DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4192

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN IMPROVED ALGORITHM FOR JOINT SELECTIVE MULTIMEDIA ENCRYPTION (JSME) - 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: To provide security in network is a global issue in cyber world as we all know in the age of universal electronic connectivity, of viruses, attackers and hackers of electronic eavesdropping there is indeed no time at which security does not matter. So, to provide security against the hackers or threatens becomes a critical issue. This paper discusses about the various different encryption algorithms that can be uses in various different disciplines viz. image encryption, audio encryption and video encryption. This paper designed a new algorithm for JSME that is termed as Joint Selective Multimedia Encryption whose purpose is to provide security of confidential information within small duration of time. The significance to use the concept of selective encryption is it provides a high level of security and consumes less time as well. The Practical use of this new designed methodology is to provide security to online video conferencing. The complete working of this new designed methodology is depends on three step encryption algorithm used for cyber security (3SEMCS). The parameters consideration during applying image, audio and video encryption is important factors.

Keywords : cryptography, encryption algorithms, selective image encryption, selective audio encryption, selective video encryption, time and security.

1. INTRODUCTION

Selective multimedia encryption (SME)[1] is used to provide high level of security to confidential information. The term selective means only sensitive part of multimedia is encrypted and can only be decrypted by the authorized or registered users. The basics of multimedia include both cryptographic techniques and multimedia techniques. Due to continuously increasing the enrollment of attackers in computer world the privacy of content is mandatory. The main significance to utilize this multimedia encryption is it produces latest research results in dynamic field. It discusses common techniques of complete, partial, and compression-combined encryption; as well as the more specialized forms, including perception, scalable, and commutative encryption. 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[2] etc. There are many common algorithms are used in different disciplines as like in the discipline of image encryption, audio encryption and video encryption. The diagrammatical representation of every type of encryption is given below in figure 1, 2 and 3:

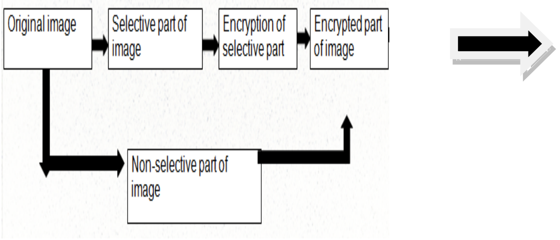

Figure1: Selective Image encryption.

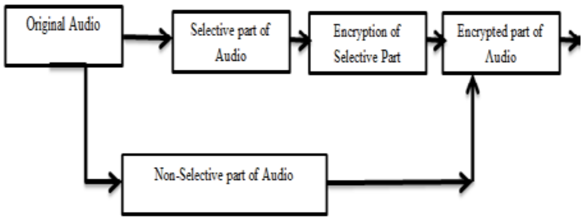

Figure 2: Selective Audio encryption.

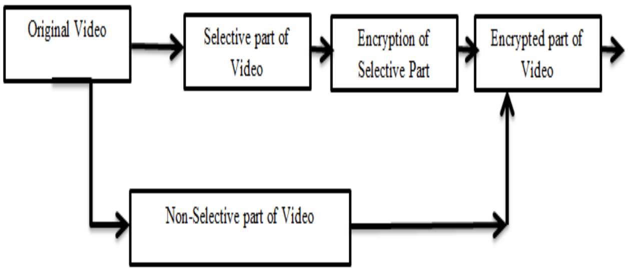

Figure 3: Selective Video encryption.

Each discipline of encryption is discussed below one by one having some following types of algorithms:

Image Encryption:

- ✓ **Shuffling Algorithm:** - Shuffling method based on parameter-varied chaotic map. Perhaps, the one-dimensional maps are the simplest mathematical objects to display chaotic behavior. The logistic maps are one kind of one-dimensional maps and have already been widely used in image encryption.

$$Xi+_1 = f(x_i) = ax_i(1 - x_i)$$

Here, *a* is the parameter of logistic map, $x_i = f^{(i)}(x_0) \in I$, $i = 0, 1, 2,\dots$ and $f: I \rightarrow I$, where *I* denotes an interval.[3]

- ✓ **Image-Scrambling-Based Algorithm: -**Image scrambling is a useful approach to secure the image data by scrambling the image into an unintelligible format. a new parameter based M-sequence which can be produced by a series shift registers. In addition, a new image scrambling algorithm based on the M-sequence is presented. The user can change the security keys, r, which indicates the number of shift operations to be implemented, or the distance parameter p, to generate many different M-sequences. This makes the scrambled images difficult to decode thus providing a high level of security protection for the images. The presented algorithm can encrypt the 2-D or 3-D images in one step. It also shows good performance in the image attacks such as filters (data loss) and noise attacks.[5]

The main parameters consideration during applying Image Encryption:

- o **Number of Pixel Change Rate: -** It is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images.
- o **Unified average changing intensity (UACI):-** UACI is helpful to identify the average intensity of difference in pixels between the two images. A small change in plaintext image must cause some significant change in cipher text image.
- o **Correlation Coefficient:-**This parameter is useful for calculating the quality of the cryptosystem. Correlation computes the degree of similarity between two variables.

