IJITKM Volume 8 • Number 1 June-Dec 2014 pp. 96-105 (ISSN 0973-4414)

Remote Reference Passing Framework for Video Encryption

Darshana Hooda, Parvinder Singh
DCRUST, Murthal

ABSTRACT: Widely used security techniques like DES, AES, RSA are computationally expensive and are not suitable for the access devices with limited computational capability. Security techniques for the browsing/display devices with limited computational capability is one of the emerging area. In this paper, we propose novel security technique based on passing the information or data by reference. Till date no method is devised to transmit data from one system to another system by reference passing instead of data itself. In this paper firstly we propose a method to transmit the data using remote references and secondly remote reference passing is used to offer common security needs of video communication i.e. confidentiality and authentication. In this paper we have described a conceptual framework, which enables data transmission based on reference passing to provide confidential communication with authentication. Most important is that, the approach to offer the security for video transmission is innovative and based on client server architecture. We strongly believe that this may lead to new developments in the area of security of multimedia applications as well as remote reference passing concept towards designing of distribution functions.

KEYWORDS: Cryptography, Remote References, Video Source, Video Sink, Dereferencing, Buffer, Video Streaming, RSA, Cryptanalysis, Complexity.

1. INTRODUCTION

Recent advances in multimedia compression and communication technologies and availability of low cost display devices have led to a phenomenal growth of digital multimedia services and applications like video chat, video conferencing, video broadcasting , video on demand, online movie transmission, , medical imaging systems, video transmission on mobiles using 3 G services etc. So there is a need to design and develop new techniques and technologies not only to protect valuable multimedia assets from unauthorized access but to address new challenges like limited computing capabilities & resources of display devices. Cryptography is evolving continuously to address the emerging security needs. Designers of cryptography are required to take care about trade-offs between security, cost and performance while designing the cryptographic techniques. It's generally easy to optimize any two of the three design goal-security and cost, security and performance, or cost and performance; however, it is very difficult to optimize all three design goals at once[1]. In many cases the level of protection of information is much higher than that is actually required to meet the potential threat. Computational capability requirements increase as the level of security imposed increases; this strongly affects the performance of application. Excessive protection coupled with low computational processing capability of end access device introduces undesirable delay during the processing of received streaming data. This delay is highly undesirable for real time application. Situation is even worse when they are used in environments, where receiving end devices may have very limited resources or low computational power.

A straight forward approach to improve cryptographic performance is to implement cryptographic algorithms in hardware. This approach has been shown to improve cryptographic performance of single algorithm. But, unfortunately there are several problems with this approach. First a secure network system requires the efficient implementation of a suite of algorithms. Secondly, hosts need to implement Internet standards, and we know that the standards change. In fact, most Internet security standards are written to allow flexibility in algorithm selection. Third, security algorithms can be broken. Hence they may have to be changed on short notice. Fourth, cryptographic hardware is not ubiquitous, cheap and readily exportable. Finally, implementing certain cryptographic algorithm in hardware provides only limited increase in performance [2]. Most hardware implementations focus on speed and, requires high end, other requirements are suitable mostly for server-end applications only [3].

Conventional cryptographic algorithms, which generally aim at encrypting text data, however, are not well suited for video encryption. This is due to the fact that the conventional crypto algorithms cannot process the large amount of video data in real time[4]. From above discussion it is concluded that there is a need of a hybrid approach which can add flexibility in algorithm selection feature of software cryptography and faster execution of hardware implementation. Transmitting data through reference is highly effective in minimizing the delay as it reduces memory read/write operations.

Presently cryptosystems are either of symmetric cryptosystem or asymmetric cryptosystem. There are many recent symmetric ciphers with special implementation properties (proposed) like Hiegh,Clefia,DESXL[5] and

Present[6].With respect to asymmetric algorithm RSA and ECC both are good but key size is a major factor in their performance. Some of hybrid techniques of symmetric & asymmetric are also proposed.

The main purpose of this work is to develop lightweight cryptographic technique to address security needs of multimedia application, while accessed/played through constrained devices. The rest of the paper is organized as follows: In section 2 we have described proposed crypto system framework and working of system is presented in section 3. The priori analysis of proposed cryptographic technique in terms of time complexity, cryptanalysis and power consumption analysis is discussed in section 4. Finally, section 5 presents concluding remarks.

