International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

Implementation of a Secure Selective Image and Voice Encryption (SSIVE): - A Privacy Enhancing Strategy

Saajan Kumar
Department of Computer Science and Engineering
Sri Sai College of Engineering and Technology,Mannawala(amritsar), Punjab (India)

Date of Submission: 03-04-2024 Date of Acceptance: 15-04-2024

ABSTRACT: In the recent decades most of the tasks are rapidly transferred into the digital world. This surge of digital content, especially in the era of multimedia applications is continuously growing and plays a crucial role. So, the data protection of digital data such as image, audio and video has become a significant challenge. The basic security requirement of these innovative platforms is to provide safer communication by the network professionals between the two or more parties lies on the same or different internet channel. As studied in the literature review, audio encryption uses very sensitive data, so it needs to provide security very carefully. The audio information utilizes float data type which strongly correlates with adjacent times so its security transfer through different networks is the most preferred research field. This paper fundamentally concentrates on selective image and voice encryption collectively. This paper implemented "SSIVE" which is termed as "Secure Selective Image and Voice Encryption" algorithm whose prime objective is to provide a high level of security within a short span of time. In this paper, authors consider two control parameters viz. size of the selective image and time taken for the encryption. Hence, a combination of different encryption algorithms like 3SEMCS, DES, SHA-1, AES and joint encryption also helps to increase/enhance the security of the data to some extent. In short, the authors say implementation of the proposed algorithm "SSIVE" increases overall security.The main advantage of encryption is to reduce the amount of data to encrypt (use only subset for encryption) for providing a sufficient level of security.

KEYWORDS: Encryption algorithms, selective Image encryption, Selective Voice Encryption (audio encryption), Time, Security, computed encryption time.

I. INTRODUCTION

In the last few decades, authors might have seen the dependency over electronic wire increase with the passage of time. Different types of communication channels are used as an example wired and wireless. Each communication channel has its own set of requirements and parameters that determine its quality of service (QOS). Whenever a user had to transfer data online, security became an important issue [13]. Further, different types of algorithms, methods, strategies, and techniques [15] are used by the network professionals for safe communication. In this paper, authors want to provide high-end security by utilizing the concept of encryption. As surveyed a variety of encryption algorithms are available in the market viz. AES (Advanced encryption standard), DES (Data encryption standard), RSA, Triple DES, SHA [14] and many more exits. There are many benefits of using the concept of encryption like cheap to implement, saves you from regulatory fines, help to protect remote workers and the most important one is it helps to increase the integrity of data which ultimately helps to increase the consumer trust.

This paper presented a way to provide safer communication through image and voice encryption. When encryption is applied over more than one type of data, say image or voice, then it is termed as a "multimedia encryption" [16] where multimedia encryption is a combination of both such as cryptographic techniques and multimedia techniques. The main advantage to utilize these techniques is its dynamic behavior and its wide range of practical applications coverage in the digital world as an example confidential video conference, confidential facsimile transmissions, medical image transmission and storage, DVD content protection, Pay-TV, Digital transmission through IEEE 1394 interface, streaming media [16] etc.
In this research paper, authors implemented a new designed methodology named "SSIVE" [16] which is termed as "Secure Selective Image and Voice Encryption" whose main purpose is to provide a sufficient level of security within a short duration of time. The implementation of newly designed methodology uses image and voice encryption collectively by simply adding noise in the audio file and roughness in the image file [3]. The prime objective of this paper is the exchange of confidential information for providing safer communication channel within a short span of time. In short, authors say "Time" is an important parameter which is computed when different types of encryptions (SSIVE >> 3SEMCS >> Joint encryption) is applied. The practical implementation of multi-level encryption helps to contribute for the reduction of online attacks and provides a sufficient or you can say a top level of security within a short span of time. Hence, it is necessary to create a strong selective audio encryption strategy to protect the data from various types of existing threats.

