A Survey On Cryptographically Secured Video Transmission

Heena Pandya[1] Haresh Suthar[2]
[1,2]Department of Electronics and Communication
[1,2]Parul Institute of Engineering & Technology, Limda, Vadodara, India

Abstract--- In the recent years, there has been a tremendous improvement and emergence of technologies for communications and digital multimedia. Such an environment has allowed for the realization of many fascinating multimedia applications. Almost instantaneous delivery of entertainment videos, pictures, and music are available to everyone who is connected to a multimedia distribution system. Hence there is a need for multimedia security for multimedia applications.
We investigate the novelty of secure data for e.g. Multimedia data Transmission using cryptographic techniques. Over the last few years several encryption algorithms have applied to secure video transmission. Comparison between Symmetric and Asymmetric methods and representative video algorithms were presented. After comparison we propose encryption algorithm that is the International Data Encryption Algorithm a Symmetric Block Cipher for protection of the multimedia data. Advantages of our encryption algorithms not only lie in fast and easy implementation but also in providing considerable security.
A software tool MATLAB will be used to implement algorithm for comparing video encryption methods.
*Keywords:*Cryptography, symmetric keys, Asymmetric keys, International Data Encryption Algorithm Standard (IDEA)

I. INTRODUCTION

Multimedia technologies have popularized applications like video conferencing, pay-per-view, Video-On Demand (VOD), video broadcast, etc. In such applications, confidentiality of the video data during transmission is extremely important. Various methods of video encryption are available and used to encrypt a selected portion of video data, for real-time applications, light-weight encryption algorithms were also proposed.

Naive, multimedia encryption algorithms rely on textual encryption schemes for the protection of the multimedia data. These are generally incapable for applications like real-time video encryption as these algorithms consume more time for encryption. This approach of selective encryption has been extensively studied in multimedia security literature over the last decade.

Usage of the selective encryption typically reduces the computational time as it needs selected data to be encrypted compared to the encryption of the whole multimedia data. However, even encryption of the selected data using the textual encryption algorithms, takes much time, thus making them not suitable for real-time encryption. Most of the techniques discard this and directly use textual encryption algorithms.

Some recent works have tried learning the distribution of the video data. This learning even though reduced some computational time but, cannot be considered as good solution for multimedia encryption .In real time application, scrambling based encryption schemes are also designed. These algorithms are computationally fast because they do not use the complex operations for the encryption. The problem with these encryption schemes is that, they are prone to the attacks and are considered to not secure.
The techniques discussed in literature are either computationally expensive or insecure for real time systems. Hence, efficient approaches are required.
We propose to present some solutions to the real-time (fast enough for most popular applications) video encryption using the selective encryption algorithms.

Fig. 1: Typical Distributed System for the Multimedia Communication [2]

II. CRYPTOGRAPHY

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, multimedia, VOD, pay-tv, etc. security becomes a tremendously important issue to deal with.
There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords.
One essential aspect for secure communications is that of cryptography. It is important to note that cryptography is *necessary* for secure communications; it is not by itself sufficient.
The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today.

A. THE PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is

an ancient art the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication*:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.
- Integrity*:* Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation*:* A mechanism to prove that the sender really sent this message.
- Cryptography, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *cipher text*, which will in turn (usually) be decrypted into usable plaintext.

B. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 2):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

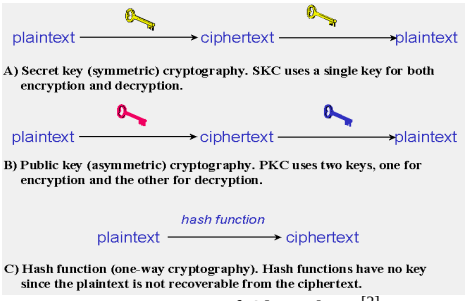

Fig. 2: Types of Algorithms [2]

III. COMPARE SYMMETRIC AND ASYMETRIC KEYS

Symmetric key	Asymmetric key
1. Works more Fast 2. Requires a secure mechanism to deliver keys properly. 3. Symmetric key provides confidentiality but not Authenticity 4. Not consuming too much computing power	1. Works more slowly. 2. Key provides a better key distribution than symmetric systems. 3. Can provide authentication and confidentiality. 4.Consuming too much computing power

IV. LITERATURE REVIEW

Studied the impact of an encryption methods and representative video algorithms with respect not only to their encryption speed but also their security level and stream size and Introduces efficient and secure video encryption approach with use of distributed & parallel environment to make secure video encryption feasible for real-time applications without any extra dedicated hardware at receiver side.

Vbr video streaming over wireless networks which Improve the combined system performance of video frame quality and playout smoothness based on the feedback information of wireless network estimation.

