Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Energy Efficient Encryption Technique for Constrained Devices

Darshana Hooda
University Computer Centre
DCRUST,Murthal, Sonepat, Haryana, India

Anshula Badak
Student M.Tech. (CSE)
MDUniversity, Rohtak, Haryana, India

Abstract - Encryption is the proven technique to offer data security but conventional encryption algorithms consume computing resources significantly and are less efficient in current scenario of multimedia consumption through hand held devices.Remote Reference Passingframework is designed to use computation intensive mathematical functionsin energy efficient way specifically suitable for security of digital multimedia content. In this paper, we have proposed trapdoor one way function under RRP framework to offer energy efficient encryption and decryption of digital multimedia content to facilitate secure multimedia communication among common mobile users. The proposed technique works prior to compression and encrypts videodata in'spatial' domain only at pixel level. Prior to compression makes this approach portable to different video codecs. Proposed security techniques offers energy efficient way for secure video communication, hence make it most viable security solution for common mobile users, where users demands privacy.

Keywords:Multimedia Security, Remote References Passing Framework, Encryption, Power Efficient, Trapdoor one way functions, Modulo Inverse.

I. INTRODUCTION

In recent, popularity of multimedia communication over internet is astounded. Today, 66% of global mobile data traffic is mobile video traffic pertaining to different multimedia services like video chatting, video conferencing, and entertainment services. These statistical figures shows heavy video consumption through mobile devices i.e. constrained devices in terms of computing resources and battery power. In current scenario due to convenience and technological advancement more and more users and businesses use smart phones as effective communication tool to discuss their business plans/activities or to share personal matters/affairs. All users have the right to maintain their privacy and confidentiality of communication, while it is travelling over communication channels. To boost faith of users in technology enhanced communication tools security mechanisms were evolved to protect the information from unauthorized access. Cryptology is the fool proof technology to offer secure communication, but in current scenario heterogeneity in communication technology and limited capabilities of accessing devices pose new challenges.

Today, energy consumption by encryption algorithm is major concern because of the critical limitation of battery power of constrained devices. Battery power is critical limitation than processor speed /memory as memory and processor technologies doubles with the introduction of every new semiconductor advancement. Users of the hand-held devices generally have complaints about the battery life of the device. Optimizing the energy efficiency of mobile application can increase battery life span. Therefore, power efficient encryption techniques are critical need of time keeping in view the exponential growth in wireless technologies and hand held devices [2,3,4].

Our aim here is to design a technique to reduce the consumption of power during the encryption/decryption processto address security needs of digital multimedia service like video chat , keeping in the view heavy load on video servers and limited resources capabilities of client devices. This paper is organized as follows: Section 2 discusses Remote Reference Passing mechanisms in detail. Section 3 describesthe proposed RRP framework with inverse buffer to minimize the encryption time. Next section covers designing of algorithm in proposed framework. Performance analysis& simulation is presented in section 5that show perceptual encryption strength, encryption/decryption time and energy efficiency of proposed method in comparison to conventional crypto framework. The last section has the conclusions of this study.

II. BACKGROUND: REMOTE REFERENCE PASSING FRAMEWORK

D. Hoodaet all propose Remote Reference Passing Security Framework, specifically designed for raw video datai.e. 24 bit color space, keeping in view high redundancy over smaller range. Said framework opens new direction in area of cryptology where in place of cryptographic algorithm, designing of distribution functions are required and these distribution function may be kept secret in addition to keys. Saidcryptographic techniques, binds system resources i.e. memory to crypto technique with emphasis on very low computational overhead on the receiving end device during the decryption process.Proposedsecurity framework is capable of offering security solutions for a wide range of multimedia services under different communication environment. RRP framework is based on innovative idea of passing reference, a method highly suitable to address security needs of video services. It helps in provisioning of client resources aware security to a multimedia services asked by client. In this framework client is active entity while as server is passive and offer security as per client device resources. This approach demonstrates very low processing overhead on video sinks &

negligible decryption time, therefore making it highly suitable for the constrained devices for a prolonged battery life. Theoretical analysis and experiment results show that developed framework offer fast, energy efficient, and reasonably secure and robust security solution for different video application only at receiving side. Encryption time remains same as conventional scheme [9].This approach is highly suitable for the constrained client devices but needs further improvement in encryption at server side keeping in the view processing of large number of client request processing concurrently. This paper presents an improved RRP framework by introducing preprocessing step for encryption at the server end and proposes a new distribution function based on modulo inverse. The next section describes the proposed modified RRP framework.