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

II. Review of Literature

Dai Wanying & Xu Xiangliang et al 2022:- In this paper, authors discusses about the role of noise signals in any audio file. The interference of unwanted/extra noise signal creates a distraction which further helps to weak the strength the signal. So, to improve the quality as well as strength of the audio file here authors purpose a new Chen memristor chaotic system that solves the periodic window problems, such as the limited chaos range and nonuniform distribution. The experimental results of new system is suitable for different types of audio signals.[1]

Abdallah A.Hanaa & Meshoul Souham et al 2022:- Authors proposes a new multi-layer cryptosystems scheme which join audio signals with other signals like speech signals. The major objective of this paper is to provide security from unauthorized access. All the three levels of encryption is considered feature of newly proposed scheme. It is important to note that as the levels of encryption is increased then security automatically increases.[2]

Albahrani Abbas Ekhlas & Alshekly Karam Tayseer et al 2021:- In this paper authors discusses about various encryption and decryption techniques. After studying about the different algorithms in detail a comparative analysis is performed with the newly proposed algorithm which is completely based on chaotic maps concept.[3]

Zhou Xiaodong &Wei Chao et al 2023:- As authors analysed s the dependency over the electronic wire is increases day by day hence digital media requires more attention. In this paper, authors discusses about various chaos based encryption algorithms also proposes a new algorithm for encryption whose results prove a higher level of security along with actual encryption of multimedia digital audio. [4]

Wu Rui, Gao Suo &Wang Xinguan et al 2022:- Authors proposes a new algorithm for audio encryption which is chaos based and named as "AEA-NCS". A 2D-Logistic-nested-infinite-collapse (2D-LNIC) is proposed by combining an infinite collapse map (1D-ICM) and a logistic map. 2 D-LNIC generates a keystream where diffusion and scrambling is performed simultaneously which further helps to enhance the security as well as performance of the newly proposed algorithm.[5]

L. Srividya & Sudha N.P et al 2016:- In this paper, authors surveyed about the different audio encryption techniques and found there are some flows are still present which actually responsible for weaken the strength of the algorithm so need to cover the gap and increase the strength of the algorithm researchers has need to focus on some specific parameter son the time of designing of encryption algorithm . So that encryption algorithm work well or faster in future. [6]

Mandi.V Mahalinga & Arpita.K. B et al 2022: - In this paper, authors use Pseudo random noise signal for encryption. The working of generation of pseudo random numbers are done by two interconnected Linear feedback shift registers. "XOR-Operation is used for the encryption and decryption of any audio signal in MATLAB. Hence, the encrypted histograms show better signal distribution like white noise which ensures more security. [7]

Tamimi . A Abdelfatah & Abdalla.M Ayman et al 2014: - In this paper, authors tested this audio shuffle encryption algorithm on different audio files of different sizes. Its results show this new designed algorithm is more effective for encrypting audio files which may either be of high quality or medium quality. [8]

Alghamdi Saeed Ali Abdullah et al 2021:- Here, authors studied about the backbone of multimedia technology is speech, audio, telephony and video conferencing . A variety of algorithms are used to provide prevention from hackers. In this paper, authors propose a new synchronization scheme for the unpredictable fractional order method. The major objective of this paper is to check the conduct against threats and after that compare with other classical encryption algorithms.[9]

Barua Nirzar & Kabir Ahasan .Md et al 2022:- In this paper, authors considers an audio file in an image format along with private key. Due to bulky in size an audio file process audio signals in the form of image format. The main benefit is to enhance the level of security when audio file is saved in the form of image format. The white noise and compression adds are easily removed by using filers. [10]

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

Singh Manraj and Kumar Amit et al 2015: - In this paper, authors have main concern is to provide a highest level of security by utilizing different types of encryption algorithms. 3SEMCS which is termed as Three Step Encryption Method for Cyber Security encryption algorithm is designed. This newly designed methodology runs on private browser called "RIMROCKS" whose main function is to provide security from the phishing sites. nly authenticated sites will be run on personnel browser and others fake sites or phishing sites will be automatically blocked by the phish tank.[11]

Kumar Pramod and pateriya Pushpendra et al 2012:- Here,authors introduced RC4 Enrichment Algorithm Approach for selective image encryption. This algorithm is derived from the standard RC4 Algorithm. The prime role of new RC4 enrichment approach is to provide a high level of selective image encryption called "PC1-RC4". The working of this newly proposed algorithm is based on 2 different stages viz. KSA and PRGA inside standard RC4 Algorithm [12].

