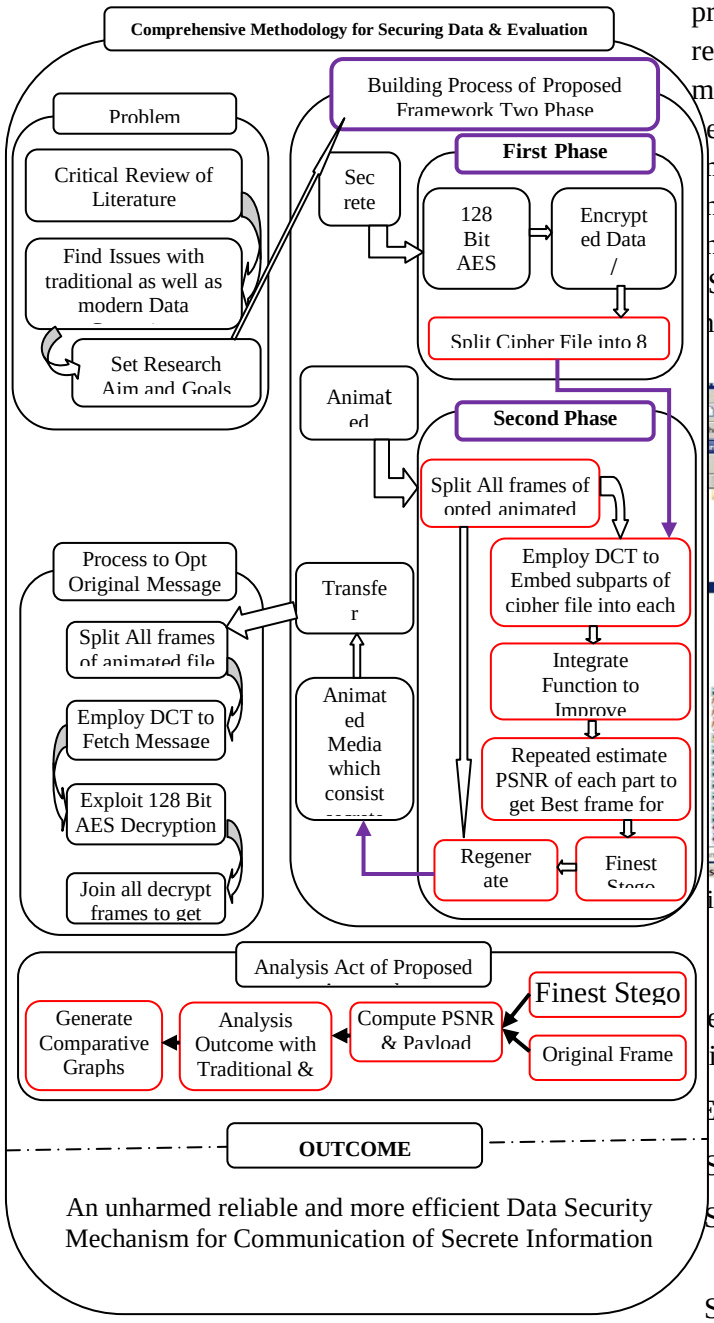
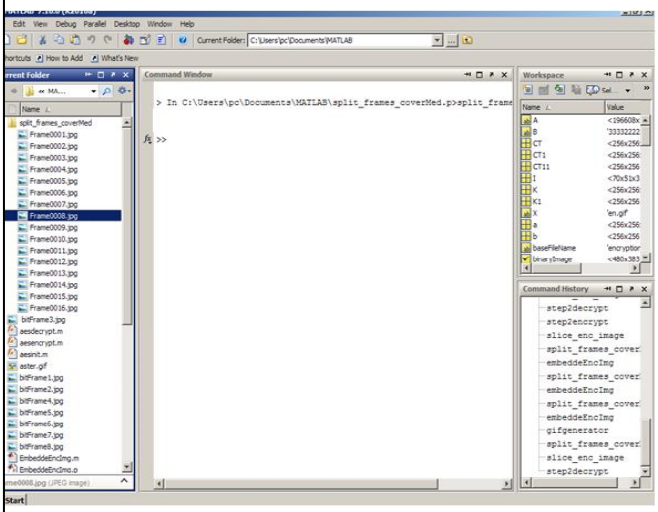


Figure 2 Proposed Methodology for Enhance Security of Secrete Information

The implemented approach splitup all the frame of opted animated file and then carry out a repeated analysis of PSNR after embed all parts of cipher message into each and every individual frame with execution of an picture quality improvement procedure. On the base of relative analysis procedure the build method pick best frame for put out of sight. After finishing of an embedding procedure the appraoch regenrate animated file which is ready for send out to its receiver. To receive an origional message the receiver of an cover animated file has to be erform reverse operation of message hiding and mbedding which is called deembedding and dycryption of n message. With the build procedure only authenticated nd user will be able to receive sended messages and high SNR value validate that proposed mechanism enhance e power of data security.



igure 3 Cracked and Extracted Frames for Enhance Security of Secrete Information

eudo code of proposed algorithm at senser side can be int out as

EGIN

Step 1: Take Secrete message.