SR. NO.	ALGORITHMS	FEATURES
1.	DES	• 56-bit keys. • particularly problematic on smartcards
2.	Blowfish	• Alternative to DES. • Key length -128 bits. • up to 16 rounds
3.	3DES	• Uses 3 keys and 3 DES executions. • Key length of 168 bits.
4.	AES	• 128, 192, 256 bit blocksize.
5.	IDEA	• 128 bit key, 64 bit block size, 8 rounds. • Doesn't use S-boxes. Uses binary addition rather than exclusive-or.

V. PRAPOSED ALGORITHM

A. International Data Encryption Algorithm

The Data Encryption Standard (DES) algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications.

Although introduced in 1976, it has proved resistant to all forms of cryptanalysis. However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours.

International Data Encryption Algorithm (IDEA) is a block cipher designed by Xenia Lai and James L. Massey of ETH-

Zürich and was first described in 1991. It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem.

IDEA was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies. It is also interesting in that it entirely avoids the use of any lookup tables or S-boxes. When the famous PGP email and file encryption product was designed by Phil Zimmermann, the developers were looking for maximum security. IDEA was their first choice for data encryption based on its proven design and its great reputation.

The IDEA encryption algorithm

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components (VLSI Chip)
- can be used efficiently
- may be exported world wide

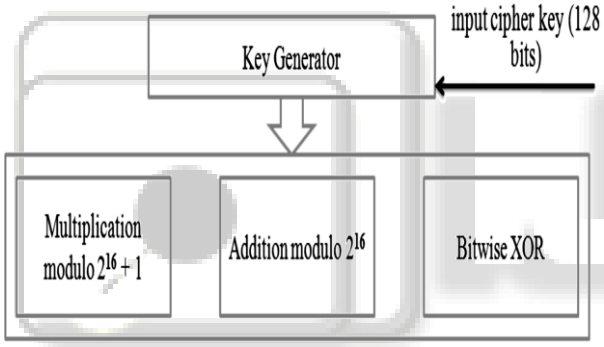

Fig. 3: Hardware components required for IDEA

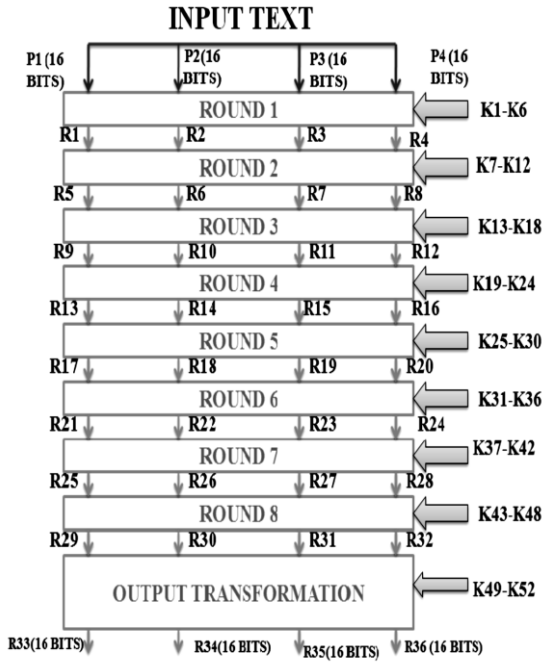

Fig. 4: Overview of IDEA algorithm

1) Description of IDEA

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process.

2) Key Generation

The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

The key sub-blocks used for the encryption and the decryption in the individual rounds are shown in Table 1. Convenience in the fusion process and post processing analysis. Before fusing the images they were registered.

After registering, the fusion approaches- simple averaging,

Round 1	$Z_1^{(1)} Z_2^{(1)} Z_3^{(1)} Z_4^{(1)} Z_5^{(1)} Z_6^{(1)}$
Round 2	$Z_1^{(2)} Z_2^{(2)} Z_3^{(2)} Z_4^{(2)} Z_5^{(2)} Z_6^{(2)}$
Round 3	$Z_1^{(3)} Z_2^{(3)} Z_3^{(3)} Z_4^{(3)} Z_5^{(3)} Z_6^{(3)}$
Round 4	$Z_1^{(4)} Z_2^{(4)} Z_3^{(4)} Z_4^{(4)} Z_5^{(4)} Z_6^{(4)}$
Round 5	$Z_1^{(5)} Z_2^{(5)} Z_3^{(5)} Z_4^{(5)} Z_5^{(5)} Z_6^{(5)}$
Round 6	$Z_1^{(6)} Z_2^{(6)} Z_3^{(6)} Z_4^{(6)} Z_5^{(6)} Z_6^{(6)}$
Round 7	$Z_1^{(7)} Z_2^{(7)} Z_3^{(7)} Z_4^{(7)} Z_5^{(7)} Z_6^{(7)}$
Round 8	$Z_1^{(8)} Z_2^{(8)} Z_3^{(8)} Z_4^{(8)} Z_5^{(8)} Z_6^{(8)}$
Output Transform	$Z_1^{(9)} Z_2^{(9)} Z_3^{(9)} Z_4^{(9)}$