III. Research Design

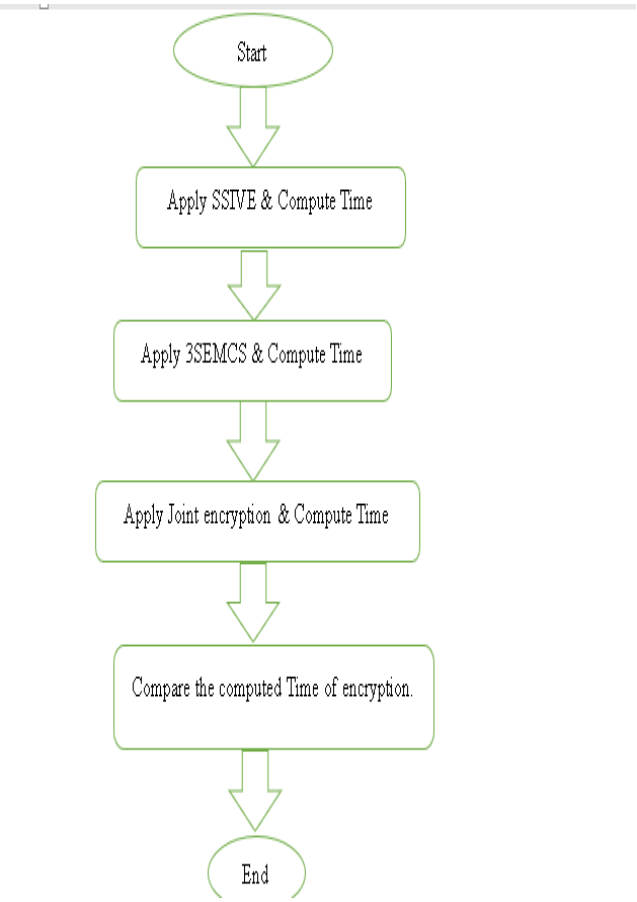


Figure.No.1: A road-map for Image and Voice Encryption.

IV. Implementation of SSIVE(Secure Selective Image and Voice Encryption)

Steps Enabled in SSIVE (Secure Selective Image and Voice Encryption).

S-1) Choose any selected area of an image for implementing the selective encryption say image may be static or dynamic. Where static image is Given image shown in the below given screenshot in figure.no.1 & dynamic image means you can choose any image randomly through camera functionality(dynamic image may be any live image) which can be shown in the below given screenshot having figure no.2. In other words, static image can be easily selected on simple mouse button click.

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

Figure.No.2:- For choosing static image :- on the click on browse" button.

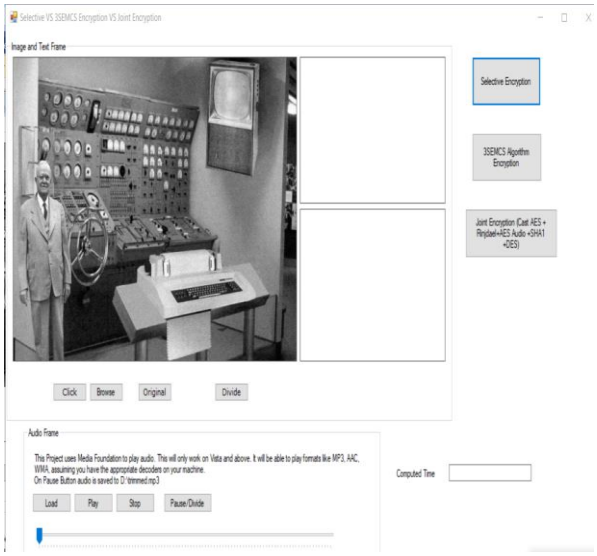
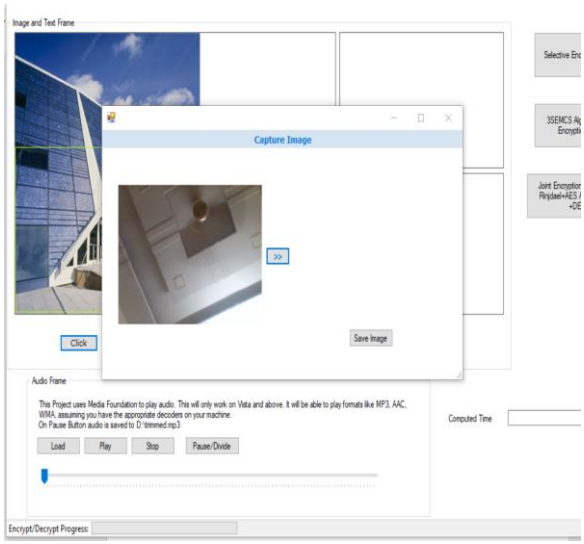
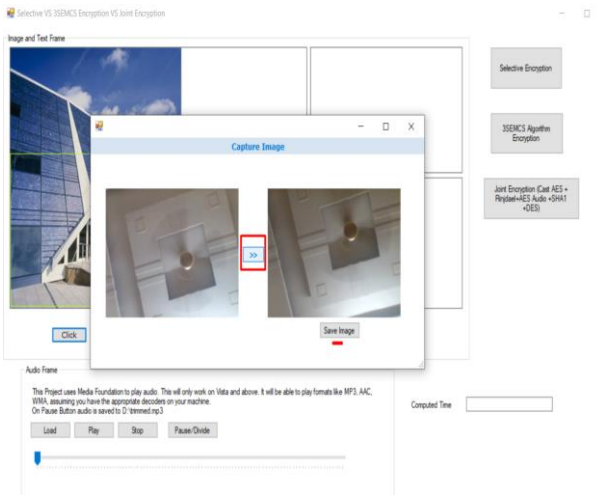


