# A Secure Selective Image and Voice Encryption (SSIVE): Privacy Enhancing Strategy

Parabjot Kaur
Department of Computer Science and Engineering
Swami Premanand Mahavidyalaya, Punjab (India)

## ABSTRACT
Over the last few years there has been explosive growth in the era of network security. As seen most of our daily life tasks are handled over the electronic wire(e-wire)/digital wire now a days & different types of users are exists on the same channel in terms of hackers, crackers, authentic users, any professional or worker, student who may be a learner, geek (who is expert in net surfing), social butterfly(who most of the time preferring the social media for daily life communication ) & entertainment buff ( who are intermediate internet users). Different types of users are performing different types of jobs as an example is a hacker is always try to gain unauthorized access for stealing information in order to commit crimes. So, to provide security on the network becomes a global issue in the cyber world/digital world. This research paper discusses about the different types of image and voice encryption algorithms used in different disciplines & also proposes a new algorithm named "SSIVE" which is termed as "Secure Selective Image and Voice Encryption" whose main/fair objective is to provide a high level of security within a short span of time that automatically increase newly proposed algorithm performance. The primary advantage of selective image and voice encryption is to reduce the amount of data to encrypt (use only subset for encryption) for providing a sufficient level of security. The Practical use of this new designed methodology is medical science applications, military forces where image protection is required at high rate. The complete working of this new designed methodology depends on three step encryption algorithms used for cyber security (3SEMCS). Hence, the selection of parameters which are considered on the time of encryption is consequential.

## Keywords
Encryption algorithms, selective Image encryption, Selective Voice Encryption, Time, Speed, Security, memory consumption, computed encryption time, execution time.

## 1. INTRODUCTION
Selective encryption [10] means only a sensitive part of the data is encrypted and can only be decrypted by the authenticated or registered users. The main objective of this concept is to provide a sufficient level of security & produce more efficient results. The main purpose to utilize encryption is to achieve "API" which is termed as "Authentication-Privacy-Integrity". Generally, two types of encryptions is used by the network professionals viz. symmetric and asymmetric encryption.[11] A single private key is used by the sender and receiver in case of symmetric encryption. And in case of asymmetric encryption a combination of public and private key is used. As authors seen a variety of encryption algorithms are available now a days as an example AES (advanced encryption standard), DES (Data encryption standard), RC4, blowfish and MD5[2] etc. It all depends on the network professional at which level security requires? This paper presented about the selective image and voice encryption. When we considered collectively then it is termed into "multimedia encryption". Multimedia encryption [16] provides security against confidential data & prevent our data from unauthorized access. Basically, multimedia encryption [16] includes both cryptographic techniques and multimedia techniques. The main significance to utilize multimedia encryption is to provide latest results dynamically. Due to its dynamic behavior, it covers a wide range of multimedia applications in digital world that requires privacy viz. confidential video conferences, confidential facsimile transmissions, medical image transmission and storage, DVD content protection, Pay-TV, Digital transmission through IEEE 1394 interface, streaming media [17] etc.

As authors had been seen in past decades & explore about the current scenarios most of the tasks are handled over the electronic wire as an example online class, online banking, online reservation, online food ordering & online selling and purchasing etc. Such kind of sites uses too confidential information (like passwords, pin codes and payment information and some personnel information) so to provide security from the third-party access who may be any hacker or cracker become too important issue.

In this research paper, authors propose a new designed methodology named "SSIVE" which is termed as "Secure Selective Image and Voice Encryption" whose main purpose is to provide a sufficient level of security and produce more efficient results. The prime objective of this paper is to exchange confidential information through a safe and secure communication channel (SSC). The main benefit to utilize "SSIVE" is to provide a safe mode of communication. A variety of parameters are considered in the selective image and voice encryption viz. encryption time, memory consumed, speed, performance, throughput, computed encryption time & execution time etc. Hence, this newly designed methodology "SSIVE" helps to reduce the number of online attacks and provide secure communication channel (SSC) along with a high end level of security.

