Secured Real Time Video Transmission with Significant Improvement in Privacy Preservation

Karishma Chaudhary[1], Gayatri Pandi (jain)[2]

1Computer Engineering Department, LJIET, Ahmedabad, Gujarat, India
2 Head and PG Co-coordinator, Computer Engineering Department,LJIET, Ahmedabad,India

ABSTRACT

In today's world, security and protection issues of the transmitted information have turned into a vital worry in media innovation. In the course of the most recent couple of years a few encryption algorithms have connected to secure video transmission. While countless encryption plans have been proposed in the literature and some have been utilized as a part of genuine items, cryptanalytic work has demonstrated the presence of security issues and different shortcomings in the greater part of the proposed interactive media encryption plans. In this paper, International Data Encryption Algorithm (IDEA) is a symmetric key encryption method and utilizations 128-bitkey more than 64-bit plain content with eight and a half round. To improve the innovation in IDEA, another methodology is presented in which we will set up two distinctive keys for encryption and decoding separately which was single key in IDEA. This will present more security in IDEA by making it an asymmetric key encryption algorithm.

Keywords :- *International Data Encryption Algorithm (IDEA), Asymmetric key encryption.*

1. INTRODUCTION

Cryptography is derived from Greek word .It has 2 parts: 'crypto' means "hidden, secret" and 'graphy' means "writing".It is a study of techniques for secure communication in the presence of third parties to maintain information securities such as data integrity, confidentiality , authentication, and non-repudiation. It is an art to transform the messages to make them secure and immune against security attacks [1]. The art of protecting information by transforming into an unreadable format, called cipher text or decrypt the message into plain text. The cipher text is only understood by someone who only knows how to decrypt it. The information is encrypted using an encryption algorithm, which specifies how the message is to be encoded. Any intruder that can see the cipher text should not be able to determine about the original message. Only an authorized party is able to decode the cipher text which requires a secret decryption key.

Types of Cryptography

There are two types of cryptography:

Secret key cryptography or Symmetric-key cryptography: In SKC, the sender and the receiver know the same secret code, which is known as key. With the same key messages are encrypted by the sender and decrypted by the receiver. It can be of two types: Stream Buffer, Block Buffer.Stream Buffer: Stream buffer encrypts the digits of a message one at a time. Stream Cipher functions is used on a stream of data one at time by operating on it by bits. It consists of two components: 1) a key stream generator and 2) mixing function. Mixing function uses XOR function, and key stream generator is unit in stream encryption algorithm. Block cipher: In Block cipher, it takes a number of bits and then encrypts them as a single unit. Data is encrypted/decrypted if data is in the forms of blocks. In simple words, the plain text is divided into blocks which are used to produce blocks of cipher text padding the plaintext in blocks. 64 bits blocks have been commonly used.[1]

Public key cryptography or Asymmetric-key cryptography: Asymmetric key (or public key) encryption is

used to solve the problem of key distribution. In PKC, two keys are used; private keys and public keys. For encryption public key is used and for decryption private key is used. Public key is known to public and private key is known to the user.

A. Cryptography Goals

There are some goals of cryptography that are given below:

1) Authentication: Sender and data receiver must be authenticated before sending and receiving data.
2) Confidentiality: The user who is authenticated, can access the messages
3) Integrity: Data is free from any kind of modification between sender and receiver.
4) Non-Repudiation: The sender the receiver cannot deny that they had sent a message.
5) Service Reliability: Attackers can attack on secure systems, which may affect the service of the user.