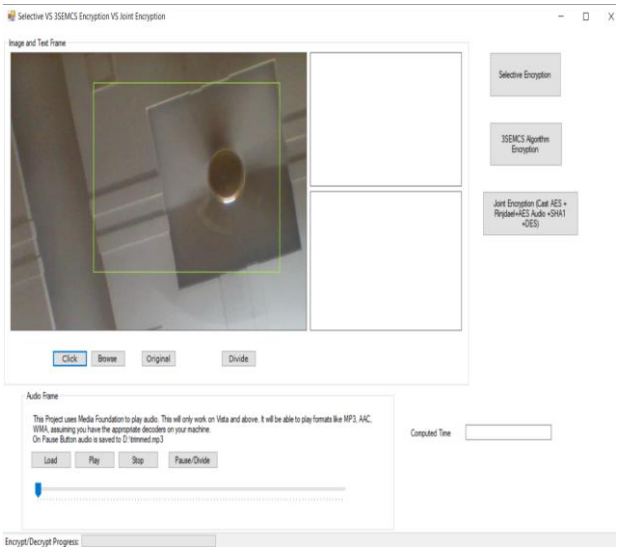
Figure.No.3:- For choosing dynamic image :- record any Live image randomly through "Camera Capture Functionality" in WEB CAMERA.



A) Save live recorded image

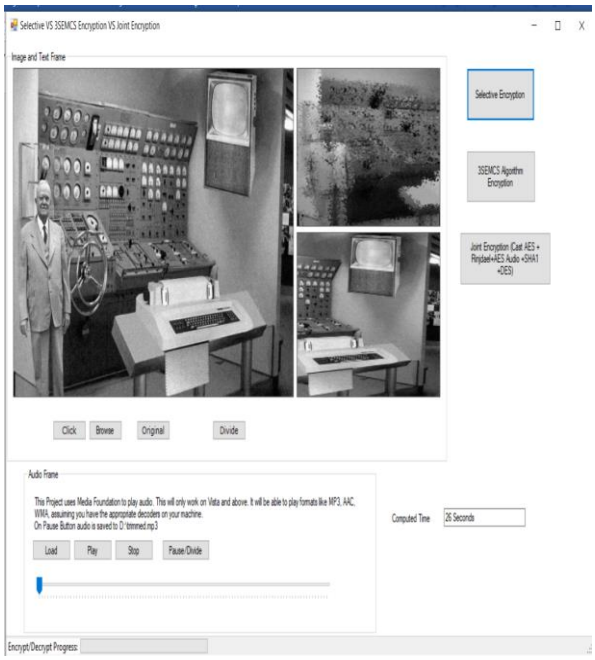


b) Now, select some portion of the image for applying "selective encryption".