2. Proposed Model

In this paper we propose a novel cryptographic model based on the concept of remote reference passing which eliminates need of any key at receiving end as shown in Figure 1. Proposed crypto module includes encryption and respective decryption module. This method offers confidentiality and authentication where the level of security highly depends on the receiving device resources. Proposed security technique adjusts itself and provides security according to the end receiving device's memory availability and introduces very low processing and computation overhead on receiving device.

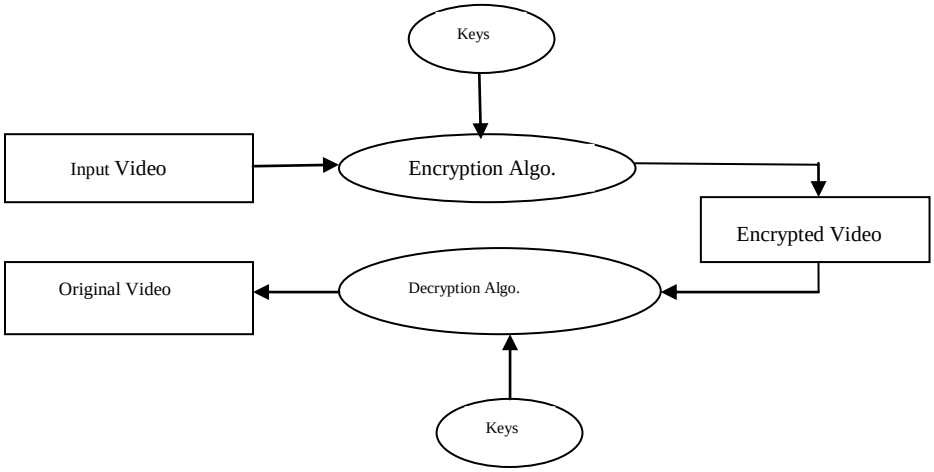


Figure 1: Conventional Crypto Model

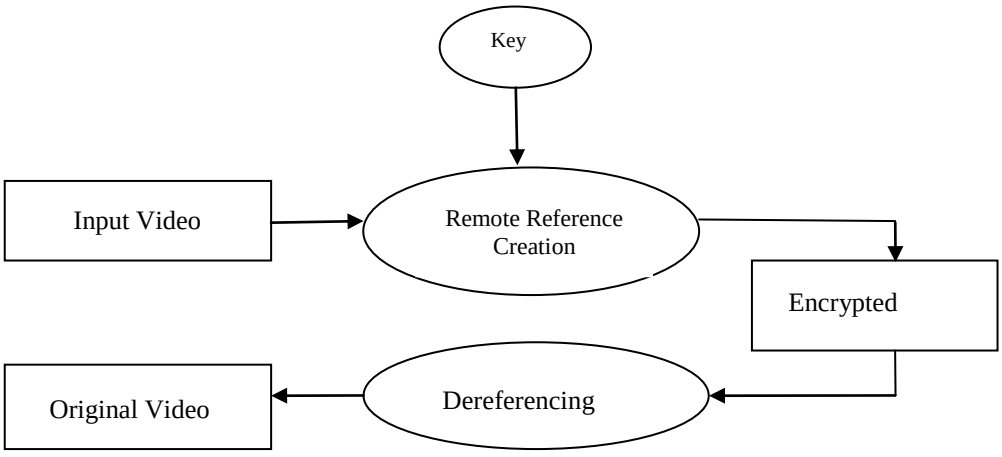


Figure 2: Proposed Crypto Model for Video Transmission

Working of Model

Proposed model is based on client server architecture. Input source of Video data is a high processing capability server while accessing devices termed as clients are having very limited computational capabilities. In proposed method to achieve secure communication, all the processing overhead is kept on the server while minimum overhead on the client machine taking into account its limited processing capability. In video transmission, delay may be accumulated due to transmission delay, compression/decompression delay, further; if security is needed then it adds encryption/decryption delay. Therefore objective of all the research dealing with the video transmission significantly takes care about delay introduced by the proposed method whether it is associated with compression or security. All these techniques should converge to minimize delay during video data transmission so that video can be enjoyed at full. Most exciting feature of the proposed model is that it introduces negligible delay at receiving end. However at Video source, all the remote reference creation takes place hence it introduces delay. Video Source systems are high end machines, so delay introduced by it is comparable to existing security techniques. Details of the working of model are illustrated in figure 3 and further working of each step is described by the respective algorithms.