2. LITERATURE REVIEW

Table1: The comparison of all above cryptography Techniques

Algorithm	Created By	Year	Key Size	Block	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64 bits	16	Festial	No	Not Strong Enough
3DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security
AES	Joan Daemen & incent Rijmen	1998	128, 192, 256 bits	128 bits	10,12, 14	Substitution Permutation	Yes	Replacement for DES, Excellent Security
Blowfish	Bruce Schneier	1993	32-448	64 bits	16	Festial	Yes	Excellent Security
RC4	Ron Rivest	1987	Variable	40-2048	256	Festial Stream	Yes	Fast Cipher in SSL
RC2	Ron Rivest	1987	8-128 64 by default	64 bits	16	Festial	-	Stream Cipher
IDEA	James Massey	1991	128 bits	64 bits	8.5	Substitution Permutation	No	Not Strong Enough
RC6	Ron Rivest, Matt Robshaw	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	Good Security
RSA	Rivest,, Shamir, Adleman	1977	1,024 to 4,096	128 bits	1	Public Key algorithm	No	Excellent Security, low speed
Diffie Hellman	Whitfield Diffie , Hellman	1976	1024 to 4096 bits	512	-	Asymmetric algorithm	Yes	Many attacks
MD5	Ronald Rivest	1992	Series of MD	512	4	Merkle–Damgård		Hash Function

3. PROPOSED METHOD

International Data Encryption Algorithm converts a 64-bit plain text into 64-bit cipher text using a single key of 128-bits both for encryption and decryption. For imparting more security to IDEA cipher, we will implement another cipher with IDEA i.e. RSA cipher. RSA cipher is an asymmetric key cipher which uses two different keys for encryption and decryption.

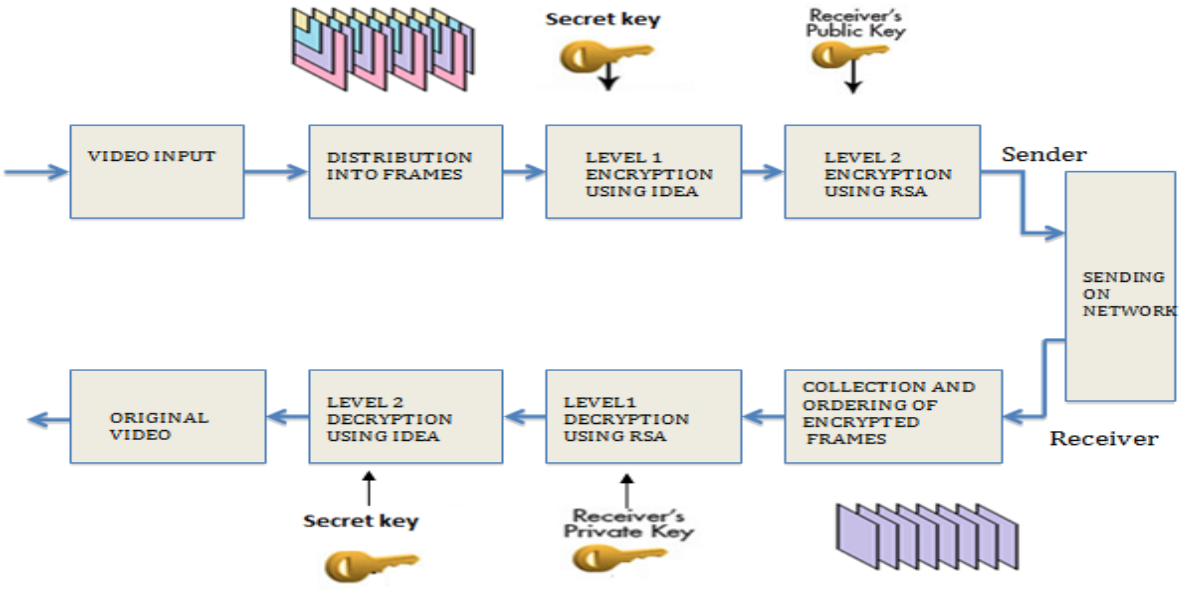

Fig 1: Flow diagram of proposed work

Encryption:

A plain text (T) acts as an input for the encryption process in proposed algorithm. The first process of encryption of proposed algorithm is the IDEA Encryption block. So, this plain text (T) goes to IDEA encryption block. Here, the key used is 'x'. The text from this block gets converted into cipher text, T1. This T1 is cipher text of IDEA encryption block and acts as input i.e. plain text for RSA encryption block. Since, RSA is an asymmetric key cipher, it uses two different keys. Hence, the key applied is 'x+y' where 'x' is the key from above block and 'y' is Public key in RSA block. Here in this block, T1 gets encrypted into final cipher text i.e. T2.The whole encryption part of proposed algorithm is described in the following flowchart.