Audio Encryption:

- ✓ **Blowfish: -** Blowfish [5] is a keyed block cipher designed in 1993 by Bruce Schneider and widely used in a large number of cryptographic products. It provides good performance in software. Blowfish has 64 bit block size and a variable key length from 32 bit to 448 bits. The algorithm works in two parts: A key expansion part and a data encryption part. The key expansion part is to convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption is by a 16 round Feistel structure and uses a large key dependent S-Boxes. It is suitable for applications where the key does not change often, like communications link or an automatic file encryption. It is comparatively faster than most encryption algorithms when implemented on 32 bit microprocessors with large data caches.
- ✓ **Twofish: -** Twofish [6] is an algorithm from counterpane Internet Security. It is highly suited for large microprocessors and also for smart card microprocessors. Twofish was designed to meet NIST's design criteria for AES. It is based on Feistel network. Specifically, they are a 128-bit symmetric block cipher with key lengths of 128 bits, 192 bits, and 256 bits. It is working efficiently both on the Intel Pentium Pro and other software and hardware platforms. It supports flexible design like accept additional key lengths, can be implementable on a wide variety of platforms and applications.
- ✓ **Three fish: -** Three fish block cipher was designed by Niels Ferguson et al. They designed them with speed, security, simplicity, and flexibility in mind. Three fish is a large tweak able block cipher [7]. Tweak serves the purpose of initialization of vectors. It is defined for three block sizes: 256, 512, and 1024 bits. The key size is equal to the block size while the tweak value is 128 bits regardless of the block size. Instead of Sboxes, Three fish uses XOR and modulus addition to achieve non-linearity and hence good security. It is also suitable for hardware and software implementations especially in 64-bit platforms since it operates on words of 64-bit size.

The main parameters consideration during applying Image Encryption:

- o Time.
- o Speed.
- o High security key.

Video Encryption:

- ✓ **Choose and encrypt: -** Encrypting and decrypting the entire video stream is not practical in real-time applications. A solution [8] is needed in which frames in the video can be selectively encrypted. By implementing such a methodology the complexity and encryption/decryption overhead is decreased to a great level. However, the level of security should also be maintained. This algorithm can be successful if a proper tradeoff can be maintained between complexity and security.

- ✓ **Crisscross Permutation: -** This proposed algorithm [9] first generates a 64 byte permutation list. This list is then quantized into an 8x8 block. This is followed by a simple splitting procedure. The random permutation list is then applied to the split blocks and the result is then encoded. Computational complexity is relatively low and hence the encryption and decryption process is not too complex. Crisscross permutation distorts the DCT coefficients and hence the video compression rate is lowered. This algorithm also cannot withstand the known-plaintext attack.

- ✓ **Pure Scrambling: -** Video bytes in each frame of the video are shuffled using permutation operation. This proposed method [10] is very handy in applications where hardware decodes the video. But in day to day application decryption is the work of software. This method is susceptible to the known-plaintext attack and hence should be used with caution. The permutation sequence can be easily figured out by comparing the known frames with the cipher text. After understanding the sequence, the attacker can easily decrypt the entire video.The most important factors to evaluate video encryptions are encryption ratio, compression efficiency, degradation, security, format compliance and speed. [8]

The main parameters consideration during applying video Encryption:

- Encryption Ratio.
- Compression Efficiency.
- Degradation.
- Format Compliance.[8]

In this research paper, authors designed a new methodology named JSMEA that is termed as a joint selective multimedia encryption algorithm whose purpose is to provide a high rank of security within short span of time. The major objective of this research paper is to reduce the online attacks of hackers and send confidential information through a secure communication channel. The most practical use of this new designed methodology is in cyber world during online video conferences. The content delivered through cyber world must be confidential if professionals use JSMEA. Different parameters considerations are used in different disciplines of encryptions as like in case of image encryption number of pixels change rate and Unified average changing intensity are important factors. Similarly in case of audio encryption, time and speed are most important factors and in case of video encryption, compression efficiency and format compliance are important factors. The attack rate of hackers will be reduced up to some extent by applying JSMEA (Joint Selective Multimedia Encryption Algorithm). Hence, users can send their confidential information through secure communication channel (SCC).