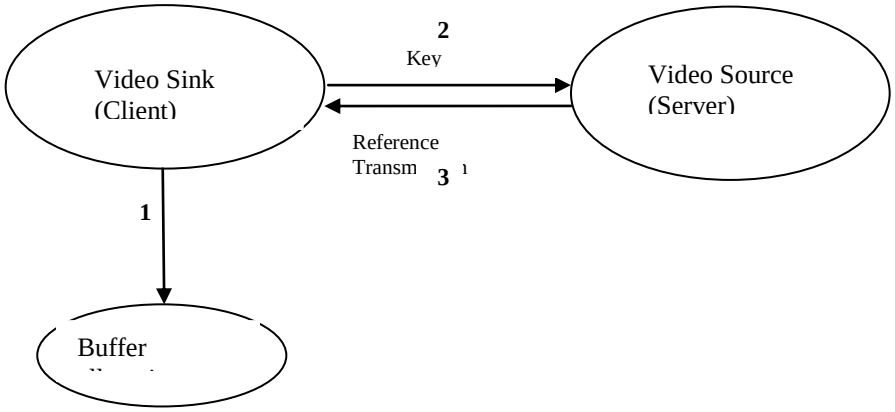


Figure 3: Working of Proposed Model

3.1 Buffer Allocation (Video Sink Module)

Video Sink prepares a buffer by placing data values in buffer and send request to Video Source to transmit intended video stream:

Buffer Preparation (B, N)
B Buffer of size N
N size of the available memory buffer
{
$B_i$ith location of Buffer B
Val_i value stored at ith location of Buffer
B=getblock(sizeof(N));
Obtain Val_1=rand(0-N);
For all i=2 to N
*B_i=(Val_{i-1}+1) Mod N
}

For buffer allocation many more schemes may be applied as per security need and availability of memory. In this reference these scheme in better way called as distribution function because of their role in arrangement of given range of value to buffer locations. Number theory principles can play significant role in designing of distribution function.

More than it, hardware implementation of said buffer also adds value to the algorithm. Security buffer may come along the processor with the liberty of distribution of the value as per user desire/requirement. This will add the flexibility lacking till now, in hardware implementation

3.2 Key Transmission

After preparation of buffer at Video Sink, B_0, Val_1, N are the keys obtained from step 1. These keys are conveyed to Video Source as indicated in step 2. No new method is devised for key exchange Any conventional method may be used for key exchanged. One Way key Exchange from client to server is needed.

3.3 Remote Reference Creation Module (Video Source Module)

Video Source creates remote references for the intended input video for video sink with the help of received keys from same through following module. Sever replaces the data value by the index of buffer(B) at client, where this value resides with the help of predetermined formula/algorithm.

Referencecreation(B_0,Val_1,N,O_i, C_i)

B_0,Val_1,N keys received from Video Sink(client Module)
O_i i^{th} byte in original file
C_i I th byte in encrypted file corresponding to O_i

```
{

  Ci = ( B0+(N-Val1+Oi)) Mod N;
}
```

3.4 Video Sink Module(Client Module)

Reference for video input is received by the video sink and original video stream is obtained by referring the address where actual data is available. The beauty of algorithm is that the client is not receiving the data but a pointer which indicates where value is located in clients Buffer 'B'.

Dereferencing Module(C_i,O_i)

$C_i$$i^{th}$ encrypted byte
$O_i$$i^{th}$ original byte obtained from C_i after dereferencing

```
{

  Oi= value at(address Ci)

}
```

4Analysis

The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. Complexities of encryption and decryption modules come under consideration, whenever efficiency of crypto algorithms is discussed. Performance of algorithm is highly dependent on the execution environment but environment dependent performance analysis like measure of efficiency of specific implementation of an algorithm, on one operating system, using one set of hardware, can provide good results that apply only to that particular environment and cannot be accurately extrapolated to different environments [7]. A theoretical analysis of algorithm can describe algorithm's behavior in a wide set of environments. So, here firstly we are presenting environment independent performance analysis of said Video Sink module , keeping in the view limited computational capabilities of video sinks. As this will help to evaluate the strength of the proposed method in general, independent of environments, it illustrate strength of the algorithm rather than environment in which they are to be implemented.

