partial MPEG-4 video encryption schema using RC6 algorithm

Dr. Abdul-Wahab Sami Ibrahim and Rafah Samih Shaker

Abstract

Securing video has increased in the past few years, security and privacy issues of video data have become a very important concern, in this paper introduce secure selective encryption applying on MPEG-4 video file based on the file format of the MPEG-4 using RC6 encryption algorithm and XOR operation,the method implement in two stage first analysis and reaching to the data frames, second applying the encryption method on (I and P) frames only, the method make all blocks in all selected frames linked with each other using one public key,the decryption begin from the last block in the last frame to the first block of the first frame using one privet key,each block encrypted by RC6 with his own key, the different keys generate by RC4 to all blocks and avoid reapeted keys, the experimental result shows that the proposed method are secure and don't increased the size of the file after encrypt it.

المستخلص

أمنية الفيديو ازدادت في السنوات القليلة الماضية, أصبحت قضايا الامنية والخصوصية لبيانات الفيديو مصدر قلق بالغ الاهمية , في هذه الورقة تم تقديم تشفير جزئي آمن على ملف من نوع MPEG-4 بالاستناد على تنسيق الملف وبأستخدام خوارزمية التشفير RC6 وعملية XOR , الطريقة نفذت بمرحلتين , المرحلة الاولى تضمنت عملية تحليل الفيديو والوصول الى بيانات الفريم, المرحلة الثانية تضمنت تطبيق طريقة التشفير على الفريمات التي من نوع (I , P) فقط , الطريقة المقترحة تجعل جميع الكتل في كل الفريمات مرتبطة مع بعضها بأستخدام مفتاح تشفير عام , اما طريقة فك الشفرة فأنها تبدأ بفتح شفرة الملف من أخر بلوك في أخر فريم الى ان تصل الى البلوك الاول في الفريم الاول بأستخدام مفتاح سري, كل بلوك يتم تشفيرة بخوارزمية RC6 بأستخدام مفتاح مختلف, المفاتيح المختلفة للبلوكات تتولد عن طريق RC4 لجميع الكتل مع تجنب المفاتيح المتكررة, وقد بينت النتائج ان الطريقة المقترحة أمنة ولاتزيد الحجم بعد التشفير .

Introduction

The uses of video become wide speared and important part in the daily life, especially after the increasing use of some application like (Viber, Skype, Tango,…. Etc..) and the visual communication between peoples, there are some other application need to protect like telemedicine where the health system suffering today from the unsecure of patient information so urgently needing to protect that specialized information. The video conferencing need to speed and secure during transmission where the visual communication in the conferencing is a new and important technology used in wide speared in the world like video conference between two companies to discuss commercial things about the products of the next three years [1]. Other protection necessary in the public life is to protect the videos recorded on surveillance cameras, these cameras contain special information about peoples in the public places so need to protect the information in these films from unauthorized persons , also need the protection of VOD (video on demand), DVDs , video conference learning, military and commercial application and so on[2].

Selective encryption

The traditional approach of encryption to encode and make access control to the video is not suitable because the large size of the video bit stream, this traditional approach, processed the media stream as text data with consideration that all bits in the plaintext have equally important , This schema called fully layered[3],selective encryption (SE) or partial encryption this schema applied on a subset of the bit stream, the aim of this scheme is to reduce the amount of encrypted data with keeping the required level of security [4].

The process of identifying the protected part depends on the application , aim of SE is to make the protected part small as possible , so small data is encrypted and the attacker can't understand the content ,The SE keep the file format unchanged and provide fast encryption so it is Appropriate to video encryption[5].

MPEG-4 Overview

MPEG-4 is an ISO / IEC standard developed by MPEG (motion picture experts group) theses committees also developed the famous standard (MPEG1, MPEG2,… etc..), MPEG-4 is not like those standards is providing the new concept due is depend on objects ,MPEG-4 have interactive visual and audio objects[6].