Table 1: Encryption of the key sub-blocks

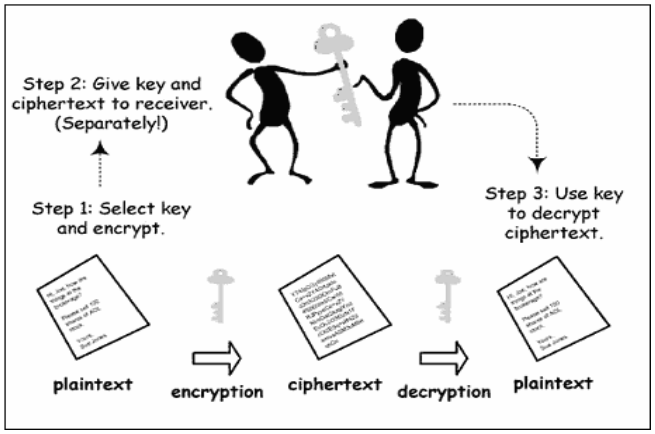

Fig. 5:.symmetric key

3) Encryption

The functional representation of the encryption process is shown in Figure 6. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail.

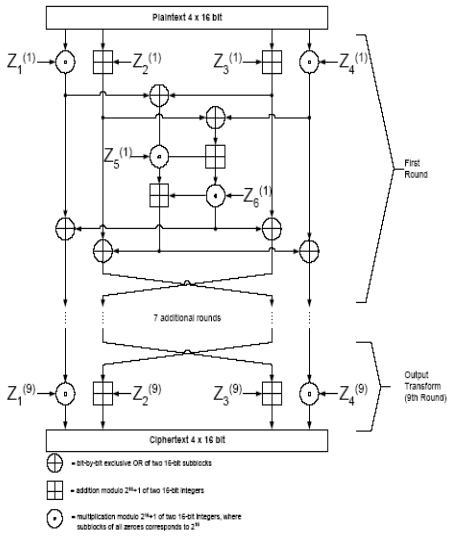

Fig. 6: The IDEA structure

FIRST LAYER: Apply two 16- bit Additions and two 16-bit Multiplications to quarter blocks using appropriate parts of the round keys.

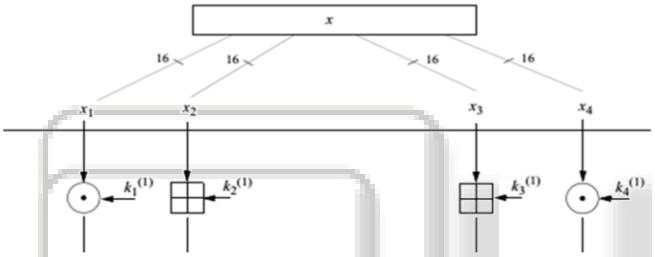

Fig. 7: First round of IDEA algorithm

SECOND LAYER: calculate two intermediate quarter blocks with 16-bit addition and multiplications using parts of round key. XOR intermediate quarter blocks from layer 1.Exchange the inner quarter blocks.

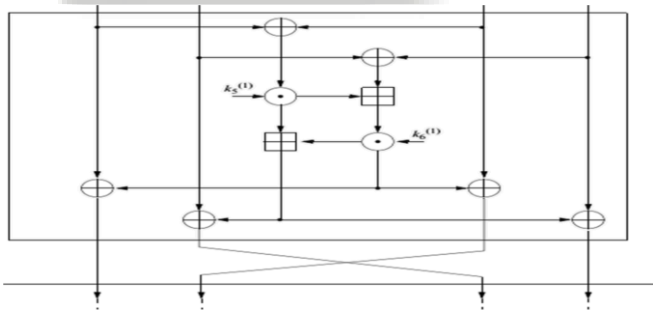

Fig. 8: Second round of IDEA algorithm

After the 8th round exchange the inner quarter blocks then apply 16-bits applications and multiplications using part of the round key

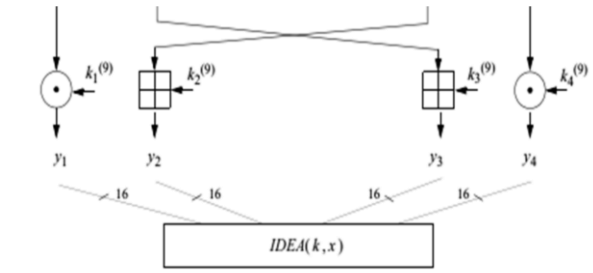

Fig. 9: Second round of IDEA algorithm [3]