III. PROPOSEDRRP FRAMEWORK WITH INVERSE BUFFER

In this work, improvement in basic RRP framework is suggested to achieve fast and secure video communication by preprocessing at server, which minimizes the delay during encryption process. Under preprocessing step, an inverse buffer is created by the server for each client to serve the request, which makes encryption process comparatively faster than the basic RRP framework. Figure 1 depicts the proposed improvement in basic RRP framework and working of each step is described in details:

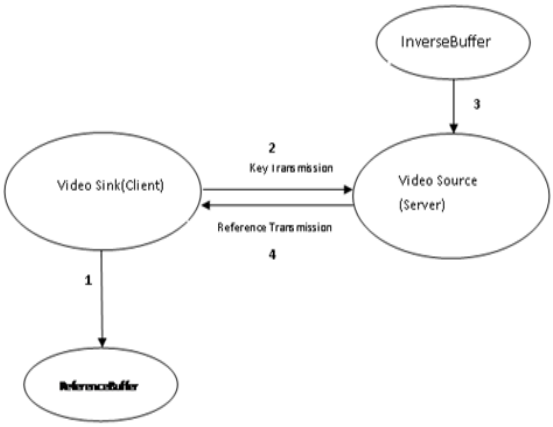

Figure 1: Workings of the Proposed Model

Step 1: Buffer Allocation (Client Module)

First of all encryption unit size is determined by the client as per the service demand and available resources. In case of digital multimedia (RGB-24 format) 8 bit or 24 bit may be taken as encryption unit. Constrained client prepares a memory buffer of size N, as per its memory availability but it should more than $2^{encryptionblocksize}$. Values to Buffer are assigned by placing data values in buffer B of size N using mathematical mapping between index and candidate video data values.

After buffer preparation,clienttransmits keys:N(Size of Buffer), B_o(Random Index of B) , and Val(Value resides at B_0)to video dataServer.

As discussed in paper by D. Hoodaet. all that buffer allocation mathematical mappings may be designed as per the security needs, and availability of memory space[9]. Hence, under this work modulo inverse is used to define distribution function. Buffer allocation is offline activity just prior to the actual transmission. Before each new demand/request from client, new buffer allocation take place i.e. session keys are generated, which are valid for one particular session, hence offer increased security. However actual implementation and use of buffers has many dimensions for exampleduring the decryption process buffer may be copied in to an array or the starting address of the buffer may be transferred to processor register or a complete buffer may be transferred to cache for fast access- hence references will be used accordingly. This is client specific activity prior to actual data transmission, which takes place offline and therefore does not affect decryption time during real time video consumption. This offline time for buffer preparation is also negligible as the size of buffer remains in between 256 to 512 from implementation perspective, when RGB color space is considered however in principle buffer can as large as memory space of client. Whenever size increases from 256 there is increase in file size if video stream considered as byte stream in 24 bit color space. So it is wise to keep size of buffer 256 for implementation issues.

Step 2: Key Transmission

After buffer preparation with designated values,constrained client sends B_o, Val, N to Server using any conventional method for key exchange. Same is shown in One Way key Exchange from client to server is required.

Step 3: Inverse Buffer Preparation (Server Module: Offline Step)

Mapping may be kept secret and communicated secretly in case of high level of security but as per common security needs and as per cryptographic principles it is assumed that mapping are publically known function , only keys remain secret. After receiving the key, the server prepares an inverse buffer using the inverse mapping corresponding to the mapping used to create reference buffer at client side.

Step 4: Encryption Module (Server Module: Online Step)

The video server creates remote references corresponding to the original input video data by substituting appropriate references from the inverse buffer. i.e. original video data byte is replaced by the respective index of buffer (B) at client,

where this value resides, using the inverse buffer.

Step 5: Decryption Module (Client Module)

Reference to buffer location fororiginal video data is received by the client. The original video stream isre-constructed by referring the reference; where the respective original data is available. The significant advantage of this algorithm is that the client is not receiving the data but a pointer/reference where intended value is stored.