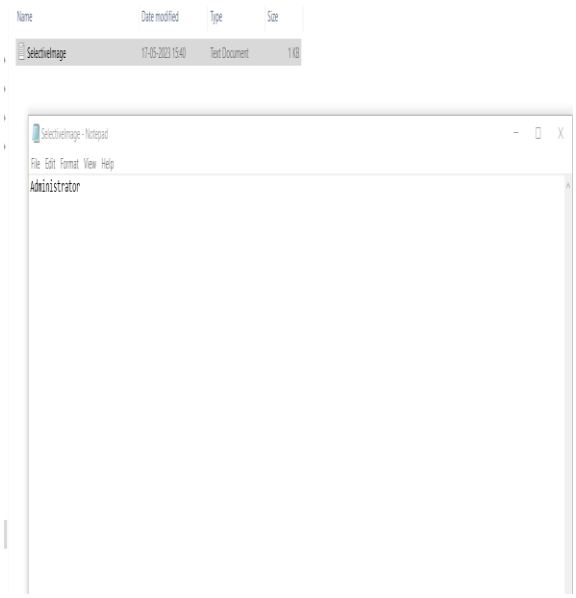


International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

Step-2) Once a selective area of an image is decided, then divide into 2 portions.

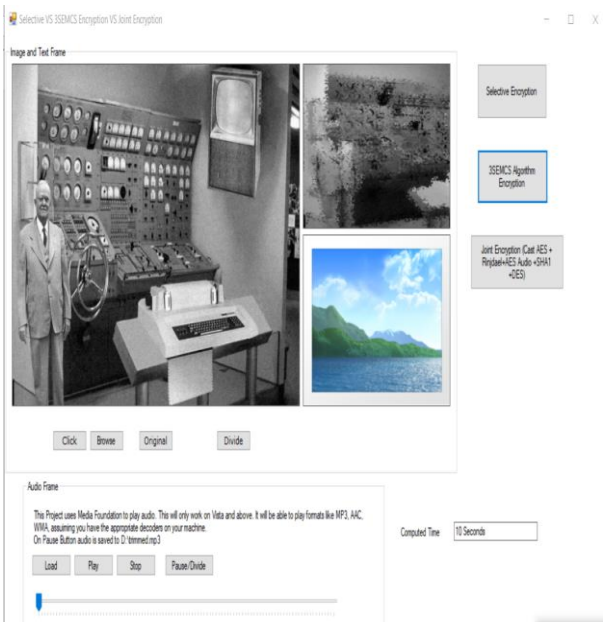


Step-3) Compute the time of processed selective image (26 seconds) along with the text image details which is hidden and displayed in the form of some keyword say for example "Administrator".

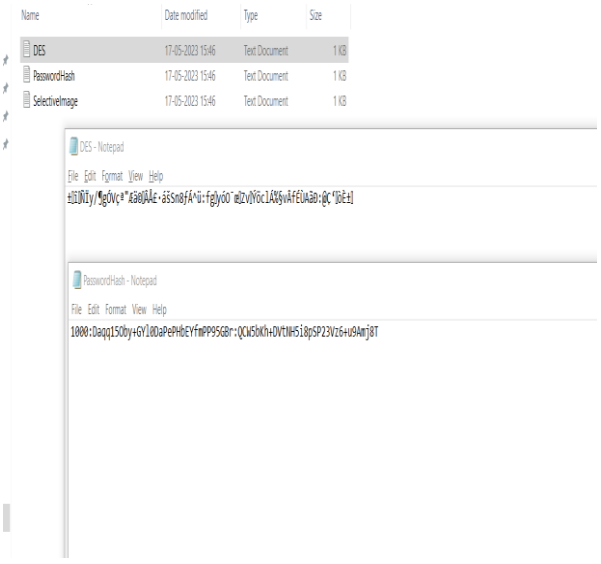


Step-4) Apply 3SEMCS (3-Step encryption method for cyber security) for the 2nd portion of a selected image.

& compute the time taken in selective image encryption.