Can consider that three types of frames in MPEG-4:-

- I-VOP(intra_video object plane):- refers to intra coded frame, it coded without any depend on other P-VOP and B-VOP frames, it searches on redundancy in the same frame only mean exploiting only the spatial redundancy , it is coded as a single frame, the encoded schema is similar to JPEG compression because it is self –references, I-VOP is always in the beginning of the video stream also called "key frame".
- P-VOP predictive coded:- its code depends on previous I-VOP or previous P-VOP, the P-VOP provide high compression compare to the I-VOP, may be caused error to propagate.
- B-VOP refer to bi-directional coded, its code depends on previous and next P-VOP or I-VOP, the nearest P-VOP and I-VOP frame from it. It is similar to P-VOP frame, it provides higher compression than P-VOP frame and not causes any error propagate because it is not used as a reference frame to any other form [7].

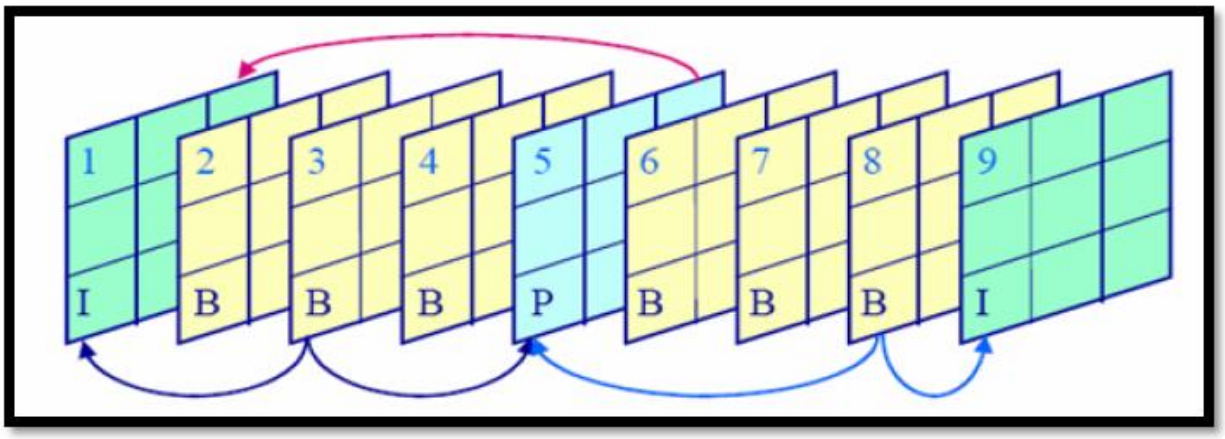


Figure (1) The three types of frames[7]

MPEG-4 media file format

MPEG-4 is the widely used video because the high quality and effective compression, the data packed in boxes, MPEG-4 consist of several boxes, each box have typed and size, those boxes can understand as data object blocks,the box which contains another box called the container box[8].

Basic concepts[8]:

- Track: represent a collection of samples (frames), may be video or audio sequence, video track represent groups of consecutive video frame, the audio track is the period of continuous compressed audio.
- Chunk: composed of several samples(frames), each chunk has different size, different location and different number of samples (frames), also each sample (frame) have different size and different location.
- Video track contains information about video sample (video frames), audio track contains information about audio sample (audio frames).
- Stsc : sample-to-chunk box, it's shows relationship between chunk and samples , samples grouped into chunks. Chunks can be different sizes, This table can be used to find the chunk map.
- Stco: The chunk offset table, gives the location of each chunk in the file.
- Stsz: sample sizes table, this box shows the size of each sample in bytes.
- Each track(video or audio) have stsz,stco and stsz.

RC6 overview

Block cipher which improvement to RC5 design to meet the requirements of security and performance ,RC6 introduced to NIST as new advanced encryption standard (AES), one of RC6 feature its use four register each one save 32 bit , RC6 is specified as RC6-w/r/b, where w is the word size ,r is number of round and b denoted to key length in bytes.

