Volume-3, Issue-10, Oct-2014 • ISSN No 2277 - 8160

Research Paper Mathematics

KLS VIDEO ENCRYPTION ALGORITHM

Monali Dave CSE, Suresh Gyan Vihar University

Dinesh Goyal CSE, Suresh Gyan Vihar University

ABSTRACT

Multimedia Communication is growing with rapid rate and it is very important to have secure communication. The communication is done via text, images or video files. Numerous encryption schemes are present today for image and video encryption, but are not much efficient. In this paper we give a method to generate an encrypted video by using encrypted video-frames. An effective and faster approach of video encryption, which is based on secure video scheme in which one can encrypt the image or video and share the encrypted message to decrypt it. So the objective behind this research paper is to propose new algorithm which will encrypt the video comparatively faster and remove the necessity of sharing the key.

KEYWORDS : Cryptography; Selective Encryption; Security; Video Encryption

INTRODUCTION

With the rapid growth of Internet and multimedia applications in distributed environments, it becomes easier for digital data owners to transfer multimedia documents across all over the world via the Internet. Therefore, multimedia security has become one of the most important aspects of communications with the continuous increasing use of digital data transmission. Video data is most commonly used multimedia data and is widely used in various kinds of content provide services and information exchange applications. In these services and applications, digital video is transmitted from service provider to end-user or exchanged between end-users over public communication channels such as satellite, wireless networks and the Internet. As these public channels are vulnerable to the attack from hackers, video security becomes more and more important.

CRYPTOGRAPHY

It is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while storing and transmitting. Data cryptography is the muddling of the content of data, such as text data, image data, audio or video files and so forth to make the data unreadable, non understandable, invisible or unintelligible during transmission or storage called coding or encryption. The ultimate goal of cryptography is to keep data safe & secure from unauthorized attackers.

SYMMETRIC KEY ALGORITHM

In symmetric key encryption, same key is used at both sender and receiver side for encryption and decryption. It is also known as secret key, because both the parties have to keep the key secret and properly protected. Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. If the key is known all the encrypted data can be easily decrypted by an intruder.

Data Encryption Standard (DES)

The DES is mostly used for the encryption of PIN(s), bank transactions, and the like. It is an example of block cipher, which uses 64 bits input key and operations are performed on blocks of 64 bits at a time. Every 8th bit in the input key is a parity check bit which means that in fact the key size is effectively reduced to 56 bits.

Advanced Encryption Standard (AES)

The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. In this algorithm a variable key length and block length can be used; the latest specification allows any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits asymmetric key algorithm.[10]

ASYMMETRIC KEY ALGORITHM

Asymmetric key algorithm is also called public key algorithm. They described a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and address the problem of secret key distribution by using two keys instead of a single key . In public key algorithm there are two keys are used. A public key, which is known to all and a private key that is secret known only by the owner.

Rivest Shamir Adelman (RSA)

Ron Rivest, Adi Shamir, and Len Adelman proposed this algorithm in 1977. It is based on the idea of factorization of integers into their prime. Assume that A and B wants to communicate with one other. B chooses two distinct large primes p and q and multiplies them together to form N, N = p*q and also an encryption exponent e, in a way, it is greatest common divisor of e and [(p-1)*(q-1)] is 1. The gcd(e,[(p-1)*(q-1)])=1. He computes his decryption key d, d=1/e (mod [(p-1)*(q-1)]). Then they makes the pair (N,e) public and keeps p and q secret. This is how generate keys, for some plain text block M and ciphertext block C: C=Me mod n, M= Cdmod n = (Me) mod n = Medmod n, the above forms are used for encryption and decryption. The values of n and e should be known by both parties, and the value of d is only known to receiver. This make a public key encryption of KU = {e,n} and private of KR {d,n}.

MPEG STRUCTURE

MPEG (Moving Picture Experts Group), approved in year 1991 and has no prerequisite for intermingled video applications.

The MPEG transformation coding algorithm includes the following steps:

- Discrete Cosine Transform (DCT)
- Quantization
- Run Length Encoding

MPEG frames are divided into three dissimilar ways encoded, which are as follows:

1) ***I-Frame***

These are binary coded frames independently adjacent frames.

2) ***P-Frame***

These are predictive coded frames, predicted from previous coded I-frame or P-frame, resulting in improvement in compression ratio (lower frame).

3) ***B-Frame***

These are bidirectional predictive frame, encoded prediction previous and future frames or I-frames or P-frames, ensures the highest level of compression.