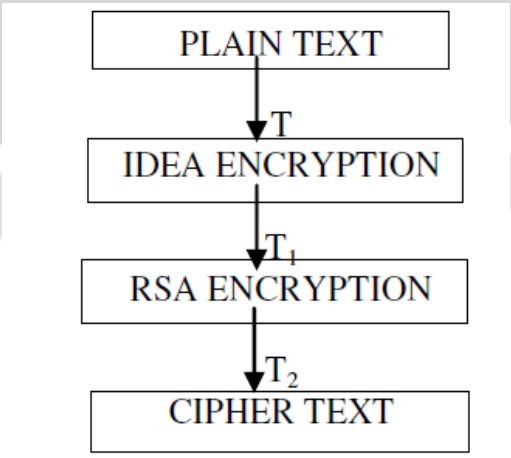

Fig 2 Flowchart representing encryption in proposed algorithm

In encryption phase, the plain text is to be encrypted and converted into cipher text using two ciphers, IDEA and RSA. Encryption by both ciphers is discussed in following phases. In order to achieve the advancements in the cipher, RSA is introduced in the IDEA cipher. This brings up two different phases of encryption:

PHASE I: We apply IDEA cipher and generate key and text. Let the key be 'x' and text be 'x/2'. This phase lasts

for 8 rounds (R1, R2, R3, R4, R5, R6, R7 and R8) and a last formation round (half round). Each full round uses different set of sub keys viz. R1, R2, R3 , R4, R5, R6, R7 and R8 uses 6 sub keys (Z1, Z2, Z3, Z4, Z5 and Z6) since These are full rounds. And the half round uses only four sub keys Z1, Z2, Z3 and Z4. This phase is same for all the IDEA ciphers. The plain text 'T' in this phase is converted into cipher text 'T1'.

PHASE II: In this phase, we introduce the RSA cipher in IDEA cipher. The RSA algorithm involves the presence Of another whole cipher which increases the steps of operation in addition to those of IDEA. As RSA is an Asymmetric key cipher, it introduces the concept of two different keys, one for encryption (public key) and the other One for decryption (private key). This phase treats T1 as an input (plain text) and encrypts it into 'T2'. T2 is the final encrypted text.

T= Plain text

T1= Cipher text after IDEA cipher and Plain text for RSA cipher.

T2= Final cipher text.

Decryption:

The cipher text (T2) of the encryption block of proposed algorithm acts as an input (plain text) for the decryption process in IDEA. Since, encryption with RSA is done at the end; decryption with RSA will take place before that of IDEA. So, the input goes to RSA decryption block. Here, the key used is 'x+z' where 'x' is the key from IDEA encryption block and 'z' is Private Key in RSA block. The text from this block gets converted into plain text, T1. This T1 is plain text of RSA decryption block and acts as input i.e. cipher text for IDEA decryption block. In IDEA block, the key applied is 'x' which is same to that of IDEA encryption block since it is symmetric key cipher. Here in this block, T1 gets decrypted into final plain text i.e. T. The whole decryption part of proposed algorithm is described in the following flowchart.

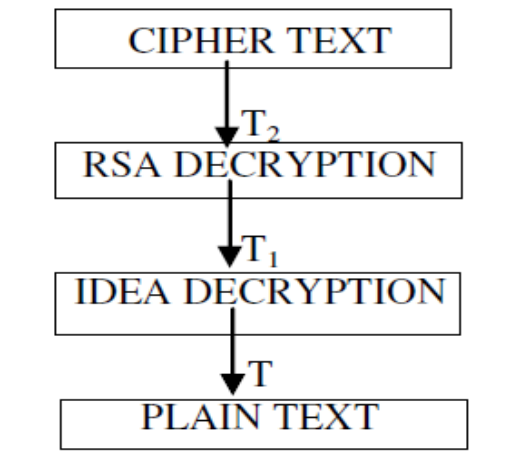

Fig 3 Flowchart representing decryption in proposed algorithm

4. SIMULATION STUDY

- Original Video is converted into number of image frames which is encrypted using RSA and IDEA. After encryption did the same process of decryption to get the original image.
- Here we have taken an original video shown below.