RC6-w/r/b Word size is w(4 bytes) ,Number of rounds is r (20 rounds as standard) and length of the key is b bytes (16, 24, 32 bytes) as standard. [9]

The Features of rc6 algorithm[10] Simplicity ,Provide high level of security ,Very fast ,Small memory requirement, Attractive, Flexible and Sufficient strength.

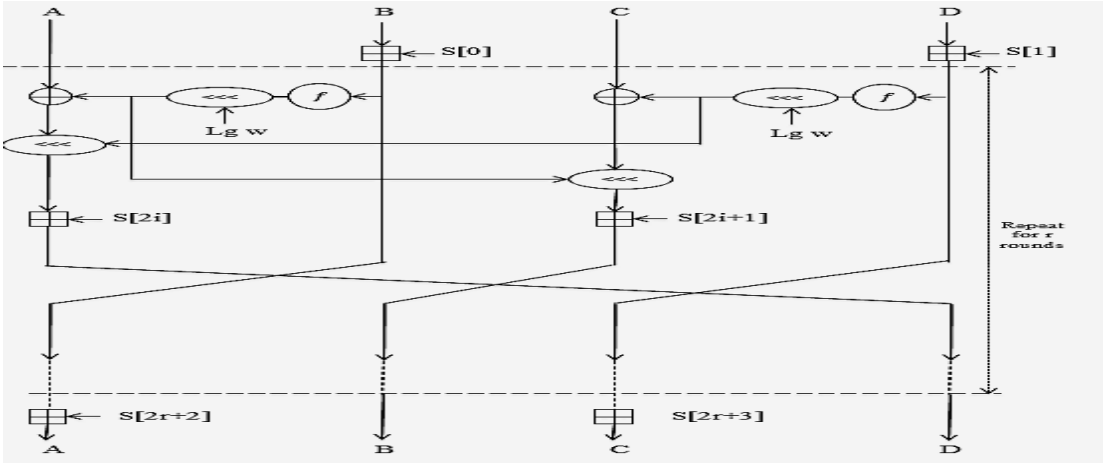


Figure (2) encryption RC6[9]

RC6 encryption algorithm uses 44 sub keys,each one have size of 4 byte,numbered from S0 to S43 and each round used 2 sub key [11].

User enter the key of b bytes,those bytes go to array L , this array have size c,

Thus first byte saved in L[0] and the last byte is stored in L[c-1], w-bit words are generated for the additive keys 2r + 4, and those are saved in array S[0,…,2r+3].

[10].the key generate algorithm as follows[9]:-

Key schedule for RC6-w/r/b
Input: User-supplied b byte key preloaded into the c-word
array L[0,….., c - 1]
Number r of rounds
Output: w-bit round keys S[0; : : : ; 2r + 3]
Procedure: S[0] = Pw
for i = 1 to 2r + 3 do
S[i] = S[i - 1] + Qw
A = B = i = j = 0
v = 3× max {c, 2r + 4}
for s = 1 to v do
{
A = S[i] = (S[i] + A + B)<<<3
B = L[j] = (L[j] + A + B)<<<(A + B)
i = (i + 1)mod(2r+4)
j = (j + 1)mod c
}

RC4 overview

RC4 is a stream cipher , based on random permutation, have variable key size from (1 to 256) used to make initialized state vector with element s[0] to s[255].

```
/* Initialization */
For i = 0 to 255 do
S[i] = i;
T[i] = K [i mod key length]

/* Initial Permutation of S */
j = 0;
For i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j])

/* Stream Generation */
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256
Swap (S[i], S[j])
t = (S[i] + S[j]) mod 256
k = S[t];
```

In encryption and decryption process, implement XOR operation between the value want to encrypt or decrypt and the Key.