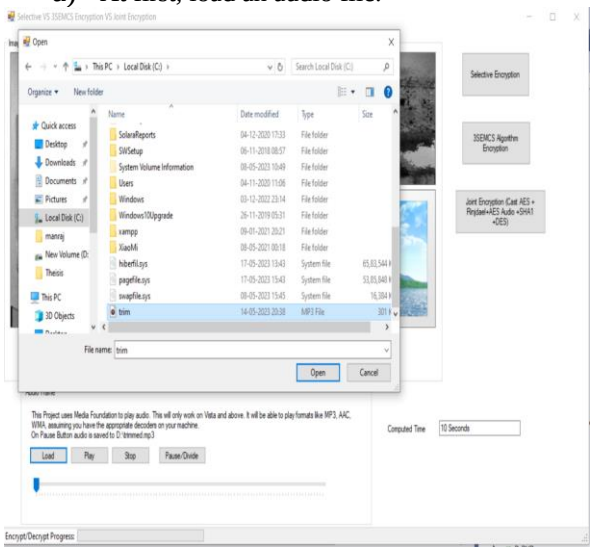
Step-5) See, in the back-end , selective encryption shown in multiple files form which is named as a DES(data Encryption Standard) , password & hash.



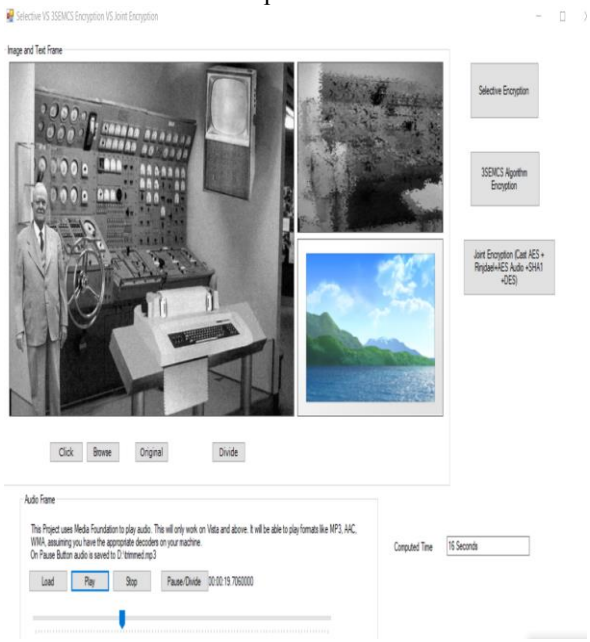
Step-5.1) Now, apply Joint Audio Encryption (which is a mixture of NAudio AES, CAST AES 256, Rinjdael, SHA1, DES).

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

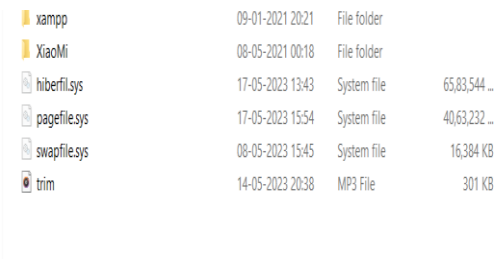
a) At first, load an audio file.



b) Once, file is loaded, then select any audio file for "trim mp3 file".



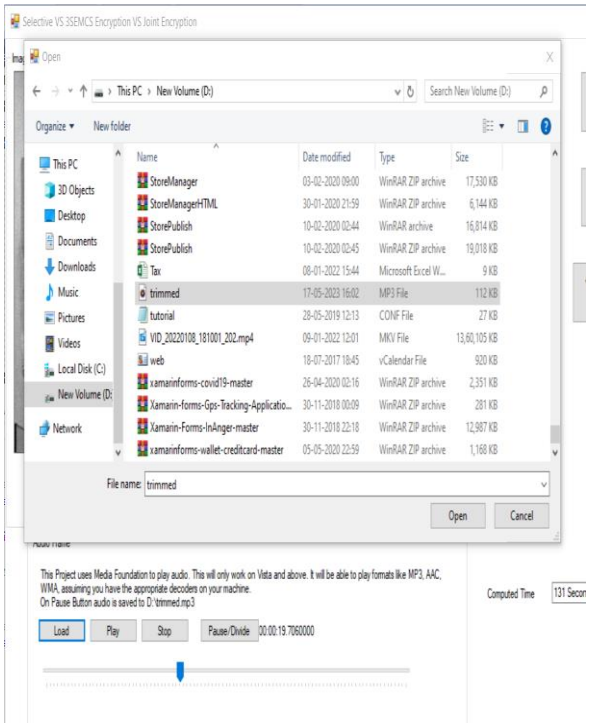
Note: - we can play and stop audio anytime & also compute time taken for selective encryption by the audio file.
See, the original file size is 301 KB and it takes only 16 seconds or the encryption.