4.1 Time Complexity of Proposed Method

Video Sink Algorithms under discussion is an online algorithm. For online algorithms computation time per unit data is significant and doesn't require a bound on the computation time. [4]

Performance of algorithms is evaluated by asymptotic notations: best case time, average case time and worst case time. Conventional Algorithm analysis was meant for offline algorithm, where input size variation was significant. In case of Video files, sizes are of same range. Therefore there is a need to analyze such video data manipulation algorithm from different perspectives. In conventional algorithm analysis it is said, method is superior if it is faster by order of magnitude. But firstly it is very difficult to device a method faster by order of magnitude and secondly

video streams are very large in nature and every single operation required for imposing security or compression adds to the cost. So rather than talking about order of magnitude notion there is a need to analyze complexity of cryptographic module taking into consideration the no. of operations per byte and hence in video streaming algorithms, it is not wise to leave lower order term and constant multiples as they affect heavily the performance of the system. For video streaming application if we are able to device a method multiple time faster rather than order of magnitude, than this is also significant contribution in performance improvement because size of video streams is very large.

Compared with the text communication, video communication is characterized by a number of peculiarities, such as large data size, real-time requirement, the requirement of standardized data compression formats and video codecs , computing capabilities of accessing device and application-specific security requirements. Different video resolutions are in use like

Technology	Resolution
Internet(Youtube, Low Resolution)	320X240
TV(VGA)	640X480
HDTV 720p	1280X720
HDTV 1080i/1080p	1920X1080

The size of one second video footage would be calculated as Video resolution X no. of bits per pixel X no. of Frames per second. Therefore size of 1 second HD video footage would be 1920*1080*24*30=1492992000=1.4 Gb and Size of 1 hour video=1.4 *60*60=5040/8=630 GB. If byte level encryption takes place and if, one operation per byte encryption is needed. Then total no. of operations are required $63X10^{10}$. 2.5 GHz machine performs 2.5 X 10^9 operations per second so it takes 630/2.5 = 250 seconds to encrypt 630 Gb data (1 Hr. HD Video) while 300 MHz machine will take 35 minutes, only if there is one operation per byte.

From above discussion it is clear that no. of operations required to process each byte affects the performance of encryption algorithm and situation becomes more critical when video sink has limited computational capability.

In general, decryption algorithm uses more than one operations per byte decryption, for example RSA most popular algorithm used for public encryption, uses the following statement for decryption $m = c^d \bmod n$. m is decrypted byte, d+1 operations are needed to decrypt one byte/char and d >1.

Proposed method involves no mathematical manipulation (operation) but only single instruction, memory reading to fetch the value from specified location is required, and therefore it introduces negligible delay during dereferencing process. Hence, it is a strong recommendation in favor of proposed method.

This general mathematical model is much more suitable for comparing different algorithms as opposed to comparing two environment as in this way we can compare efficiency of methods rather than environments.

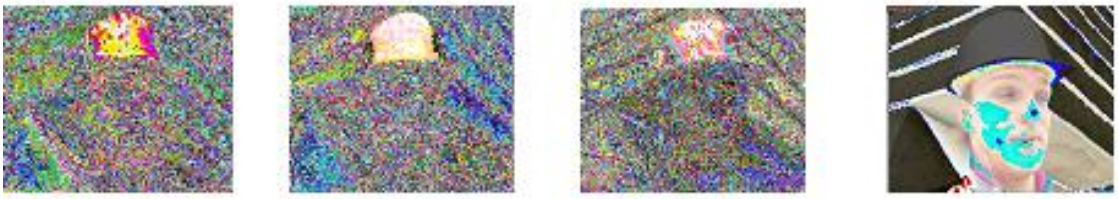
4.2 **Security Analysis of Proposed framework**