The proposed encryption schema

The encryption system work in two stages, first stage analysis MPEG-4 and extract the data from it by using (stsz,stsc and stco) and generate algorithm combined them to make a framework make reaching to the data easy and directly, The second stage applying the substitution cipher on the data extracted,The encryption system encrypted (I and P)frames only.

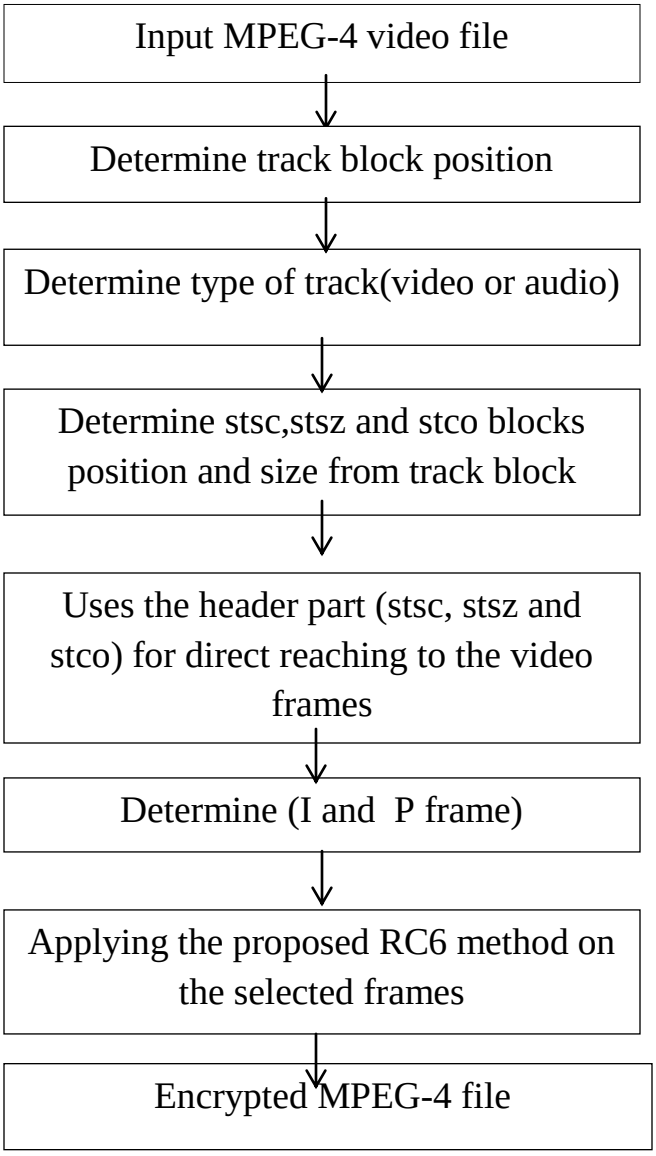
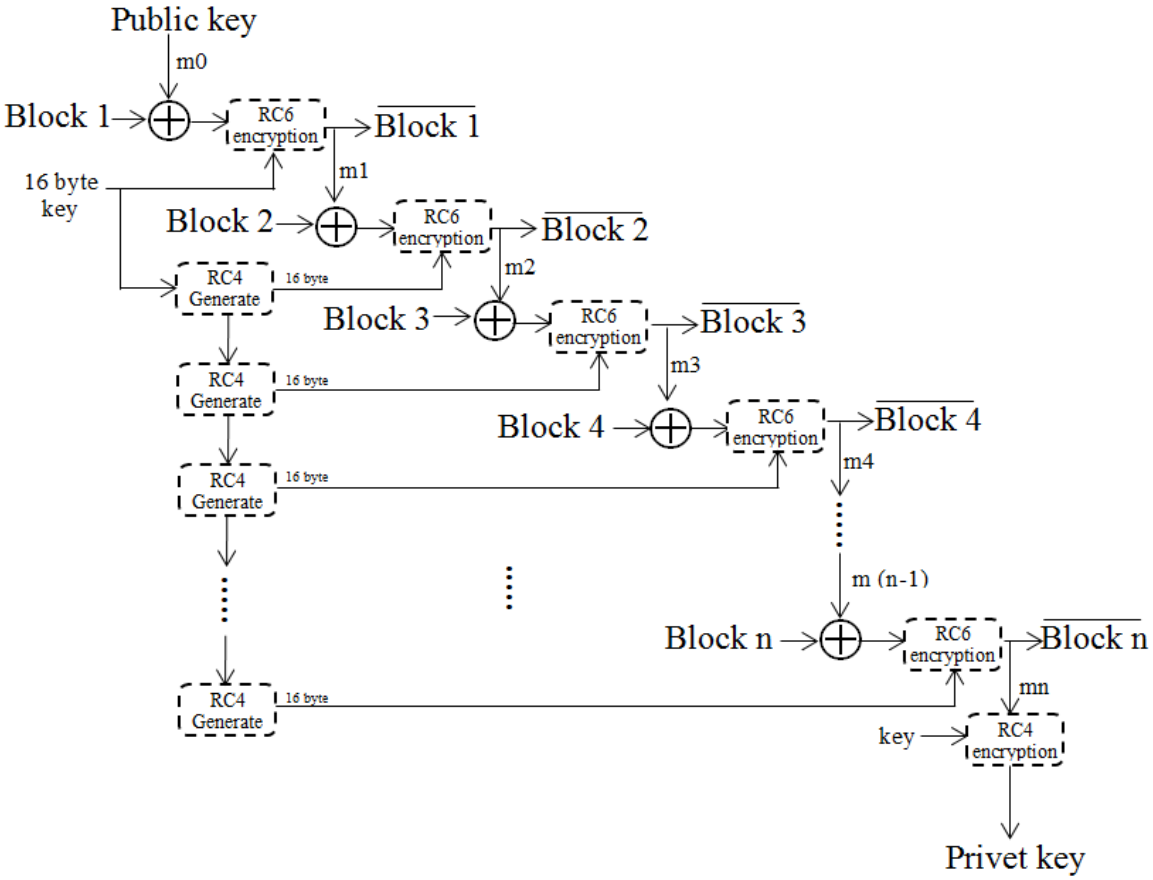