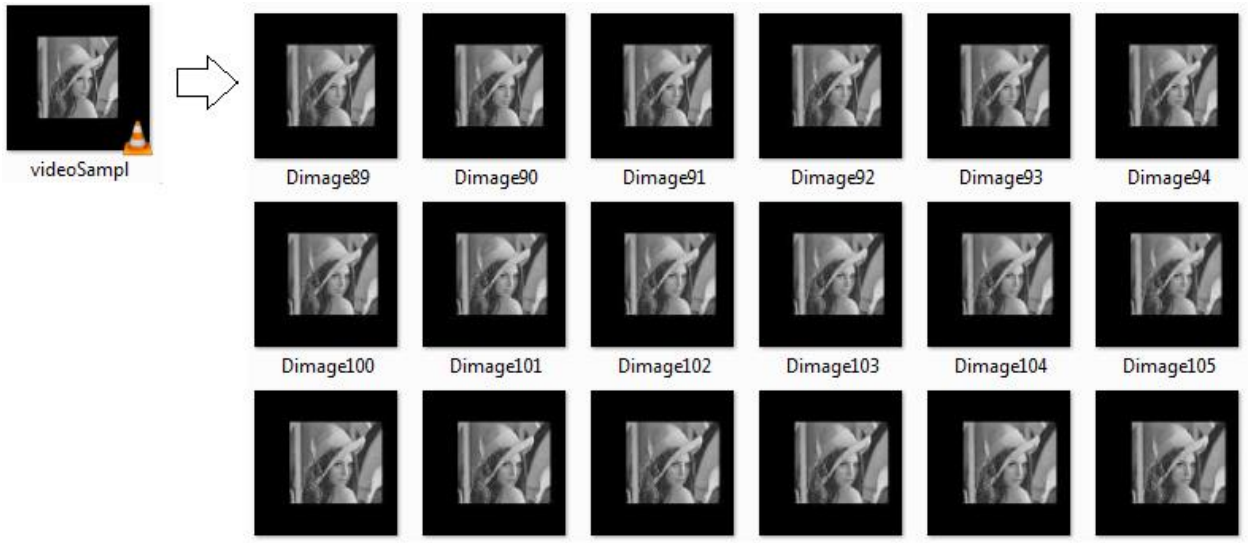

Fig 4 Video Converted into frames

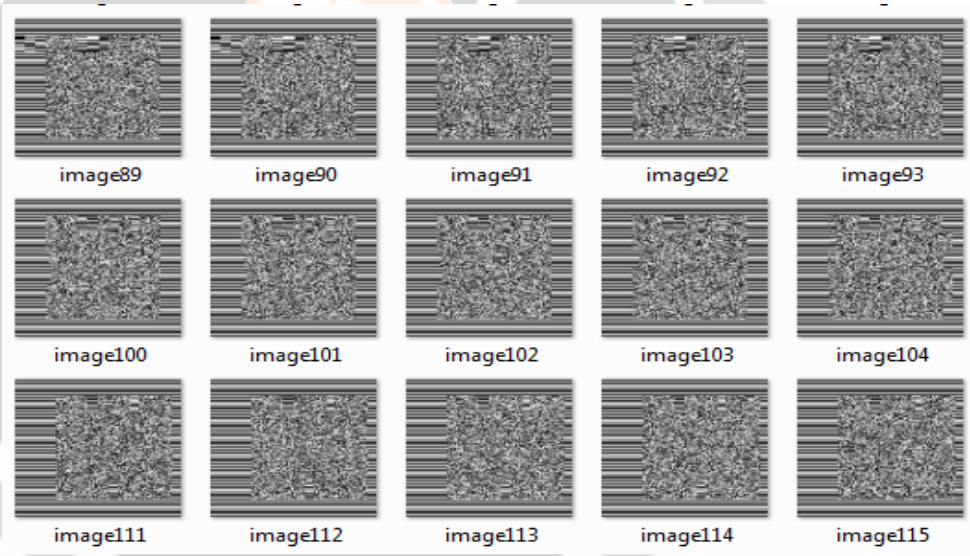

Fig 5 Encryption using IDEA + RSA

Fig 6 Image Encryption and Decryption using proposed algorithm

Table 2: Result of proposed Algorithm

Sr.no.	Encryption and Decryption Method	MSE	PSNR in db
1.	AES(image)	14.6603	30.4694
2.	IDEA (image)	32.7208	34.7538
3.	AES(video)	2.1449	37.3303
4.	IDEA (video)	2.077	39.9318