Protection by AES, DES, RSA(Even not feasible for text/video encryption) provides maximum security but needs special hardware for real time processing. There is apparent trade-off between security and the speed of video processing. Here our objective is to design client device resources aware encryption keeping in view multimedia consumption through constrained devices. Further, today everyone from ordinary mobile user to diplomats, are highly concern with security of their sensitive information travelling on network. Proposed framework has ability to offer different security levels as per need of different multimedia applications depending on the mathematical mapping/value distribution function used. During designing the cryptosystem we take care about the attacks and generally design the system in the way that cost of breaking the cryptosystem should remain higher than the value of content and generally this depends on key space. Under classical cryptanalysis it is assumed that attacker knows the everything about cryptosystem except the key, hence as per Kirchhoff's law strength of security highly depends on the size of key space. Larger the key space implies lesser the probability of breaking the system in definite time limits. In case of multimedia application cost of content is not generally very high and it is highly difficult to obtain same high quality video without knowing the key. In case of communication, two type of communication possible by ordinary users where value of information remains very low but for diplomat/sensitive communication, value of information is very high. Lianet at. describe that security of multimedia content depends on two aspects: cryptographic security and perceptual security. Cryptographic security refers to the security of the encryption key and encryption strategy while as perceptual security deals with information revealed by the encrypted video.

Cryptographic security of video is mainly vulnerable towards two types of attacks in common: first one attack for determining the key such as exhaustive attack popularly known as brute-force attack, probability attack and classical attacks like cipher text only, known plaintext and chosen plaintext/ciphertext attack. On the other hand special attack for videos like frame regrouping and frame erasure attack[11].

Brute Force Attack: This brute force attack is based on exhaustive key search and is feasible only for the cryptosystems with relatively small key space. Under proposed RRP framework video sink prepares a buffer by placing data values in buffer B of size N using mathematical mapping between index and candidate video data values. Next receiver transmits N(Size of Buffer depends on size of encryption unit), B_0(Random Index of B) and Val(randomly generated value placed at location B_0) keys to Video Source to transmit intended video stream. For buffer allocation, many scheme may be applied as per security need and availability of memory. Possible arrangements of values at buffer of size N may determine by the permutation. Therefore arrangements of {0,1,2…… N-1} values may be carried out in N! ways and $N \geq 256$. This number is big enough to to guess the arrangement, but as per conventional cryptanalysis it is assumed that this arrangement algorithm (encryption)
Is known publically hence security of method cannot be relied through this. Under RRP client transmit session specific information(B_0, Val, N) to the server and these values are used as security keys. One set remain valid for only one particular session. However, it is possible to change the keys after regular intervals during the session, but it adds reasonable overhead.
$B_0 \in \{0…….G\}$: Memory Range
Val $\in \{0,1…….2^n\}$ n: size of encryption unit
$N = 2^n$; $n \geq 8$, for space optimization & implementation issue it is better to choose n as multiple of 8 to view video as byte stream.
Therefore, the effective key space of the proposed framework is G x N x $2^n \approx$ 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 best algorithm to break this encryption algorithm is of exponential-time complexity. Problem of breaking the proposed encryption algorithm is intractable , because as n increases finding their solution quickly become infeasible. Further, class NP consisting of all the problems that can be solved in polynomial time only in nondeterministic fashion. There fore brute force attack problem for proposed framework is NP hard. Brute force attack is applied in the known ciphertext/plaintext attacks where exhaustive key search is needed.
Other significant security issue in multimedia encryption is perceptual encryption.

Perceptual Encryption: Unpredictability of the Encrypted Part
Broadly multimedia services may be categories into two categories as per security needs. Both categories need different kind of security. Entertainment applications have loose security needs while personalized video services require high degree of security. The value of video data in entertainment/virtual education applications is associated with video quality and timeliness. In entertainment industry high quality video is priced and requires an authorized access , while low quality versions or little disguised videos may free , to stimulate the user to purchase high quality version[12]. Personalized video applications are sensitive applications and usually have strict security requirements equal to those demanded for text encryption. The encryption algorithms for personalized video services have to withstand not only classical cryptanalytic attacks but also the perceptual attack[13,14] in order to ensure that no visible information related to the sensitive communication is disclosed. Proposed framework adds flexibility for service specific security provisioning along with consideration of client device resources.