Figure (3) the general structure for the video encryption system

The encryption method shown below:-



Figure(4) Block diagram of The encryption method

As shown in figure(4) the proposed method based on block cipher,all blocks in all frames connected with others from the first block in the first frame to the last block in the last frame (for I and P frames only) used one public key and one privet key, each block encrypted by RC6 encryption algorithm, RC6 encrypted the block using two different input each one have size of (16 byte)the first input is generate by RC4,the second input comes from the block after make XOR operation on it.

For example : propose the sender is Alice and the receiver is Bob, supposed Alice want to send message "M" to Bob to do this in the proposed method, Alice will select the blocks want to encrypt it and choose key used as public key, know Alice encrypted "M" , Alice encrypted "M" by generate the sequence keys (m1,m2,m3,……mn).

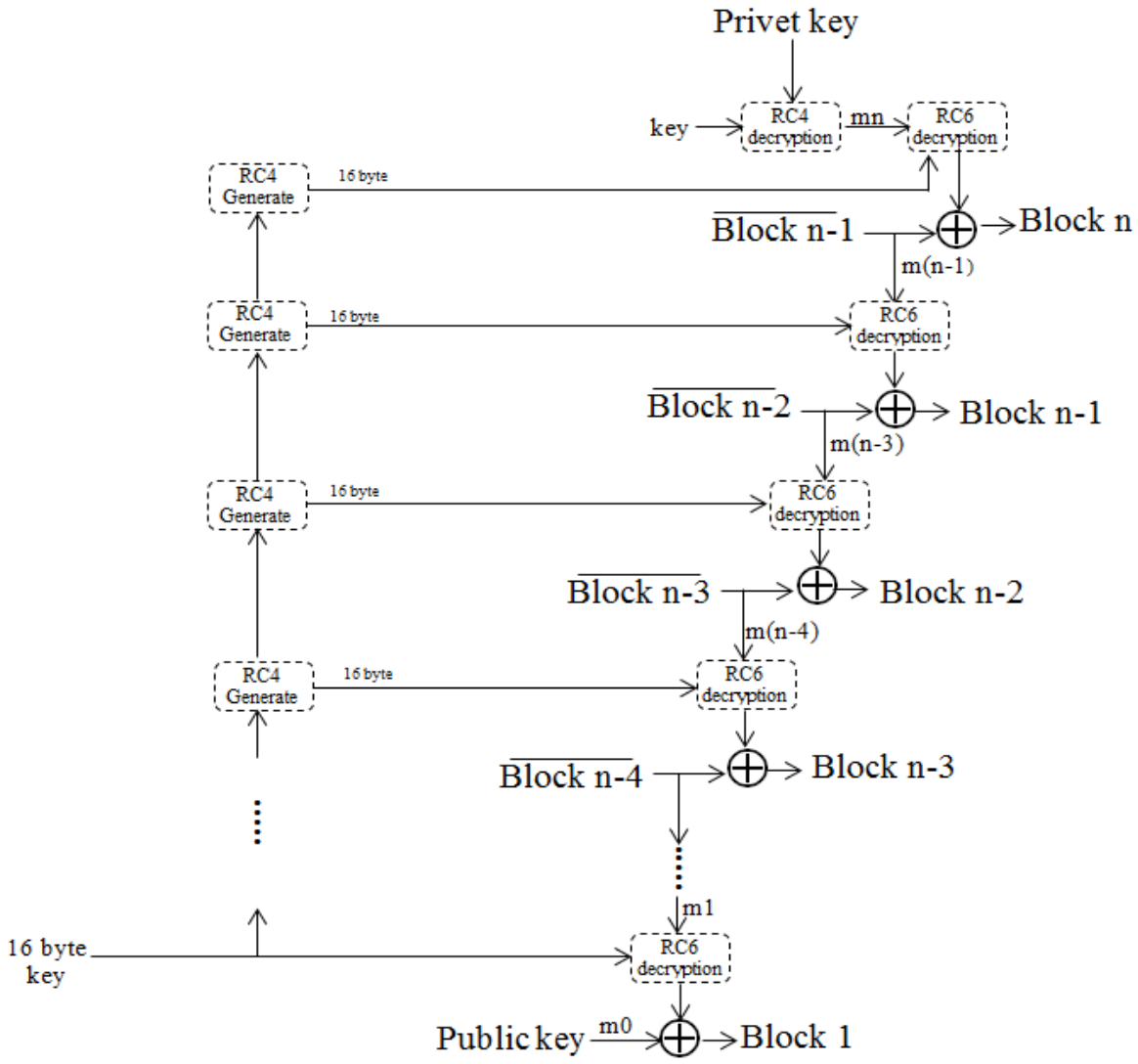
C1=encryption RC6 $_{key}$ (P1⊕m1)

C2=encryption RC6 $_{key}$ (P2⊕m2)

C3=encryption RC6 $_{key}$ (P3⊕m3)

Each input block have size is 16 byte, the encrypted block also 16 byte and the keys is also 16 byte =128 bit.