On the click of "Pause button", audio file is divided and save by the file name "trimmed file in D Drive".
d) After that click on pause/divide button for reducing the size of audio file through mp3 file cutter which further helps to generate a "trimmed file".
Hence, audio is divided and saved in to the "Trim file" which can be shown in the below given screenshot:-

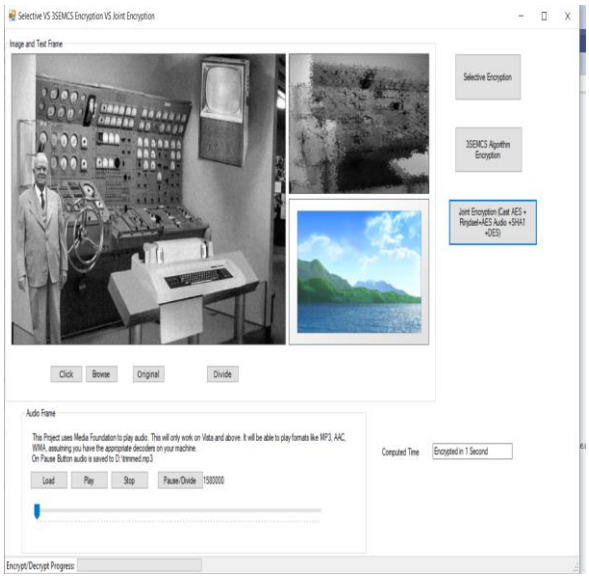
e) Now, check the file size and compare with the original file which is reduced o 112KB where the original size of an image was 301 KB.

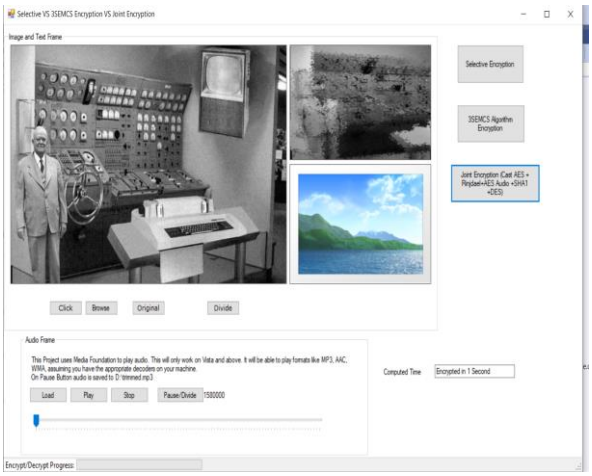
International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com



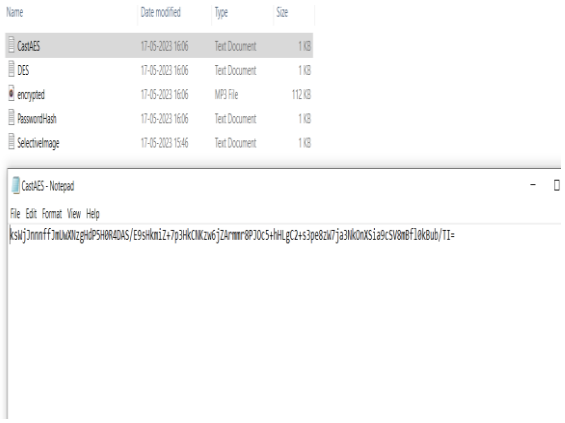
Note: - how much time an audio file takes for selective encryption it all depends on the minimum and maximum size of audio file.

Step-6) Now apply Joint encryption & compute time taken after applying the joint encryption it hardly takes 1 second which is too minimum span of time.





