DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5012

ISSN No. 0976-5697

Volume 8, No. 9,November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IMPLEMENTATION OF JSMEA (JOINT SELECTIVE MULTIMEDIA ENCRYPTION ALGORITHM) - A PRIVACY ENHANCING STRATEGY

Rajwinder Kaur
Department of Computer Science & Engg
Sri Sai College of Engg and Technology, Manawala
(Amritsar) Punjab (India)

Rimmy Chuchra
Department of Computer Science & Engg
Sri Sai College of Engg and Technology, Manawala
(Amritsar) Punjab (India)

Abstract: Cyber world plays a vital for exchanging information electronically. Different types of mechanisms and strategies are used for sending different types of information say information may be in the form of text, image, audio as well as video.The main motive is transference of information from the one end to other end must be safe and secure. So, that any third party say hackers or crackers could not access your confidential information and user can send their information successfullythrough secure communication channel. The video trend is more preferable now a days because of its size is large. As three types of mixed data is send through video like image, audio and video. So, it's the duty of security professionals to provide security on all. During online transmission of data, to provide a secure channel is an important factor. For providing secure mode of channel two parameters are mainly considered viz time as well as speed. As per author's investigation, Joint Selective encryption is the best way to achieve high level security during online data transmission via secure communication channel. There are several types of encryption algorithms are used as an example DES, SHA-1, Password hash, 3SEMCS and CAST AES 256 etc. There are many multimedia applications in digital world that requires privacy as an example confidential video conferences, confidential facsimile transmissions, medical image transmission and storage, DVD content protection, Pay-TV, Digital transmission through IEEE 1394 interface, streaming media.Forachieving a high level of security time required for new selective video joint encryption must be less that ultimately helps to improve thespeed of the proposed methodology named JSMEA that is termed as a Joint Selective Multimedia Encryption Algorithm that automatically increases the overall performance of the system.

This thesis introduces new improved algorithm JSME that is termed as Joint Selective Multimedia Encryption for selective image, audio and video encryption. This approach is derived from the standard RC4 algorithm. RC4 algorithm is already used for selective image and text encryption. Presently, this existing approach takes a lot of time that degrades the speed and slows down the system performance. Due to noticing these problems these existing algorithms shows variety of its weaknesses in vulnerable form. This vulnerable form shows attacker can easily launch attack inside the RC4 algorithm when required. So in this concern, this thesis has worked that on the one side to reduce the chances of attack and on another side provide strong selective multimedia encryption within short duration of time that ultimately provide high level of security. This paper has designed the RC4 based new improved enrichment approach to making strong the RC4 algorithm, "Extended-RC4". This approach is based on new KSA and PRGA algorithm process, which are the two stages inside the RC4 algorithm.

Keywords: cryptography, encryption algorithms, selective Multimedia Encryption, Web, Video Conferencing.time and security.

I. INTRODUCTION

Now a days, most of the daily life tasks are handled over cyber channel so to provide security over cyber media during transmission of data is a critical issue. For providing security on confidential data the method of encryption is most commonly used. Generally, two classes of encryption is to be applied as like symmetric encryption and asymmetric encryption. Security professionals can secure their data by utilizing several different types of encryption algorithms as an example ceaser cipher, RSA, mono cipher and poly cipher etc. Such kind of encryption algorithms can be applied on different-2 key sizes [12]. As authors studied in their survey, today's selective multimedia encryption [1] is preferred due to its several distinct features that are listed below:-

- ✓ Provide high level of security.
- ✓ Selected part of content is only encrypted that save time as well as cost.
- ✓ Reduce Processing Overhead.
- ✓ Less Delay.
- ✓ Less Error Correction.
- ✓ Good Compatibility etc.

In addition, the main benefit to utilize selective multimedia encryption [1] is to produce latest research results in different dynamic fields. Most importantly, the results concluded from the previous studies that are to be used in daily real life is the usage of several selective multimedia applications are greater as an example medical image transmission & storage, DVD Content Protection, confidential facsimile transmissions,Pay-TV and streaming media as well [2]. The more use of selective multimedia encryption [1] shows it is latest now in trend in the field of digital world. Even this may also face some problems during implementation of selective multimedia encryption but still works good only for dynamic applications but not working properly in case of static mode of applications. One exceptional case should be considered by the authors there are many practical constraints exists especially in the case of mobile multimedia applications which make such a scheme good but not practically approachable in real life scenarios as an example low battery life, limited device area limit the applications and higher power mobile requirements etc. This is the biggest drawback of mobile multimedia encryption.