## 2. REVIEW OF LITERATURE
**Ayoup Ahmed & Hussein Amr et al 2016: -** In this paper, authors discuses about selective image encryption and how it is important in various applications as they analyzed full image encryption is too massive. They proposed a technique which reduce execution time & increase robustness of encrypted image.[1]

**Zia Unsub & McCartney Mark et al 2022: -** Here, authors suggested when move towards image encryption then instead of using AES, DES and RSA which are standard encryption algorithms we have to use "Chaos-based encryption techniques" because of these techniques have good computational efficiency.[2]

**Massoudi A & Lefebvre.F et al 2008:-** In the past decades, authors analyzed due to high transmission rate and limited bandwidth standard encryption algorithms shows own inadequate behavior. In addition, when authors considered a

theoretical background, number of challenges are also found in case of selective encryption in different applications.[3]

**Panzade Prajwal & Takabi Daniel et al 2022:-** Authors discussed about how encryption is used in the era of machine learning without disclosing their inputs. They also analyzed the performance of the encryption algorithms in the different applications of machine learning.[4]

**Alluhaidan Saleh Ala et al 2022: -** This paper considered an example of healthcare industry where crucial data say medical records of patient's is stored. As E-heath security also demand for CIA features which means consistency, integrity and authentication which ensure data is not accessed by any unauthorized people. And it will be secure at the server end. Different sample tests are applied on the MATLAB simulation environment for testing its behavior with the newly proposed approach named "ITPKLEIN-EHO Approach".[5]

**Alothman Basil Raya et al 2015: -** In this paper, authors consider two types of encryption algorithms viz. symmetric and encryption algorithms and perform comparative analysis on both types whose main purpose is to provide security when data is transmitted through electronic wire. The type of data which is going o be transmitted may be of any type say image or video.[6]

**Miao Suoxia and Liu Lingfeng et al 2016:-** Authors used shuffling method for showing chaotic behavior. The logistic maps are one kind of one-dimensional maps and have already been widely used in image encryption.[7]

**Chuchra .R and Seth R.K. et al 2015: -** Different types of databases attacks are discussed in this paper. For the enhancement of password security during sign_in is the main idea of the authors. The proposed methodology named "TESA" which is termed as Three step encryption algorithm" whose function is to provide a high level of security on the time of account accessing. The whole functionality of designed methodology depends on automatic hash address generation.[8]

**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 a private browser called "RIMROCKS" whose main function is to provide security from the phishing sites. only authenticated sites will be run on personnel browser and others fake sites, or phishing sites will be automatically blocked by the phish tank.[9]

**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 [10].

**Verma O P, Aggarwal Ritu and Tyagi Shobha et al 2011: -** On the basis of different parameters like time, speed and noise factor encryption is applied for observing the algorithm performance.[11]

**Gandhi A. Rashmi and Gosai M.Atul et al 2015:-** Tn this paper, authors presented about compressive introduction about cryptographic techniques for different data types viz.text,image,audio and video files. On the basis of certain different parameters different cryptographic techniques are considered as an example throughput, Speed, CPU time, Battery power, memory requirement.[12]

**Zhao Tieyu and Ran Qiwen et al 2015:-** This paper discussed about asymmetric cryptography by sharing fingerprint. The motto to use fingerprint is provide encryption and decryption along with the same key which is fingerprint and more authentic. The receiver can easily identify the authenticity of cipher text. Hence, the simulation results show highly robust encryption scheme.[13]

**Kingston A., Colosimo S., Campisi P., Autrusseau F et al 2007 :-** Here, authors introduce a new concept of joint encryption along with lossless compression used for large images. Standard encryption techniques, such as AES, DES, 3DES, or IDEA can be applied to encrypt very small percentages of high-resolution images. As the proposed scheme uses standard encryption, and only transmits uncorrelated data along with the encrypted part, this technique takes benefit of the security related to the chosen encryption standard, here, we assess its performances in terms of processing time and compression ratio.[14]

**Wu C.-P & Kuo -C. J. et al 2005:-** In this paper, authors uses simple permutations and combinations to encrypt every byte for achieving a high level of security. As they analyzed it is not a best suitable method for real time applications because of as every byte is encrypted so takes long time.[15]

## 3. RESEARCH DESIGN

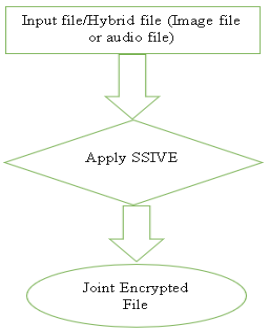


**Figure.No.1: A roadmap for SSIVE( Secure Selective Image and Voice Encryption )**

## 4. PROPOSED METHODOLOGY – SSIVE (SECURE SELECTIVE IMAGE AND VOICE ENCRYPTION)

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

The following steps of proposed methodology SSIVE are given below: -

Step-1) Input Data Set. // Live Recording of Any user Image and Voice.

Step-2) Save input Dataset. // Store into the database on save button click.

Step-3) Select Significant (Selective Confidential) data of Input Data Set.