VIDEO ENCRYPTION SCHEME

With digital video transmission, encryption methodologies are needed that can protect digital video from attacks during transmission. Because of the huge size of digital videos, they are usually transmit-

ted in compressed formats such as MPEG [1], or H.264/AVC [2]. Thus, the encryption algorithms for digital video are usually working in the compressed domain. Several video security encryption algorithms for streaming have been put forward. In most of them tried the encryption process optimization with respect to the encryption speed, and display process.

Naïve Algorithm

The most straight-forward method to encrypt every byte in the MPEG stream using standard encryption schemes such as DES or AES. The idea of Naïve algorithm is to treat the MPEG bit-stream as text data and does not use any of the special structure. Naïve algorithm ensures the security level to the entire MPEG stream by standard encryption schemes because no effective algorithm to break encryption schemes especially AES and triple DES so far. However, it cannot be applied on big video, because it is very slow especially when we use triple DES. And the delay increases because of the encryption operation and overload will be unacceptable for real time video encryption.

Pure Permutation

The idea of pure permutation algorithm is simply scrambles the bytes within a frame of MPEG stream by permutation. It is very much useful where the hardware decodes the video, but software should be used for decryption. It provides very low security because once the permutation list is figured out; all the frames can easily decrypt. If only one I-frame of MPEG stream is known, it's more than enough to decrypt the permutation list according to the Shannon's theorem.

Zig-zag Permutation

The main idea of Zig-Zag permutation approach **[3]** is instead of mapping the 8x8 block to 1x64 vector in "Zig-zag" order, it maps the individual 8x8 block to a 1x64 vector by using a random permutation list (secret key). However zig-zag permutation is vulnerable to ciphertext and known plaintext attack. The former attack the attack relies on the fact of statistical properties of the DCT coefficient, where gathering of non-zero AC coefficients in the upper left corner of the I-block. And in latter, if we know certain frames of the video in advance (known-plaintext) the secret key could be easily figured out by simply comparing the known plaintext with the corresponding encrypted frame.

VIDEO ENCRYPTION ALGORITHM

There are different four video encryption algorithms Algorithm I, Algorithm II (VEA), Algorithm III (MVEA), and Algorithm IV (RVEA) had been introduced by Bhargava, Shi and Wang.

Algorithm I

Algorithm I uses the permutation of Huffman code-words in intra-coded (I-frames). In this compression and encryption are done in a single step. The secretive part of this algorithm is a permutation p which is used to permute standard MPEG Huffman codeword list. To save the compression ratio, the permutation p must be in a way that it only permutes the code-words with same number of bits. If some of video frames known in advance the adversary could easily figure out and reconstruct the secret permutation p by comparing the known frames with the encrypted frames.

Algorithm II (VEA)

The algorithm was proposed, since the I-blocks carry the most important information so the scheme sufficient to encrypt only the sign bit of the DC coefficients in the I-frame blocks by simply XORs sign bits of DC coefficients with a secret key. The security level of this approach depends on the key length. However, if key is of too long key size that's infeasible and impractical. And if with a short key size, the system could be easily attacked.

Algorithm III (MVEA)

Bharagava and Shi in [4] have made an improvement to the Algorithm II (VEA). Rather than encrypting only the sign bit of DC coefficient in the I-frame block, the sign bit of the differential values of DC coefficient and motion vectors in P-frames and B-frames can be encrypted by XORing them with the secret key. However this improvement makes the video playback more random and more un-viewable. Just like the Algorithm II (VEA), the Algorithm III (MVEA) is relies on the size of the secret key.

Algorithm IV (RVEA)

The difference between Algorithm IV (RVEA) and Algorithm III (MVEA) is that Algorithm IV (RVEA) uses a traditional symmetric key cryptography to encrypt the sign bit of DCT coefficient and the sign bit of motion vectors. The algorithm increases the speeds of the process of encryption by only encrypt certain sign bit in MPEG stream. Therefore, it is much better than the previous three algorithms Algorithm I, Algorithm II (VEA), and Algorithm III (MVEA) in terms of security. Furthermore, it saves up to 90% of the computation time comparing with Naïve approach.