Hence, authors, encryption during communication of multimedia content may create a problem when any user establishes their application beyond AES and DES in a binary sequence [4]. Note that, on the other hand if the multimedia content is highly valuable or represents a government or military secrets, the cryptographic security level must be highest as possible. So, the security professionals during designing of encryption algorithms must take care of maintaining the highest level of security of multimedia content on the time of real time transmission of data having limited bandwidth which is not easy to establish.

In this research paper, authors implemented a new designed methodology "JSMEA" that is termed as Joint Selective Multimedia Encryption Algorithm [11] whose purpose is to provide a high level of security within minimum duration of time. So, that prevention of confidential data is to be easily provided from hackers or crackers. Authors implemented JSMEA in DOT NET platform version 2015. The major objective of this research paper is to achieve a highest level of security of confidential data during transmission and save time through a secure communication channel. The practical use of such type of applications is to provide high level of security duringvideo conferencing and video phone calls etc. During implementation of JSMEA(Joint Selective Multimedia Encryption Algorithm) several different types of encryption is used viz.Image encryption[3],audio encryption [5] [6] [7], video encryption [8][10], 3-Step Encryption method [9] collectively.

As authors studied in their review of literature, such kind of practical applications are more demanding for the privacy of confidential information via a secure mode of communication. Hence, authors tested their work the confidential content that can be delivered through cyber world it should be too confidential if security professionals may use their newly developed algorithm named JSMEA (Joint Selective Multimedia Encryption Algorithm).

II. RESEARCH DESIGN

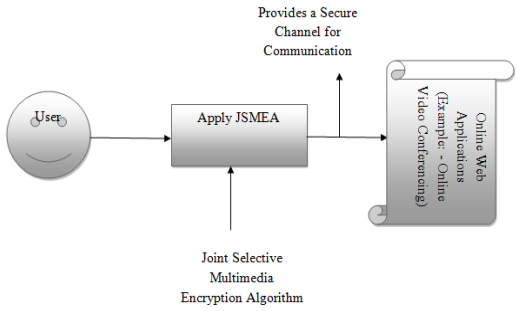

Figure 1: A Roadmap for JSMEA.

III. ALGORITHMIC STEPS FOR JSME (JOINT SELECTIVE MULTIMEDIA ENCRYPTION)

Step -1) Design Hybrid frame (that includes image, text, audio and video type content).

Step -2) Select the portion of an image &divide hybrid frame into three portions.

Step - 3) Then Apply Audio Encryption on The Audio frame.

(Note that N-Audio encryption is applied on Audio frame – whose function is to listen selected music that can be posted automatically to audio file accordingly that specific portion of frame is selected).

Step - 4) After that Video Encryption is applied.

// Confusion Encryption is applied on Video Frame – on simple clicking on CUE button the little bit color is changing & the selected portion is to be saved in C Drive. The condition is web cam software must be installed in the system.

// For applying video encryption the web cam software must be installed on your PC/System).

Step 5) Apply Selective Encryption on hybrid frame&note Computed Time (26 Seconds Consumed).

Step 6) Apply 3SEMCS Encryption on hybrid frame&note Computed Time (10 Seconds Consumed).

Step 7) Apply Joint Encryption on hybrid frame & note Computed Time (1 Second Consumed) that improve performance of the system.

(In the final step, Joint Encryption is applied on single button click on the selected portions of image, text, audio and video & Note Time Count. (That is how much time is to be consumed for joint encryption).

Step 8) End.

IV IMPLEMENTATION OF JSMEA

Step -1) Design Hybrid frame (that includes image, text, audio and video type content).

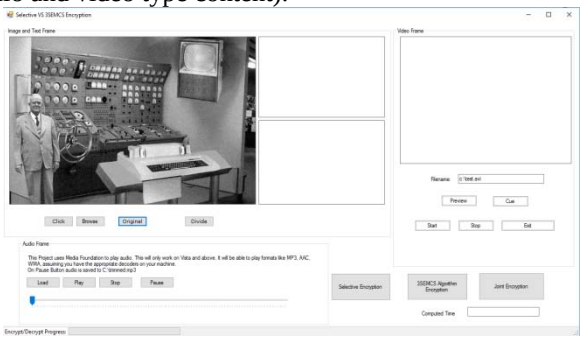

Figure.2: Design of Hybrid Frame.