Step-7) In the back end, audio encryption save some related details has file named *"CASTAES"* which is encrypted audio file.



Step8) End.

V. Results and Discussions

he outcomes of this research have provided insight into the difference in the computed time when different types of encryption say SSIVE, 3SEMCS and joint encryption is practically implemented. However, individually time is calculated in all 3 different cases of encryption. This section represents how the time taken by encryption process varies when different types of encryption algorithms is applied. The benefits and limitations of encryption is also discussed.

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 2, Mar.-Apr., 2024 pp: 207-214 ISSN: 2584-2145
www.ijemh.com

VI. CONCLUSION

In this paper, an effort has been made to create an understanding of different encryption algorithms based on different parameters consideration viz. size of the encrypted image, time & performance etc. The present research of this paper implemented newly designed algorithm named "SSIVE" which is termed as Secure Selective Image and Voice Encryption. The prime advantage of this algorithm is to ensure the highest level of security within a short span of time. The other main purpose to implement this newly designed algorithm "SSIVE" is to reduce the time of data encryption by applying selective data encryption. Hence, multi-level joint encryption facilitates us to achieve the highest level of security.

REFERENCES

[1]. Dai Wanying & Xu Xiangliang, , Audio encryption algorithm based on Chen Memristor Chaotic System, MDPI, Discrete and continuous Memristive nonlinear systems and symmetry, December 2022. DOI :- https://doi.org/10.3390/sym14010017

[2]. Abdallah A.Hanaa & Meshoul Souham, A Multi-layered Audio Signal Encryption Approach for Secure Voice Communication, MDPI, Advances intelligent systems and networks, December 2022.

[3]. Albahrani Abbas Ekhlas & Alshekly Karam Tayseer, A review on audio encryption algorithms using chaos maps based techniques, Journal of cyber security and mobility, November 2021.

[4]. Zhou Xiaodong &Wei Chao, A study of encryption for multimedia digital audio security, international journal of advanced computer science and applications,2023.

[5]. Wu Rui, Gao Suo &Wang Xinguan, AEA-NCS: An audio encryption algorithm based on a nested chaotic system, Chaos, Solitons & Fractals, ELSEVIER, December 2022

[6]. L Srividya & Sudha N.P, Literature Survey on recent Audio Encryption Technique, International Journal of Electronics and Communication Engineering and Technology, IAEME Publication, December 2016.

[7]. Mandi.V Mahalinga & Arpita.K.B, Effective audio encryption using Pseudo Noise Generation Architecture, Journal of pharmaceutical negative results,2022.

[8]. Tamimi . A Abdelfatah & Abdalla.M Ayman, An Audio Shuffle-Encryption Algorithm, Proceeding of the World Congress on Engineering and Computer Science, October 2014,USA.

[9]. Alghamdi Saeed Ali Abdullah, Design and Implementation of Voice Encryption System using Fractional-Order Chaotic Maps, International research Journal of Modernization in Engineering, Technology and Science, June 2021.

[10]. Barua Nirzar & Kabir Ahasan .Md, Encryption and Decryption of Audio by changing properties and noise reduction, International journal of Innovative Science and Research Technology, September 2022.

[11]. Singh Manraj and Kumar Amit. Proposing 3SEMCS- Three Step Encryption Method for Cyber Security in Modern Cryptography. International Journal of Computer Applications, US, April 2015.

[12]. Kumar Pramod and pateriya Pushpendra. RC4 Enrichment Algorithm Approach for Selective Image Encryption. International Journal of Computer Science and Communication Networks May 2012.

[13]. Kumar Atul & Dua Mohit, Audio encryption using Chaotic map based dynamic diffusion and double DNA encoding, Applied Acoustics, Elsevier, February 2023.

[14]. Sadkhan . B Sattar Eng & Sherbaz – AI Ali, Chaos based cryptography for voice encryption in wireless communication, Research Gate December 2014.

[15]. Pawar.B Vishakha & Tijare . A Pritish, A review paper on audio encryption, International Journal of Resesrach in Advent Technology, December 2014.

[16]. Parabhjot Kaur, A Secure Selective Image and Voice Encryption (SSIVE): Privacy Enhancing Strategy, International Journal of Computer Applications, November 2023.