SELECTIVE ENCRYPTION ALGORITHM

AEGIS

Maples and Spanos in [5][6] have introduced AEGIS, a new secure MPEG video mechanism. It encrypts only the I-frame of all MPEG groups of frames in MPEG video stream and leave B-frame and P-frame unencrypted. In addition, to add more security to the MPEG video stream, Aegis also encrypts the sequence header which contains all of the decoding initialization parameters such as the picture height, width, frame rate, bit rate, and buffer size. Encryption of the sequence header makes the MPEG identity of stream concealed and the MPEG video stream unrecognizable. Finally, it encrypts the IOS end code (last 32 bits of MPEG stream) as a result to further conceal the bit stream of MPEG identity. It has the main drawback of increasing the length of string and consequentially the encryption time.

Sign Bit of DCT Coefficients

Shi and Bharagava [**7**] used a secret key to transform the sign bits of the DCT coefficients of MPEG video data. The secret key (k1, k2, k3….. k2m) with length of 2m is generated randomly, where the number of keys and the length of key is not limited. If the sign bits of AC and DC coefficients are represented by S, (s1, s2, s3…. s2m), then the data to be encrypted is computed as Ek(Si) = bi xor si of length 2m. The encryption operation changes the sign bits of DCT coefficients randomly. The decryption function Ek-1 is the same as the encryption function since Ek (Ek) = S. For a key of length m an adversary needs to try 2m times in order to find a key. Several keys can be used to enhance the security in this algorithm.

Byte Encryption

Griswold et al. in [8][9] have proposed an approach to encrypt bytes randomly in an MPEG stream for free distribution, while the actual bytes at the corresponding positions are transferred in encrypted form to legitimate users. This is in actual equivalent to encrypting byte at random positions. In order to guarantee a certain level of security, large amount of bytes are needed to be encrypted and care to be taken about which bytes are encrypted. In addition to the security problems, both schemes destroy the MPEG bit-stream syntax partially and potentially emulate important MPEG markers causing a decoder to crash.[10]

RELATED WORK

Mayank Arya et al (2012) proposed an approach for digital video encryption algorithm based on matrix computation scheme which uses a concept of video frame and xor operation. The proposed work was able to fully encrypt the video frame and have a better performance that can be measured by different Parameters. However, the approach is feasible only for a certain class of video sequences and video codes.

Priyanka Agarwal et al (2012) proposed the technique which selects the part of the image by the arranging the bit stream in grid form and choosing the grid's diagonal. The traditional cryptosystem has issues in many different areas such as mobile phone services, wireless networking, and applications in homeland security is energy consumption for encryption of the large volume visual data. The partial encryption algorithm of images was done.

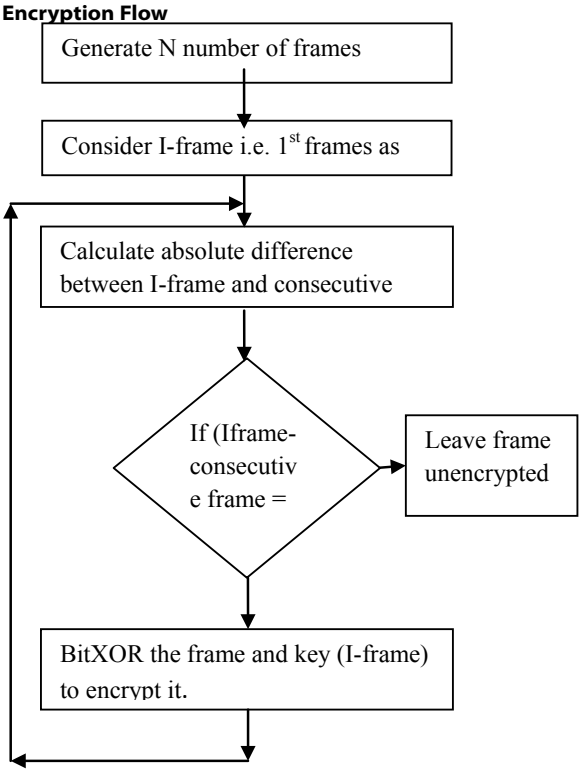
M Abomhara et al (2010) proposed the comparative study and a description and comparison between encryption methods and representative video algorithms were showed. With not only respect to their encryption speed but also their security level and stream size. There is a trade-offs when applying different encryption algorithms to MPEG video stream and its choice rely on the applications.