Step -2) Select the portion of an image &divide hybrid frame into three portions.

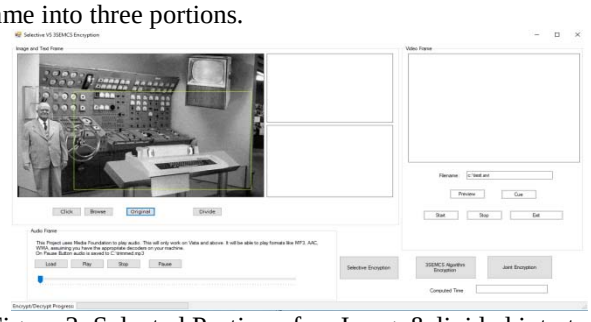

Figure.3: Selected Portion of an Image&divided into two parts.

Step - 3) Then Apply Audio Encryption on The Audio frame.

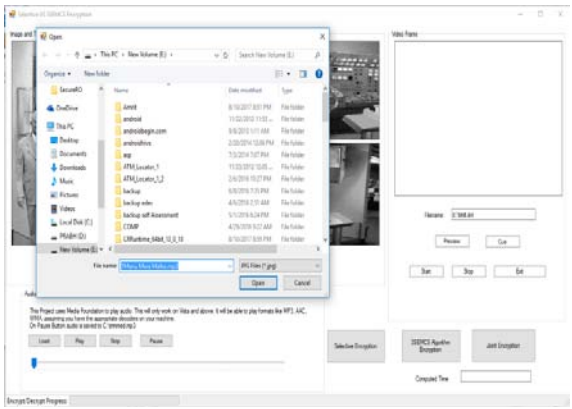

Figure.4: Apply Audio Encryption.

Step - 4) After that Video Encryption is applied.

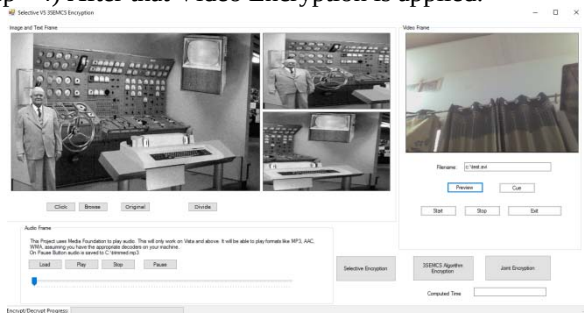

Figure.5: Apply Video Encryption.

The role of web cam is to preview
Here, Cue is most important factor…

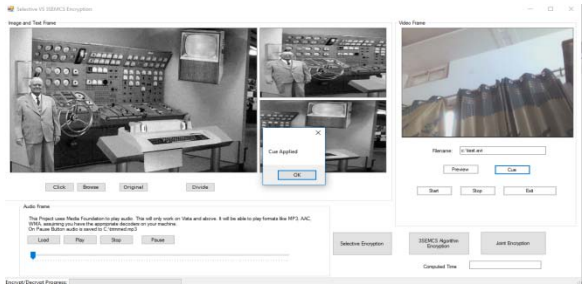

Figure.6: Apply Cue while clicking on Cue Button.

Step 5) Apply Selective Encryption on hybrid frame&note Computed Time (26 Seconds Consumed).

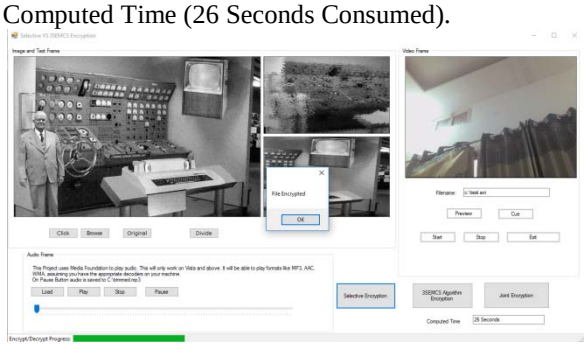

Figure.7: Apply Selective Encryption collectively on Hybrid Frame.

Step 6) Apply 3SEMCS Encryption on hybrid frame&note Computed Time (10 Seconds Consumed).