IV. PROPOSED MATHEMATICAL MAPPING

Number theory principle plays important role in coding theory. Trapdoorone way functions are considered good for cryptographic techniques as it is easy to compute in one direction but difficult enough to compute in the other direction. Modular inverse of a number is a lot more difficult to solve so in this paper we are using this principle to define the mapping between reference sequence and video data stream at byte level.

4.1 Mathematics behind Algorithm

Proposed technique is based on the number theory principles.

Definition Let a and n > 0 be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class** of a modulo n, and is denoted by $[a]_n$, where :

$[a]_n = \{ x \text{ in } \mathbf{Z} \mid x \equiv a \pmod n \}$.

The collection of all congruence classes modulo n is called the **set of integers modulo n**, denoted by $\mathbf{Z}_n$.

Definition : If $[a]_n$ belongs to $\mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$, for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$iffgcd(a,n)=1 and is denoted by $[a]_n^{-1}$.

In general, $a^{-1} \equiv x \pmod n$ has a unique solution iffa and n are relatively prime. Further if n is prime then every number in the range 1 to n-1 will have exactly one inverse modulo in that range.

4.2 Proposed Algorithm

Based on the principle of inverse modulo, buffer at receiver device is created for the range of value {1…N}. So n be take prime larger than $2^{\text{sizeofencryptionunit}}$.

Reverse mapping is used to reconstruct the respective a for inverse modulo b.

BufferAllocation(B,Key,n)

{

B Buffer of size n; n≥256

B_i i^{th} location of buffer B

Generate Key

Key_1, Key_2=rand(1..n-1)

1. Select prime number n such that n>256

2. Allocate values for 1….n locations of Buffer

For i=1 to n

index= (i+Key_1) mod n //shifting of index location

* B_{index}= (a +Key_2) mod n // value shifting

where a<==(i*a $\equiv$1 (mod n))

}

Referencecreation(Key_1, Key_2,n,B_i,C_i, I)

{

Key, m, n received from client

$B_i$ith byte of video stream

C_i cipher byte corresponding to B_i

I Inverse buffer , Preprocessing step

1. Inverse buffer preparation

For i=1 to n

*a <==(i*a $\equiv$1 mod n)*

a= (a+Key_2) mod n

I[a]=i

2.Encode B_i Video byte

C_i=I[B_i]

C_i=(C_i+ Key_1) mod n

3.Send C_i to client

}

Decryption(B,C_i)

{

B buffer containing the data

C_i cipher byte received from source in form of reference

1. Obtain original video byte by referencing the location $C_i$in buffer B

$O_i = B[C_i]$

}

V. PERFORMANCE ANALYSIS AND SIMULATION RESULTS

Simulation of the above encryption and decryption modules is carried out using MATLAB. The respective programs are executed on the computer with Processor Intel® Core(TM)2 Duo CPU T5670 @ 1.80 GHz, 1.00 GB RAM. During experiment, sample video sequence 'Foreman' in QCIF format is used for in RGB-24(176X144) base color model. Experiments are carried out to show perceptual encryption strength , quality of reconstructed/decrypted video and encryption/decryption time taken by the proposed technique doing so. Personalized video applications are sensitive applications usually demands privacy . The encryption algorithms for personalized video services have to withstand not only classical cryptanalytic attacks but also the perceptual attack in order to ensure that no visible information related to the sensitive communication is disclosed. One more video sequence 'Xylophone' (size 320X240X24 bits per frame) in RGB -24 bit color space is also used to evaluate the generality of developed algorithm for time and visual distortion of encrypted frames.

(a) Foreman Video Sequence

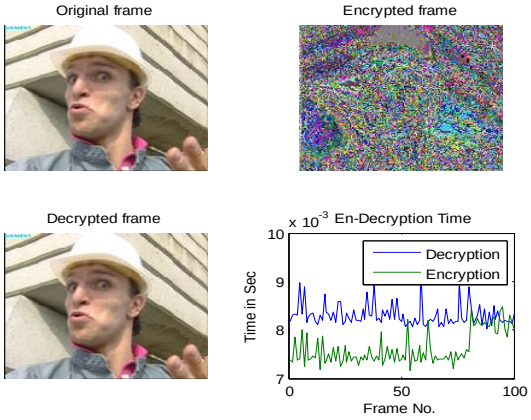

Figure 2(a): Perceptual Security and Encryption/ Decryption Time under Improved RRP Framework