4) Decryption

Round 1	$Z_1^{(9)-1}$ -$Z_2^{(9)}$-$Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
Round 2	$Z_1^{(8)-1}$ -$Z_3^{(8)}$-$Z_2^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
Round 3	$Z_1^{(7)-1}$ -$Z_3^{(7)}$-$Z_2^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
Round 4	$Z_1^{(6)-1}$ -$Z_3^{(6)}$-$Z_2^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
Round 5	$Z_1^{(5)-1}$ -$Z_3^{(5)}$-$Z_2^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
Round 6	$Z_1^{(4)-1}$ -$Z_3^{(4)}$-$Z_2^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
Round 7	$Z_1^{(3)-1}$ -$Z_3^{(3)}$-$Z_2^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Round 8	$Z_1^{(2)-1}$ -$Z_3^{(2)}$-$Z_2^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Output Transform	$Z_1^{(1)-1}$ -$Z_2^{(1)}$-$Z_3^{(1)}$ $Z_4^{(1)-1}$

Table 2: Decryption of the key sub-blocks [3]

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process.

5) Implementation

Although IDEA involves only simple 16-bit operations, software implementations of this algorithm still cannot offer the encryption rate required for on-line encryption in high-speed networks. Software implementation running on a Sun Enterprise E4500 machine with twelve 400MHz Ultra-Hi processor, performs 2.30 x 10^6 encryptions per second or a equivalent encryption rate of 147.13Mb/sec, still cannot be applied to applications such as encryption for 155Mb/sec Asynchronous Transfer Mode (ATM) networks. Hardware implementations offer significant speed improvements over software implementations by exploiting parallelism among operators. In addition, they are likely to be cheaper, have lower power consumption and smaller footprint than a high speed software implementation.

6) Applications

Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were highest security requirements along with easy hardware and software implementation for fast execution.

The IDEA algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are:

1) Audio and video data for cable TV, pay TV, video conferencing, distance learning, business TV, VoIP
2) Sensitive financial and commercial data
3) Email via public networks
4) Transmission links via modem, router or ATM link, GSM technology

5) Smart cards

VI. CONCLUSION

Video communication for commercial usage, e.g. in video on demand services or business meetings , to transmit secure video using IDEA algorithm,by compairing all the encryption and decription algorithams parameters such a way that the information should not be stolen by other by using Cryptography technique.

VII. FUTURE WORK

In Future, The two methods namely, Data Encryption Standard (DES) and our proposed algorithm International Data Encryption Algorithm Standard (IDEA) will compared in such a manner which gives secure video at the destination when implemented on MATLAB, whose result is best that the video quality remains good after

REFERENCES

[1] C. Narsimha Raju, Video Specific Fast Encryption Algorithms, International Institute of Information Technology Hyderabad, India May 2009
[2] F. Liu and H. Koenig, "A Novel Encryption Algorithm for High Resolution Video," in Proceedings. Of ACM Multimedia NOSSDAV, pp. 69–74, 2005
[3] I. Agi and L. Gong, "An empirical study of MPEG video transmission," in Proceedings of the Internet Society Symposium on Network and Distributed Systems Security, pp. 137–144, 1996.
[4] J. B. Kam and G. I. Davida. Structured design of substitution- permutation encryption networks. IEEE Transactions on Computers.
[5] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video.," in Web, www.gadegast.de/frank/doc/secmpeg.pdf, 1995.
[6] L. Qiao and K. Nahrstedt, "A new algorithm for MPEG video encryption," in Proceedings of First International Conference on Imaging Science System and Technology, pp. 21–29, 1997
[7] L. Jun, Z. LingLing, X. Changsheng, and H. Hao, "A two-way selective encryption algorithm for mpeg video," in IWNAS '06: Proceedings of the 2006 International Workshop on Networking, Architecture,and Storages, (Washington, DC, USA), pp. 183–187, IEEE Computer Society, 2006.
[8] Maples T.B. and Spans G.A. Performance study of a selective encryption scheme for the security of networked, real-time video. In ICCC'95, 1995.
[9] Qiao L. and Nahrstedt K. Comparison of mpeg encryption algorithms. International Journal on Computer & Graphics, 22(3), 1998.
[10] T. B. Maples and G. A. Spanos, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video.," in Proceedings of Fourth International Workshop on Multimedia Software Development '96), 1995.
[11] Trupti Dandamwar " Introduction to Real Time & Secure Video Transmission using Distributed & Parallel Approach" International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 5, October 2012
[12] M. Abomhara, "An Overview of Video Encryption Techniques" International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010