Step 2: Defend security of secrete message with AES 128 bit encryption procedure.

Step 3: Increase protection complexity by cracking cipher message into subparts.

Step 4: Opt animated file and extract all frame for conceal an visibility of cipher message.

Step 6: Embed cipher parts of secrete message in extracted frame using DCT.

Step 7: Enhance quality of embedded frame and compute PSNR to opt best one.

Step 8: Cover cipher message into finest worth frame and rebuild animated file.

Step 9: Transfer File to its receiver.

END

Pseudo code of proposed algorithm at message receiver side can be point out as

BEGIN

Step 1: Obtain Animated file which conceal secrete message.

Step 2: Extract all frames of animated cover media.

Step 3: De-embed cipher bitframe.

Step 4: Employ untheticate key for reconstruct bitframe into a unit.

Step 6: Decrypt cipher message using 128 bit AES decryption methodology.

Step 7: Get Origional message.

END

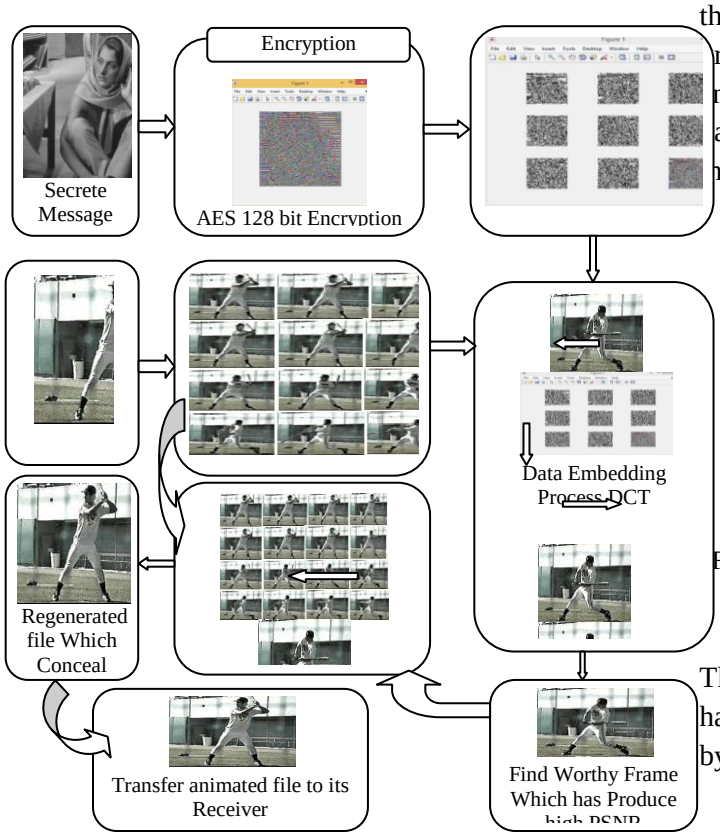


Figure 4 Working Ladder of Proposed Approach at Message Sender and Receiver Side

VI RESULT ANALYSIS

In direction to demonstrate true competence of proposed approach over an accessible data security practices different experiment setups has build with similar data properties as was consumed by existing approaches to explain their performances. Literature related to information security has exposed nearly all propsoed appraoches use disimmilar type of data to show their effeciveness, therefore it hard to compare the performance of new developed algorithm in comparison of existing one, may be new algorithm produce different or low results with the data (secrete information/cover media) as use by existing algorithm.

Proposed Approach Vs Hybrid Method based on 3-DES, DWT & LSB

In accessible approach [9] authors has effectively integrate the functionality of selected methods. The comparative and experimental results have shown that designed approach has produced significant outcomes in terms of PSNR. For the experiment they use different cover media and form of messages, 64*64 and 128*128 image messages size. To demonstrate an actual effort of their designed approach they have perform a comparison against of two other rojected approaches by employ 128*128 message size nd 512*512 size for cover media. Therefore same content as considered in this experiment to analyze an act of ntended approach of this investigation.

(a) Secrete Message (b) Cover Media

Figure 5 Images utilize as Secrete Message & Cover Media in Hybrid Method [9]

The experimental outcomes of this investigation approach has also compared with another two methods as employed by the authors of Hybrid method.

Table 4.3 Proportional PSNR of Proposed, Hybrid & Other Two Approach [9]

PSNR (%)			
. R. D. Farahani & A. Pourmohammad [9], 2013	S. P. Ravi and L. Dhanalakshmi [9], 2015	Hybrid Approach [9], 2016	Proposed Approach
25.18	44.58	49.21	59.70

The following figures depict an significance of proposed approach over an accessible information security method [9].