(a) ExponentialFn. (b) Modulo inverse (c) Step function (d)Linear Function
Figure 4: The Encryption Results of Different Distribution Functions/Mathematical Mappings

Perceptual encryption strength of the proposed framework depends on the distribution property of mathematical mapping, hence different mathematical mapping/distribution function like linear function, step function, randomized or exponential function may used to achieve different level of perceptual encryption. Higher the randomized distribution of values over buffer produces higher distortion level. Given results are showing image distortions caused by different distribution functions/mathematical mapping:

From above discussion, it is observed that proposed framework offers different security levels and key space is sufficiently large to resist brute force attack. Unlike conventional cryptographic algorithm, this new approach establishes tradeoff between security strength and memory buffer size. However, to increase perceptual security strength there is need to design highly randomized distribution function and keeping in the view different level of perceptual security demands of different multimedia services, there is need to define parameterized distribution function to control the level of distortion of video as per needs of services. The limitation of proposed security framework is that motion remain unencrypted, hence motion is predictable.Therefore, there is further need of improvement to encrypt the motion as well.

4.3 Power Consumption Analysis of Proposed Method

Energy Consumption of the software/program can be estimated by measuring instruction level power consumption assumingthat each instruction consumes a finite amount of power. This energy consumption model provides base for the estimation of power cost of the software. As the constrained display/browsing devices are becoming popular for example 'Aaksh' tablets, the need of software consuming less power & computing resources is becoming ever important. Ignoring some of the I/O constraints it can be safely stated that the power consumption depends on the instructions executed by the CPU at machine level. For processor, each instruction (Like Mov, Add, Mul, Store, read etc.) has defined base energy costs, not necessarily same because number of cycles needed to execute the instructions differ instruction to instruction.

V. Tiwari, S. Malik and A. Wolf proposed instruction level power model to assess impact of software to the overall power consumption. The average power P consumed by the programduring its execution , is estimated by $P=I*V_{cc}$, where I is the average current and V_{cc} is the supply voltage. As power is the rate at which energy is consumed, therefore energy consumption of a program is estimated by E=P*T, where T is the execution time of the program defined as $T=N*\tau$, where N is the number of cycles taken by the program and τ is the clock period. This discussion establishes that power consumption of program is directly proportional to the number of cycles taken by the program when executed by the processor. On basis of this, it is concluded that minimization of instructions/cycles during execution of program results in less power consumption. Proposed method (Decryption) is optimized in terms of number of instructions/cycles executed by program, when compared with existing technique like RSA algorithm [10].

However, V. Tiwari, S. Malik and A. Wolf also state that memory operands have high energy cost but almost all decryption programs need memory operands so in general reduced memory operand makes any software power efficient[10]. Proposed decryption performs only, single reading & writing operation so optimized in terms of number of instructions hence offers power optimized solution. This is apparent from the posteriori testing of proposed technique, given below.

Comparative Posteriori Testing of Proposed Method

For comparative purposes we executed two dummy programs, (A) Decryption algorithms use mod operator like RSA use the statement $m=c_i^d \bmod n$ for decryption, so we used simple code $(val\text{-}c_i) \bmod n$. This code was executed 10^9 times; this program execution took a total running time of 22 seconds.(B) Secondly we took the code in the proposed model and again ran it 10^9 times; this took a total time of 14 second .

From the above observation, it is clear that relative to the existing models the proposed model improves the efficiency by 40% hence it is concluded less execution time means less power consumption. This improvement is based on the execution performed on 'Aakash' tablets (processor speed 1 GHz, RAM 512 MB) under C++ environment.

In summary, it can be inferred that the developed method is a low power design and has potential to address security needs of constrained devices like 'Aakash'.

5 Simulation Results

We use MATLAB to simulate the above encryption and decryption algorithms. We run programs on the computer with Processor Intel® Core(TM)2 Duo CPU T5670 @ 1.80 GHz, 1.00 GB RAM. Our method uses standard image color model RGB & directly manipulate each frame completely at byte level i.e. n=8. In experiment, benchmark video sequence 'Foreman' have been used for the analysis as raw digital video in RGB-24(QCIF:176X144) base

color model. One more video sequence xylophone (size320x240) is also take to measure decryption time. Encryption and Decryption on said video is performed firstly under conventional crypto system and next under proposed RRP security framework. Linear mathematical mapping on alternate pixel is applied for the given below results. In given simulation encryption unit size is 8 and buffer size is 2^8, hence no change in size of encrypted video is observed.