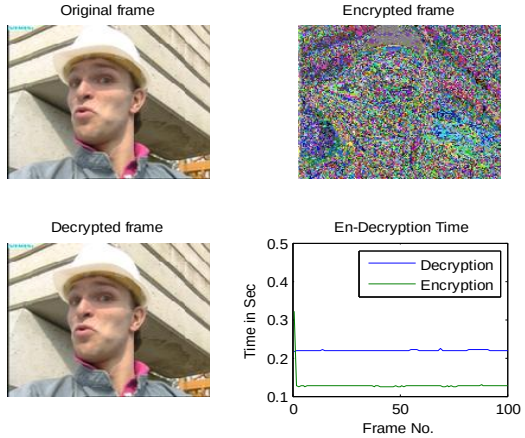

Figure 2(b) : Perceptual Security and Encryption/ Decryption under conventional crypto framework

(b) Xylophone Video Sequence

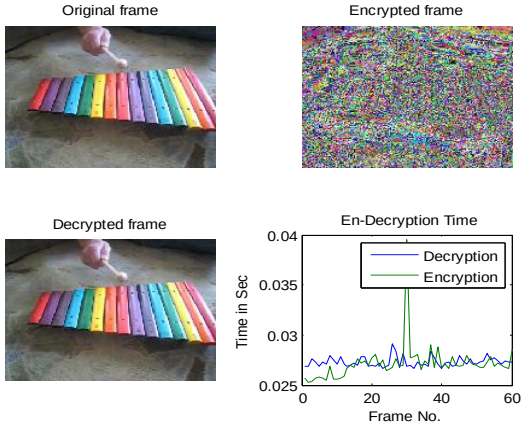

Figure 3(a): Perceptual Security and Encryption/ Decryption Time under Proposed RRP Framework

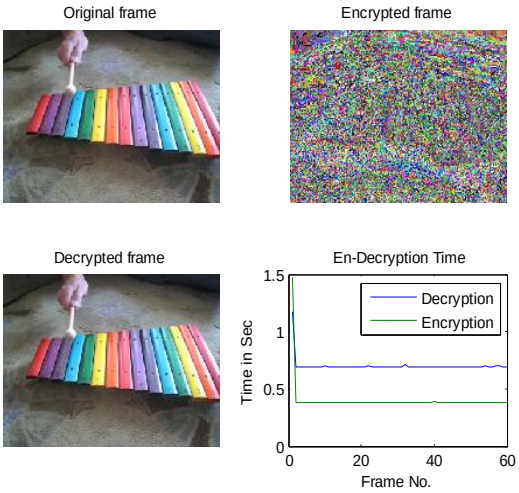

Figure 3(b) : Perceptual Security and Encryption/ Decryption under conventional crypto framework

On the basis of simulation results (fig 2 & 3) following conclusions are drawn:

(i) Encryption time for proposed is significantly low and further minimization in encryption and decryption process is only possible through environment specific customization. Theoretically, for naïve approach further minimization is not possible. This makes it most significant method to meet stringent real time processing need of multimedia applications. Mathematical functions are always computation intensive hence consumes more computational resources, one of the major reasonthat they are not commonly suitable for encryption. Proposed RRP framework opens new direction towards the use of mathematical function efficiently and effectively to address security needs of multimedia content for common users.

(ii) Further, when inverse modulo is used in conventional crypto framework for perceptual security, encryption time is estimated .12 seconds while as decryption time .22 seconds. Same method when implemented under proposed RRP framework then estimated encryption and decryption time is significantly lessi.e approximately within the range .007-.009 seconds. It proves that preprocessing offers optimistic future insecurity of multimedia application for common users.

Table 1: Approximate results inferred from figures 2 & 3

Video Frame	Frame Size	Encryption T.		Decryption T.	
		Conventional	RRP	Conventional	RRP
Foreman	176x144	.12 s	.007	.22s	.009
Xylophone	320x240	.40 s	.027	.70s	.028

(iii) Energy consumption by a program is calculated by

$E=V_c \times I \times N \times \tau$

Where V_c The Supply Voltage

I The average current in amperes drawn from the power source for T seconds

N Number of Clock cycles

τ The clock period

V_c and τ are fixed with respect to the hardware, therefore $E\alpha I \times N$, as stated [11] that at application level it is more meaningful to take into consideration T than N and therefore, energy may expressed as $E \alpha I \times T$. Since, for any given hardware V_c is fixed [8].