Step-4) Divide Significant Selective Confidential data set into 2 equal parts.

Step-5) Apply Multi-Stage Encryption or Multi-Level Encryption on the first selected portion (That is Image Encryption is applied) and note down the readings of some certain parameters of Cryptographic Algorithms viz. Computed Encryption time, Memory Consumption, Execution Speed and Time. And store results in Table.No.1 in the database.

Step-6) Apply Multi-stage encryption on the 2nd selected portion (i.e. voice encryption is applied) and note down the readings of some certain parameters of Cryptographic Algorithms viz. Computed Encryption time, Memory Consumption, Execution Speed and Time(actual performance). And store results in Table.No.2 in the database.

Step-7) after that Apply Combinational Encryption is applied together and note down the readings of some certain parameters of Cryptographic Algorithms viz. Computed Encryption time, Memory Consumption, Execution Speed and Time (actual performance). And store results in Table.No.3 in the database.

Step-8) then Compare the results of step 5, 6 and 7 of cryptographic algorithm.

Step-9) Draw the graph of individual cryptographic algorithm parameter.

(i) like on X-axis image encryption (file size in KB) & on Y-axis computed encryption time. Similarly, (like on X-axis Voice encryption (file size in KB) & on Y-axis Computed encryption time.

(ii) like on X-axis image encryption (file size in KB) & on Y-axis execution speed & time(performance). Similarly, (like on X-axis Voice encryption (file size in KB) & on Y-axis execution speed & time(performance)).

(iii) like on X-axis image encryption (file size in KB) & on Y-axis Memory consumption. Similarly, (like on X-axis Voice encryption (file size in KB) & on Y-axis Memory consumption.

## 5. CONCLUSIONS

Along with the changing trends in the network security, different types of challenges are in the frontline as an example phishing attacks, IOT attacks, machine learning/ Artificial Intelligence attacks and software vulnerabilities and the most prime challenges are ransomware attacks and cloud attacks. This paper discussed about different types of encryption algorithms used in different disciplines of encryption say image encryption and voice encryption and correspondingly proposed a new designed methodology named “SSIVE” which is termed as “Secure Selective Image and Voice Encryption.” The major objective of this research paper is to achieve a sufficient level of security in the minimum time. The purpose to design this newly designed algorithm is to reduce the amount of data to encrypt and provide high security. This multi-level encryption helps to produce good results by considering different types of parameters. In the end, no any constraints (such as file size, image extension etc.) are applied on the time of input applied.

## 6. REFERENCES

[1] Ayoup Ahmed & Hussein Amr, Efficient Selective Image Encryption, Springer December 2016.

[2] Zia Unsub & McCartney Mark , Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, SpringerLink, April 2022.

[3] Massoudi A & Lefebvre.F,Overview on selective encryption of image and video: Challenges and perspectives, EURASIP Journal on Information Security, Springer Open, December 2008.

[4] Panzade Prajwal & TakabiDaniel, Sok: Privacy preserving machine learning using functional encryption: opportunities and challenges,arXiv:2204.05136v2[cs.CR], September 2022.

[5] Alluhaidan Saleh Ala, Secure medical data model using integrated transformed paillier and KLEIN algorithm encryption technique with elephant herd optimization for healthcare applications, National Library of Medicine, PMC PubMed Central, October 2022.

[6] Alothman Basil Raya, A performance based comparative encryption and decryption technique for image and video for mobile computing, IGI Global, Publisher of Timely Knowledge,2015.

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

[8] Chuchra .R and Seth R.K. Modeling Implementation of TSEA - Three Step Encryption Algorithm for Enhancing Password Security. International Journal of Computer Applications, US, September 2015.

[9] 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.

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

[11] Verma O P, Aggarwal Ritu and Tyagi Shobha, Performance Analysis Of Data Encryption Algorithms, IEEE, 2011.

[12] Gandhi A. Rashmi and Gosai M.Atul , A Study on Current Scenario of Audio Encryption, International journal of Computer Applications, April 2015.

[13] Zhao Tieyu and Ran Qiwen, Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography, ELSEVIER, September 2015.

[14] Kingston A., Colosimo S., Campisi P., Autrusseau F.,” Lossless Image Compression & Selective encryption using a discrete random transform, IEEE, 2007.

[15] Wu C.-P & Kuo -C. J., Design of integrated multimedia compression and encryption systems, IEEE Trans. Multimedia, 2005.

[16] Vyavahare B. Raviraj and Bajaj. J Amit, Study of secure data transmission using Audio File”, International Journal of advanced research in computer and communication engineering, February 2015.

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