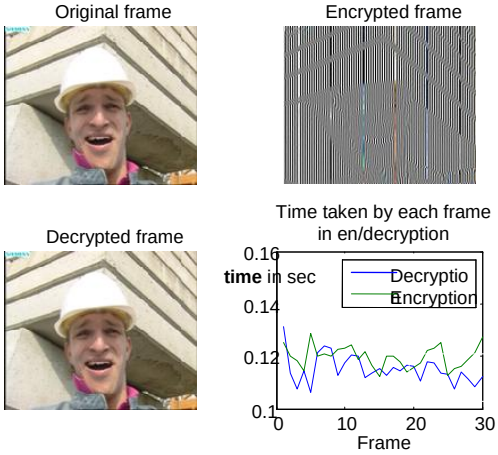


Figure 5: Encryption/Decryption under Conventional Crypto Framework

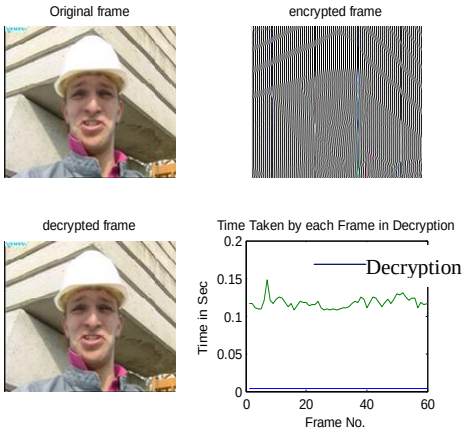


Figure 6: Encryption/Decryption under Proposed RRP Framework

From above results we can see, there is significant difference in decryption time under conventional crypto framework and Proposed RRP security framework. Decryption time under proposed RRP security frame is highly negligible approximately .005 seconds and constant for each frame, hence in today's scenario proposed RRP framework may become viable security solution for all kind of users and all type of multimedia services. Further constant time information at client also makes it probably secure against side channel attack.

Further results are presented to show the different size video, decryption time and increased buffer size however encryption unit size is same as above. When buffer size is not as $2^{\text{sizeofencryptionunit}}$ simply size of encrypted video is increased so to achieve best results buffer size should equals to $2^{\text{sizeofencryptionunit}}$.

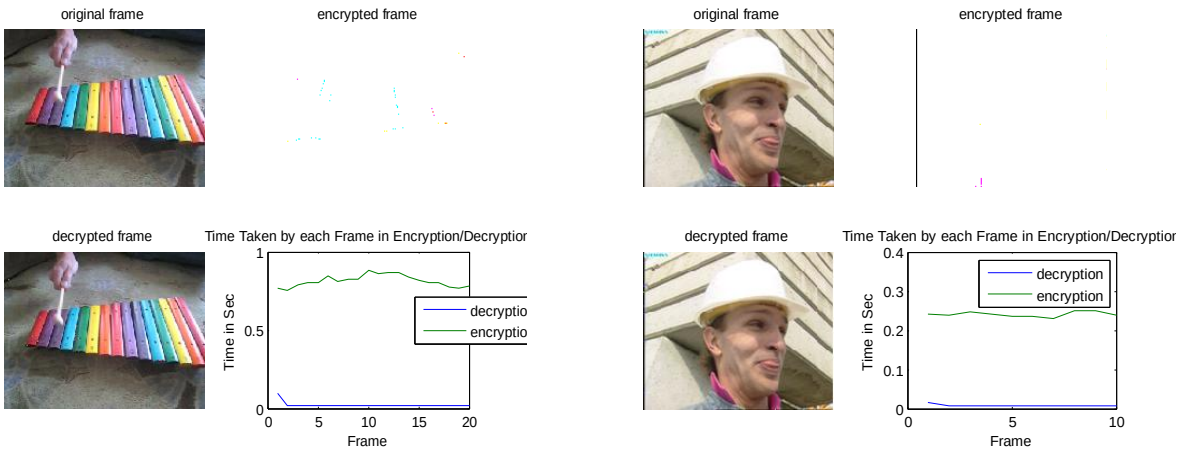


Figure 7: Encryption unit size 8, buffer size 512, increased size of encrypted video

Proposed technique may be integrated with scrambling for more confusion at texture level and more manipulation at scrambling level may help in hiding motion information. This integration doesn't add much cost to decryption process.