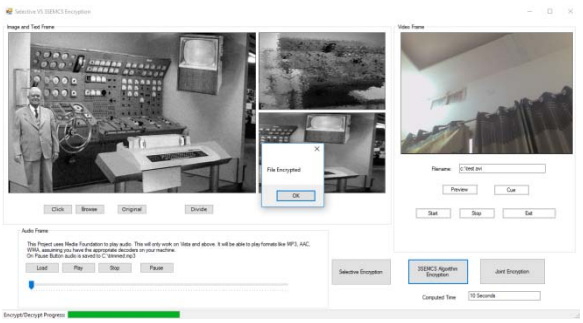

Figure.8: Apply 3 Step Encryption Algorithm.

Step 7) Apply Joint Encryption on hybrid frame & note Computed Time (1 Second Consumed) that improve performance of the system.

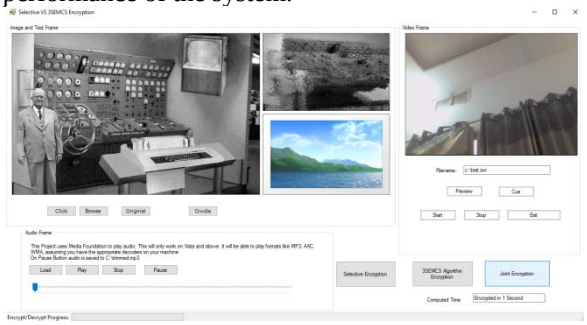

Figure.9: Apply Joint Encryption on Hybrid Frame Collectively.

Step 8) End.

V. CONCLUSION

A new joint selective multimedia encryption algorithm (JSMEA) is proposed. The motive to design this new algorithm is to provide security to confidential information during information exchange through cyber medium.The main significance to propose this algorithm is to provide secure communication between two parties within short span of time. As results produced by authors shows while running joint selective multimedia encryption algorithm takes less time (sometimes exception case - or you can say take less than one minute) that can automatically reduce the chances of attacks launch by attackers.Ultimately, this proposed algorithm helps to protect the sensitive part of multimedia data when encryption is applied. Multimedia encryption can be applied either by public key cryptography or private key cryptography. And the size of the key in both of the cases may consider any & in special case multiple keys can be applied randomly. The proposed algorithm has a large key space to resist brute force attack. The algorithm is very sensitive to its secret keys.

VI. FUTURE SCOPE

In future, this work can be extended by considering bulk of hybrid frames into mainframeon the time of browsing and select some sensitive part of multimedia data from the given hybrid frame and apply joint selective multimedia encryption. It will further provide a sufficient amount of security or high degree of security within small duration of time that automatically improves the speed and performance of the system.

VII. REFERENCES

[1]Ravi Raj B.Vyavahare and AmitJ.Bajaj,"Study of secure data transmission using Audio File", International Journal of advanced research in computer and communication engineering, Volume 4,Issue 2,Febuary 2015.

[2] Stinson, D.R.: Cryptography: Theory and Practice. CRC Press, Boca Raton (2006).

[3]Suoxia Miao and Lingfeng Liu," A new Image Encryption Algorithm based on Logistic Chaotic Map with varying parameter", Springer plus, 2016.

[4]Wen, J., Luttrell, M., Severa, M.: Access control of standard video bitstreams. In: Proc. IEEE Intl. Conf. Media Future, 2001.

[5] O P Verma, RituAgarwal, DhirajDafouti, ShobhaTyagi, "Performance Analysis of Data Encryption Algorithms", IEEE, 2011.

[6] Dr.S.A.MRizvi, Dr.SyedZeeshanHussain, Neeta Wadhwa, "Performance Analysis of AES and Twofish Encryption Schemes", International Conference on Communication Systems and Network Technologies, 2011.

[7] Khaldoon M. Mhaidat, Mohammad A. Altahat, Osama D. Al-Khaleel, "High Throughput Hardware Implementation of Threefish Block Cipher on FPGA".

[8] Ajay Kulkarni,Saurabhkulkarni," Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study",Int journal of computer applications,Vol.65,No.1 ,March 2013.

[9]ShubhamChuchra&Manraj Singh," Proposing 3SEMCS- Three Step Encryption Method for Cyber Security in Modern Cryptography", Vol.139, No.6, April 2016.

[10] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf

[11] RajwinderKaur and RimmyChuchra," An Improved Algorithm For Joint Selective Multimedia Encryption (JSME) - A Privacy Enhancing Strategy", Vol.8, No.7, July-Aug 2017.

[12]A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J.Quisquater. "Overview on Selective Encryption of Image and Video: Challenges and Perspectives".