2. RESEARCH DESIGN

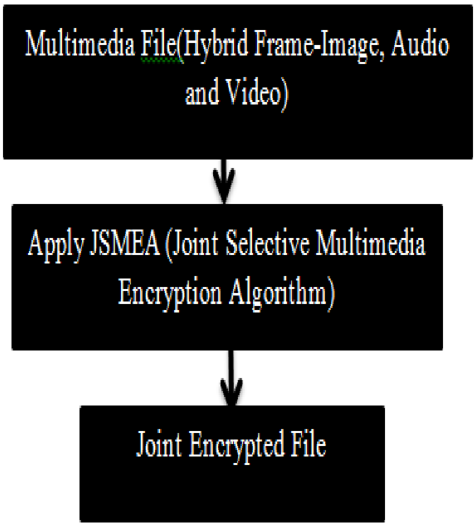
Multimedia File(Hybrid Frame-Image, Audio and Video)
Apply JSMEA (Joint Selective Multimedia Encryption Algorithm)
Joint Encrypted File

Figure 4: A Platform for Joint Encryption (JE).

3. PROPOSED METHODOLOGY (JSMEA-JOINT SELECTIVE MULTIMEDIA ENCRYPTION ALGORITHM)

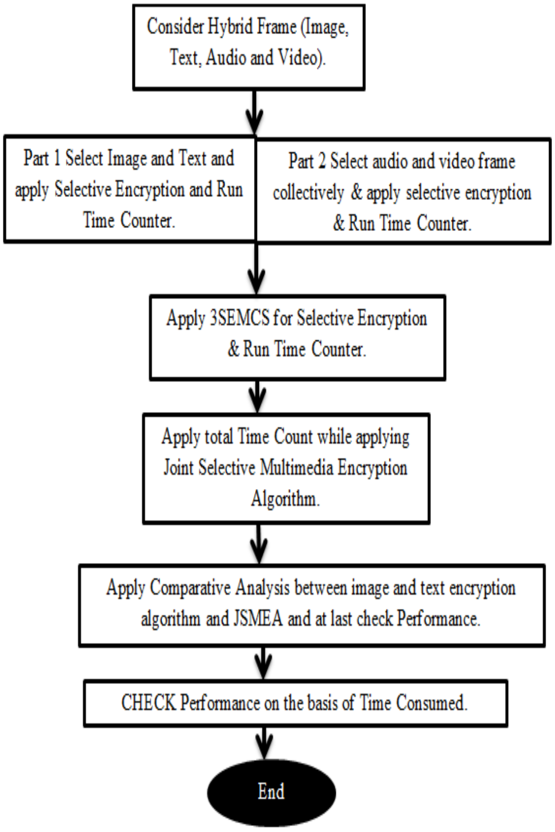
Consider Hybrid Frame (Image, Text, Audio and Video).
Part 1 Select Image and Text and apply Selective Encryption and Run Time Counter.
Part 2 Select audio and video frame collectively & apply selective encryption & Run Time Counter.
Apply 3SEMCS for Selective Encryption & Run Time Counter.
Apply total Time Count while applying Joint Selective Multimedia Encryption Algorithm.
Apply Comparative Analysis between image and text encryption algorithm and JSMEA and at last check Performance.
CHECK Performance on the basis of Time Consumed.
End

Figure 5: A Roadmap for JSMEA (Joint Selective Multimedia Encryption Algorithm).

4. CONCLUSION

This paper discussed about different types of encryption algorithms used in different disciplines of encryption say image encryption, audio encryption and video encryption and correspondingly proposed a new designed methodology JSMEA is named as Joint Selective Multimedia Encryption algorithm. The major objective of this research paper is to reduce online attacks of hackers and send confidential information through a secure communication channel. The purpose to design this new designed algorithm is to provide a highest level of security to our confidential information within small duration of time. Different parameters considerations considered during different disciplines of encryptions plays a vital role in multimedia encryption. There is no multimedia file size constraints are considered during input time or in other words you may say when frames are selected for applying hybrid or joint encryption.

5. REFERENCES

[1] Raviraj B.Vyavahare and Amit J.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] YICONG ZHOU and KAREN PANETTA, “An image scrambling algorithm using parameters based M-Sequences”, IEEE, USA.

[5] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, “Performance Analysis of Data Encryption Algorithms”, IEEE, 2011.

[6] Dr.S.A.M Rizvi, Dr.Syed Zeeshan Hussain, 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,Saurabh kulkarni,” Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study”,Int journal of computer applications,Vol.65,No.1 ,March 2013.

[9] L. Tang, for encrypting and decrypting MPEG video data efficiently," in Proceedings of The Fourth ACM Intl. Multimedia Conference (ACM Multimedia), (Boston, MA), pp. 219-230, November 1996.

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