Hence, from above it is inferred that energy consumption is directly proportional to execution time taken by encryption/decryption module. For proposed encryption/Decryption technique execution time is significantly low as comparison to conventional cryptographic algorithms i.e. RSA and many others, which indicates that proposed framework is energy efficient design.

This energy efficient design makes it viable security solution for constrained devices.

(iv) Visual Degradation

Simulation results shows said scheme offer highly disguised video. No visual information is disclosed hence highly suitable for privacy or confidential communication.

(v) Security Strength

The security of proposed method is also reasonable as it is based on one way trapdoor function, which are easy to compute in one direction but inversion of same is difficult enough. To address security needs of common users RRP framework is best viable option under constrained environment. Therefore, it is strongly recommended that when information value is not so high; a fast, not very highly secure but reasonably secure encryption technique also offers promising results and future in addressing security requirement of common users.

Security of proposed method is

Let total space of receiver is G-//Initial index key space
Size of encryption unit is N (Always multiple of 8 considering Video byte stream)
Size of Buffer= 2^N //Any prime number $>2^N$
Probability of breaking the system= $\frac{1}{G*2^N*2^N}$
Therefore, the effective key space of the proposed framework is G x 2^N x 2^N. This number is large enough and in principal size of encryption unit can be as large as $\log_2 G$. This can make key space extremely large, and we know that the time complexity of attack is proportional to the number of possible keys, hence optimum algorithm to break this encryption algorithm is of exponential-time complexity.Security of RSA relies on its key size only. Smaller size encryption and decryption exponents are major security concern. Under this approach, high level of security may be achieved if we take large size of memory buffer.
Further, high level of security may be achieved
-By taking different buffers for each color
-Increasing the size of buffer.
Remote Reference Passing Security framework establishes tradeoff between security level and memory.

VI. CONCLUSION

Existing security techniques are either based on symmetric or Asymmetric encryptions. Asymmetric encryption uses mathematical functions for encryption and decryption, which are computation intensive hence not considered for video encryption. However RRP framework offers a way to use mathematical function for encryption and incorporates features of asymmetric key cryptography and symmetric key cryptography. Proposed method is an energy efficient technique in terms of encryption and decryption process hence highly suitable in current scenario of heavy multimedia consumption on constrained devices. Proposed method offers energy efficient way for secure video communication.

REFERENCES

[1] Daemen J. and Rijmen, Rijndael: The Advanced Encryption Standard, Dr. Dobb's Journal pp 137-139, 2001
[2] P. RuangChaijatupon, P. Krishanmurthy, "Encryption and Power Consumption in Wireless LAN's", Third IEEE workshop on wireless LANS, pp 148-152, Newton, Massachusetts, Sep 27-28, 2001
[3] Chandramouli R. , Battery Power Aware Encryption, ACM Transactions on Information and System Security, Volume 9, Issue 2.
[4] Prasithsangaree P, Krishanmurthy P, Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", in the Proceedings of the IEEE GLOBECOM 2003, pp 1445-1449
[5] L. Agi, L.Gong, An empirical study of MPEG video transmission, in:Proceedings of the Internet Society Symposium on Network and Distributed system security, San Diego, CA, 1996,137-144 .
[6] Daniel Socek, HariKalra, Spyros S., Mogliveras, Oge Marques, Dubravko C., Borko F. New approach to encryption and staganography for digital video. Multimedia Systems, SpringerVerlog, 2007
[7] DarshanaHooda, Parvinder Singh, A New Approach to Design Programmable Secure Network Interface Card, International Journal Computer Applications, Vol 62(8):33-36, International Journal Computer Applications, January 2013
[8] VivekTiwari, Sharad Malik and Andrew Wolfe, Power Analysis of Embedded Software: A first Step Towards Software Power Minimization, IEEE Transaction on Very Large Scale Integration Systems, Vol. 2, No.4, Decemeber 1994
[9] DarshanaHooda and Parvinder Singh,Self-Adjustable Security Technique Based on Remote Reference Passing for Digital Multimedia Services; CSI Transaction on ICT,CSIT Publication, Springer Verlag, 1(2):117-125, June 2013