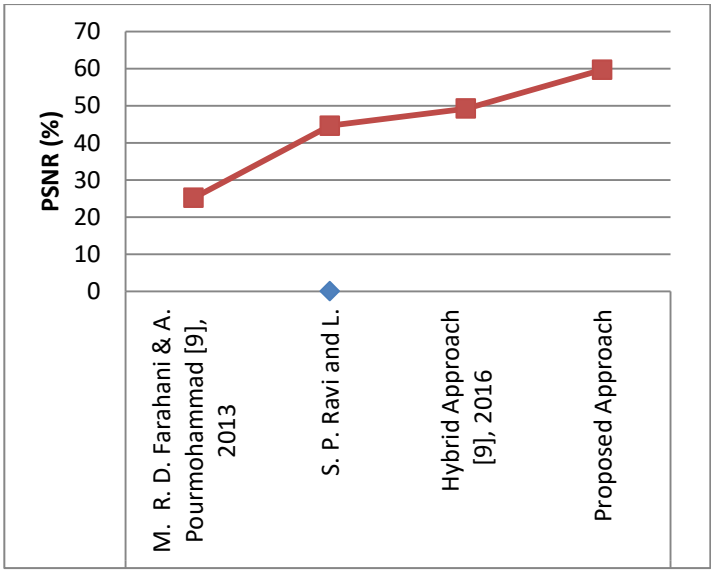


Figure 6 Relative PSNR of Proposed and Other Approaches

The figure depict that proposed approach has outperformed in comparison of all accessible data security methods. To explain the effectiveness of proposed approach with change size of payload messages another experiment has done with the same statistics as employed by SSCBH algorithm [10]

VII CONCLUSION

At initial level approach utilize 128 bit AES encryption mechanism for securing the secrete message and after that it crack cipher information into 8 separated parts and demand a cover media to conceal the existence of cipher information.

The cracking process of cipher information efficiently increase the security level of secrete message but to make it more secure a other optimized security scheme has also exploited in to this investigation work. In addition to encryption of secrete message and it cracking procedure the proposed scheme utilize one other mechanical process that robotically splits the frames of selected animated cover media and elect the best suited frame for hiding the existence of cipher information. Modified versions of Discrete Cosine Transformer (DCT) utilize to embed cipher information. Additionally one other incorporated process, frame optimization method utilizes into proposed mechanism for enhancing the quality of stego frame, frame that hide secrete data in it. Relative simulated outcome confirm that, the anticipated approach has offer high level of security for secrete messages in front of obtainable algorithms with improve PSNR value.

FUTURE WORK

However the experimental results clearly indicate the efficiency of proposed scheme but future work can be in done in following direction.

1. To improve PSNR value utilizes other methods into hybrid framework.
2. To improve QOS of security scheme implement more optimized mechanical process.
3. To improve safety levels of secrete message may utilize higher bit encryption mechanism with a more powerful optimized Steganography scheme.

REFERENCES

[1] Arvind Kumar, Km. Pooja “Steganography A Data Hiding Technique” International Journal of Computer Applications (0975 –8887) Volume 9–No.7, November 2010, pp.-19-23.

[2] P. Paulpandi, Dr. T. Meyyappan “Hiding Messages Using Motion Vector Technique In Video Steganography” International Journal of Engineering Trends and Technology-Volume3 Issue 3-2012, pp.-361-365

[3] Jun Zhang, Ingemar J. Cox and Gwenael Doerr.G “Steganalysis for LSB Matching in Images with High-frequency Noise” IEEE Workshop on Multimedia Signal Processing, issue 1-3, pp.385- 388, 2007.

[4] S. M. Ashar, T M Shah, R. Khalid “Message Encryption With Image Processing” IEEE, 7th International Multi Topic Conference, INMIC 2003, pp.- 7-15.

[5] Yeuan-Kuen Lee and Ling-Hwei Chen. "A High Capacity Image Steganographic Model", accepted by IEEE Proceedings Vision, Image and Signal Processing, 2000, pp.- 288-294.

[6] Hamid Izadinia, Fereshteh Sadeghi, Mohammad Rahmati "A New Steganographic Method Using Quantization Index Modulation" IEEE International Conference on Computer and Automation Engineering, 2009, pp.-181-185.

[7] Subba Rao Y.V, Brahmananda Rao S.Sy, Rukma Rekha N "Secure Image Steganography based on Randomized Sequence of Cipher Bits" IEEE Eighth International Conference on Information Technology: New Generations, 2011, pp.-332-335.

[8] Daphney Jerly Dsouza, Girish S "A method of data hiding in QR code using image steganography", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 4, Issue 3, 2017, pp.- 1111-1113.

[9] Giovani Ardiansyah, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto "Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm" IEEE 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp.- 249-254.

[10] Siddalingesh Bandi, Manjunatha Reddy. H S "Steganography for Secure Communication Using BPCS and HDWT" International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5 Issue I, January 2017, pp.-161-168.