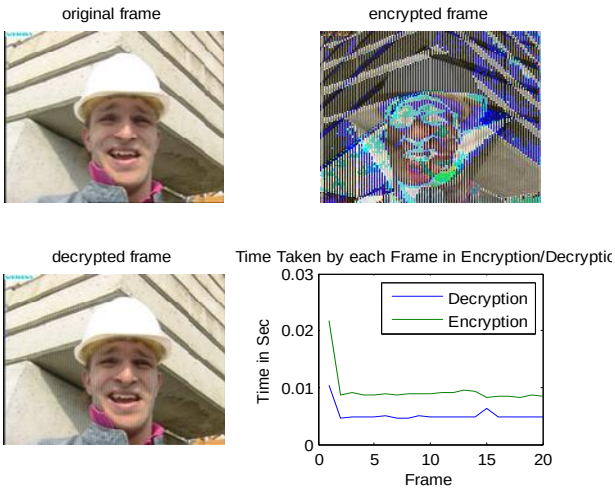


Figure 8: Integration of Scrambling with Proposed Framework

From above results we can see, there is significant difference in decryption time under conventional crypto framework and Proposed RRP security framework, hence in today's scenario proposed RRP framework may become viable security solution for all kind of users and all type of multimedia services.

6Conclusions

Current software implementations of cryptographic techniques are slower and hardware implementation restricts the flexibility in selection of algorithm as per security needs of applications. We have proposed a method, which incorporates flexibility of software implementation and faster execution of hardware implementation. Proposed security frameworkis capable to offer security solution for wide range of multimedia services under different communication environment. Proposed framework is based on innovativeidea of passing reference as till date no method is devised , to transmit data from one system to another by sending the reference instead of data.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. Proposed architecture is highly suitable for wide range ofvideo streaming applications in heterogeneous environment and offers reasonably good security. This approach demonstrates very low processing overhead on video sinks & negligible decryption time, therefore making it highly suitable for the constrained devices for prolonged battery life.

We strongly believe this may lead to new developments in the area of security of multimedia applications as well as remote reference passing concept. Further, Chip realization of proposed model can make it more effective & productive as it has potential for commercial production.

References

1. Thomas Eisenbarth, Sandeep Kumar, ChristofPaar and Axel Poschmann,"A Survey of Lightweight-Cryptography Implementations" ,IEEE journal of Design and Test of ICs for Secure Embedded Computing,Vol 24 , Issue 6, 2007 , pp. 522 - 533
2. Erich Nahum, Sean O'Malley, HilarieOrman, Richard Schroeppel, "Towards High Performance Cryptographic Softwares", Research Report by NSF , grant by ARPA & NCSC
3. L. Batina et al., "Hardware Architectures for Public KeyCryptography Integration", VLSI J., Vol. 34, no. 6, 2003,pp. 1-64.
4. Joan Boyar and Lene M. Favrholdt,"The relative worst order ratio for on-line algorithms", ACM Transactions on Algorithms, 3(2), 2007. Article No. 22.
5. G. Leander et al., ''New Lightweight DES Variants'', Proc.Fast Software Encryption (FSE 07), LNCS 4593, Springer-Verlag, 2007, pp. 196-210.
6. A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher", Proc. Workshop Cryptographic Hardware andEmbedded Systems (CHES 07), LNCS 4727, Springer,2007, pp. 450-466

7. Adam Dunn, Environment ,"Independent Performance Analyses of Cryptographic algorithms" , 26 Australian Computer Science Conference(ACSC2003), available in ACM Library.
8. H Eberele, "A high speed DES implementation for network applications", Technical report 90, Digital Equipment Corporation Systems Research Centre, Sept. 1992
9. Paul C. van Oorschot,Alfred J. Menezes, and Scott a. Vanstone,Hand book of applied cryptography, CRC pressInc., Florida, 1996.
10. Vivek Tiwari, 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
11. Xiaofeng Wang, Nanning Zheng &Lihua Tian, Hash key-based video encryption scheme for H.264/AVC, Signal Processing:Image Communication 25(2010), 427-437.
12. Fuwen Liu, Hartmut Koenig. A Survey of Video Encryption Algorithms. Computer & Security 29(2010) ,3-15 .
13. A. Uhl and a. Pommer. Image and Video Encryption: from Digital Rights Management to Secured Personal Communication, Advances in Information Security, vol 15, Boston, USA: Springer Science+ business Media, Inc., 2005.
14. C.P. Wu and C. C. J. Kuo. Design of Integrated Multimedia Compression and Encryption Systems, IEEE transaction on multimedia(7)(5):828-839; October 2005