5. CONCLUSIONS & FUTURE SCOPE

Since, IDEA had weak key classes which hindered in the faultless security of the data; there was a need of such a Cipher which does not have weak keys. Proposed algorithm made it possible to fade away the weak keys from the cipher hence increased the data security. It uses RSA algorithm in addition to the IDEA cipher making an enhancement in it. Now the keys cannot be detected easily. So, data recovery is not possible. The addition of RSA cipher has included the concept of two different keys each for encryption and decryption which was only one key in IDEA.

Proposed algorithm has united IDEA cipher with RSA cipher for making the keys strong hence undetectable and unrecoverable. But it makes it a heavy operation to be taken out as the whole operation gets divided into two. One operation is that which involves the IDEA cipher and another operation involves the RSA cipher. This division of operations makes it a lengthy procedure to be carried out which takes much of time and efforts. So, such an algorithm can be created which uses less time and fewer efforts.

6. REFERENCES

1. Anjula Gupta , Navpreet Kaur Walia, "Cryptography Algorithms: A Review", 2014 IJEDR , Volume 2, Issue 2 , ISSN: 2321-9939,pp 1667-1672

2. Chia Long Wu,Chen Hao Hu,"Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", Innovations in Bio-Inspired computing and Applications(IBICA), 2012, pp. 307 – 311.

3. Da Silva, J.C.L ,"Factoring Semi primes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2010, pp.182–183

4. Xiaochun Cao, Na Liu, Ling Du, Chao Li, "PRESERVING PRIVACY FOR VIDEO SURVEILLANCE VIA VISUAL CRYPTOGRAPHY" , Signal and Information Processing (ChinaSIP), 2014 IEEE China Summit & International Conference, Conference Location :Xi'an, DOI:10.1109/ChinaSIP.2014.6889315, Print ISBN:978-1-4799-5401-8, INSPEC Accession Number:14563468, Date of Conference:9-13 July 2014, pp:607 – 610

5. Majid Masoumi , Shervin Amiri , "A Blind scene-based watermarking for video copyright protection" , ELSEVIER,International Journal of Electronics and Communications (AEÜ), Accepted 28 November 2012,pp:528 – 535

6. Pooja Deshmukh, Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption" , IEEE Information Communication and Embedded Systems (ICICES), 2014 International Conference ,

Conference Location :Chennai, Print ISBN:978-1-4799-3835-3, INSPEC Accession Number:14915668, Date of Conference:27-28 Feb. 2014, pp:1 – 5

7. Heena Pandya, Haresh Suthar, "A Survey On Cryptographically Secured Video Transmission", International Journal for Scientific Research & Development,Vol. 1, Issue 11, 2014 , ISSN (online): 2321-0613, pp:2508-2512

8. Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security", International Journal of Computer Sciences and Engineering, Volume-2, Issue-4 E-ISSN: 2347-2693, Accepted: 12/04/2014 Published: 30/04/2014, pp:76-82

9. Archita bhatnagar, monika pangaria, vivek shrivastava , "Enhancement of security in international data encryption algorithm (idea) by increasing its key length", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013,pp:3869-3871

10. Yansong Jennifer Ren, Lawrence O'Gorman, Fangzhe Chang, Thomas L. Wood, and John R. Zhang"Authenticating Lossy Surveillance Video", Information Forensics and Security, IEEE Transactions , Date of Publication :23 August 2013, Date of Current Version :10 September 2013, Issue Date :Oct. 2013, Sponsored by :IEEE Signal Processing Society, ISSN :1556-6013, INSPEC Accession Number:13747543, DOI:10.1109/TIFS.2013.2279542, pp:1678 -1687