PROPOSED WORK

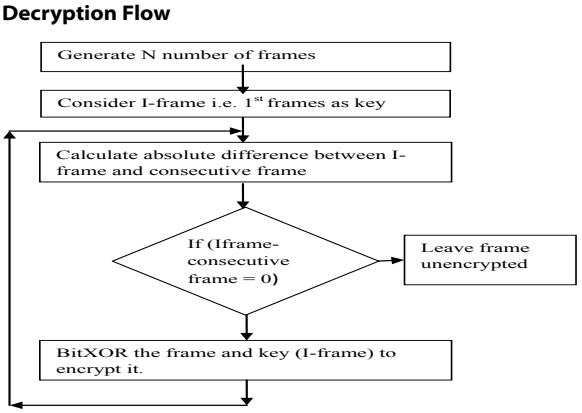
The main objective behind this research is to develop an algorithm

which encrypts the data comparatively faster than the existing video encryption algorithm and remove the need of sharing the key for decryption process. In this paper we have proposed a new scheme for video encryption which based on encryption of P-frame and B-Frame. Here we have encrypted only the motion vectors or frames containing motion in the video. In this method, we collect all the video frames and then take first frame or I-Frame as key and select consecutive frames one by one to calculate absolute difference for encryption and decryption process. After applying the encryption algorithm we combine all frame, make video which is in encrypted form. Let V be a video sequence consisting of m frames denoted by $I_1, I_2 \ldots I_m$. Furthermore, we assume the first frame (I_1) as key. In this system video stream assumes as a collection of still images. First frame is not encrypted as it is still I-Frame. Select second frame and calculate the absolute difference between the second frame and I-Frame. If the absolute difference occurs to be 0(zero), shows there is no motion in the frame and it is left unencrypted. However, if the difference is not zero, perform the bitxor operation between the key (I-Frame) and the frame. We now have the final encrypted image. Afetr encrypting all the images, reconstruct the encrypted video from the encrypted images, Now we can transfer the video through secure channel but we do not have to share the key, as it will be the first I-Frame of video during decryption. At the receiver side reverse process is applied.

Encryption Flow



Decryption Flow



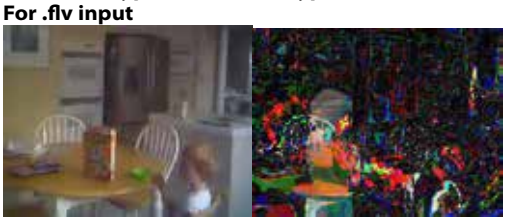
EXPERIMENTAL RESULT

This section of the paper contains the result analysis of the proposed encryption scheme. The formation algorithm has been successfully implemented in 4 different videos of different formats. Several simulation results are provided to show the performance of the algorithms for video encryption.

For .mp4 input

Before Encryption After Encryption

For .flv input

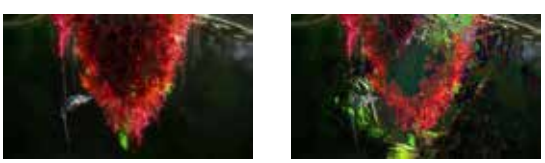


Before Encryption After Encryption

For .avi format

Before Encryption After Encryption

For .wmv input



Before Encryption After Encryption

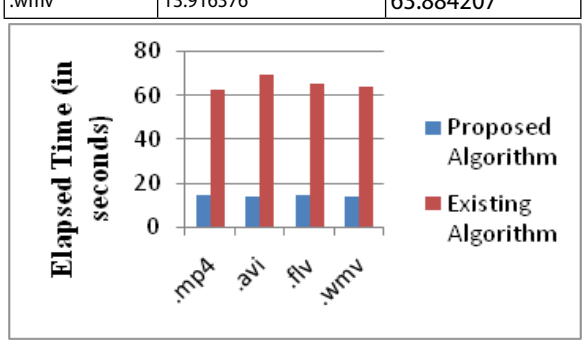
RESULT ANALYSIS

The analysis here proves that the proposed algorithm is faster than the pre existing algorithms.

Elapsed Time Analysis

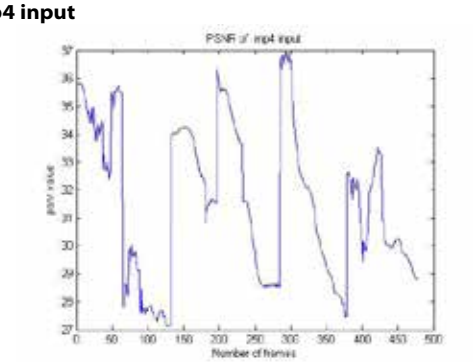
TABLE I. ELAPSED TIME COMPARISON

FORMATS	ELAPSED TIME (Seconds)	
	Proposed Algorithm	Existing Algorithm
.mp4	14.350064	62.922521
.avi	13.920573	69.814672
.flv	14.142308	65.683695
.wmv	13.916376	63.884207

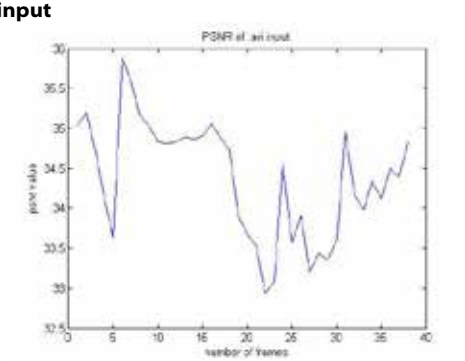


PSNR Analysis

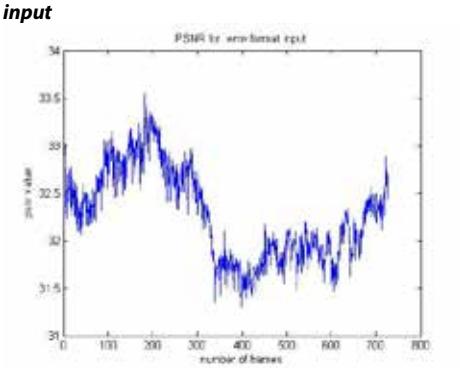
.mp4 input



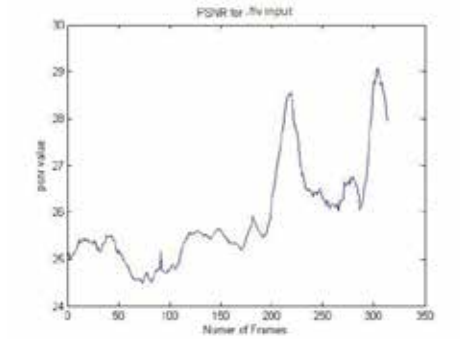
.avi input



.wmv input



.flv input



CONCLUSION

The analysis of the result proves that the proposed algorithm is capable of encrypting the video at faster rate, without anything to worry about the key. It also have an advantage that it will take less encoding space as only the selected part is encoded. The data loss is very less in selective type of algorithm in comparison to other naïve or layered algorithms used for encryption, as most of the part of the video remains unencrypted and only compressed. The PSNR values wherever are less than 30 are actually because of the type of compression technique used for the video and it varies with the different formats. For further research it is proposed that this approach can be made more complex and also we can use different keys for encrypting the different frames of the video as we are using the single key. Further we will extend the work by making improvements with above changes to increase the complexity and security of the work.

REFERENCES

[1] MPEG Technology Group, \http://www.chiariglione.org/mpeg/," (Accessed on March 2, 2009) | [2] Ostermann, J., Bormans, J., List, P., Marpe, D., Narroschke, M., Pereira, F., Stockhammer, T., Wedi, T. "Video coding with H.264/AVC: tools, performance, and complexity. IEEE circuits and system magazine , Vol 4,issue 1 , pp. 7-28, 2004 | [3] L. Tang, For encrypting and decrypting MPEG video data efficiently," in Proceedings of The Fourth ACM International Multimedia Conference (ACM Multimedia'96), (Bosten, MA), pp. 219{230, November 1996. | [4] B. Bhargava and C. Shi, "An Efficient MPEG Video Encryption Algorithm", IEEE Proceedings of the 17th Symposium on Reliable Distributed Systems, 1998, Pages 381 – 386. | [5] T.B. Maples and G.A. Spanos, "Performance study of selective encryption scheme for the security of networked real-time video," in Proceedings of the 4th International Conference on Computer and Communications, Las Vegas, NV, 1995 | [6] G.A. Spanos and T.B. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," in Conference on Computers and Communications, 1996, pp. 72-78 | [7] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," Proceedings of the 6th International Multimedia Conference, Bristol, UK, September 12-16, 1998. | [8] C. Griwotz, \ Video protection by partial content corruption," in Proceedings of Multimedia and Security Workshop at the 6th ACM International Multimedia Conference, (Bristol, England), pp. 37{39, 1998. | [9] C. Griwotz, O. Merkel, J. Dittmann, and R. Steinmetz, \Protecting vod the easier way," in Proceedings of Multimedia and Security Workshop at the 6th ACM International Multimedia Conference, (Bristol, England), pp. 21{28, 1998. | [10] M. Abomhara, Omar Zakaria, Othman O. Khalifa, "An overview of video encryption techniques," in International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201. | |