The decryption method begin to decrypt from the last block to the first one , as shown in figure (5)



Figure(5)Block diagram of The decryption method

Experimental Results

To evaluate the performance of the proposed system, different MPEG-4 videos were tasted, each video was different in size, display time, frame per seconds and bit rate, the characteristics of each video are shown in table:

Table (1)characteristics of the tested video

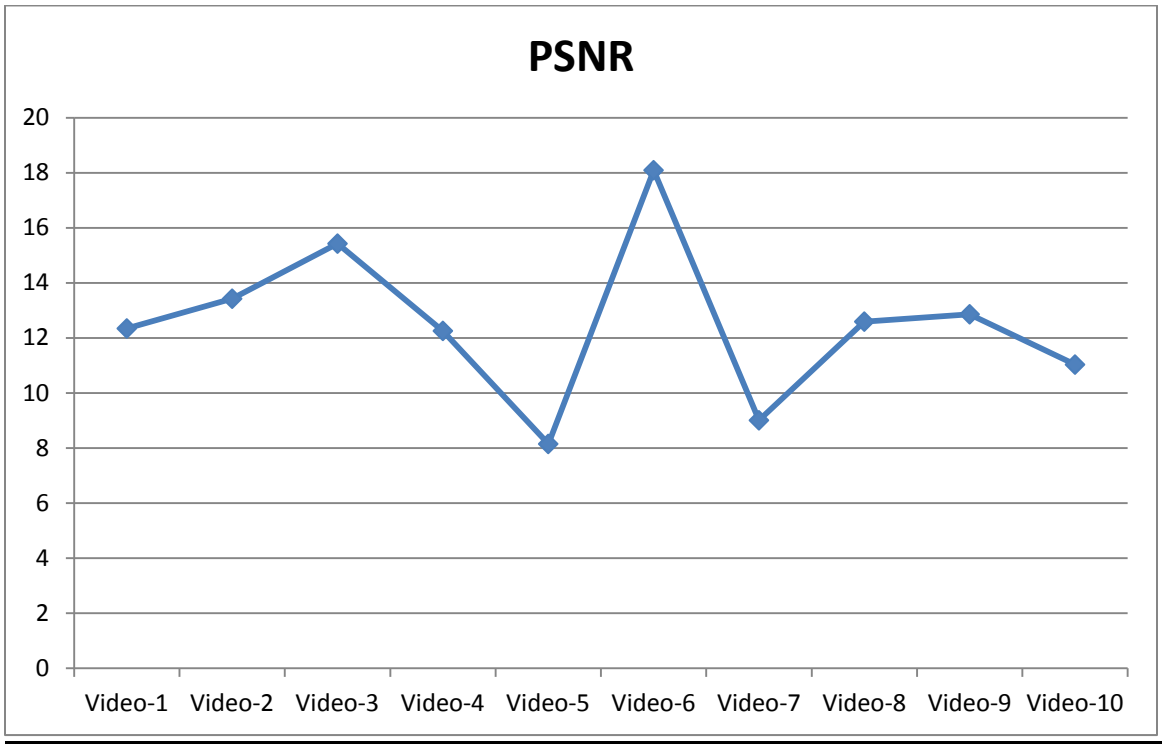
File name	*File Size*	*Length*	*Frames/ Sec*	*Bitrate (kbps)*	*Frame height*	*Frame width*	*Number of frames*
Video-1	*0.98MB*	*00:00:10*	*24*	*824*	*480*	*640*	*241*
Video-2	*16.7 MB*	*00:05:22*	*18*	*434*	*480*	*856*	*5804*
Video-3	*1.21MB*	*00:00:36*	*30*	*281*	*288*	*352*	*1080*
Video-4	*1.83 MB*	*00:00:09*	*30*	*1534*	*288*	*352*	*296*
Video-5	*23.3 MB*	*00:31:26*	*18*	*102*	*240*	*472*	*33950*
Video-6	*17.3MB*	*00:06:30*	*18*	*372*	*240*	*432*	*7032*
Video-7	*75.2 KB*	*00:00:01*	*29*	*604*	*240*	*432*	*22*
Video-8	*591 KB*	*00:00:15*	*12*	*320*	*240*	*360*	*180*
Video-9	*289 KB*	*00:00:04*	*15*	*589*	*240*	*320*	*64*
Video-10	*14.5 MB*	*00:11:12*	*12*	*180*	*120*	*160*	*8072*

1-Result of quality analysis

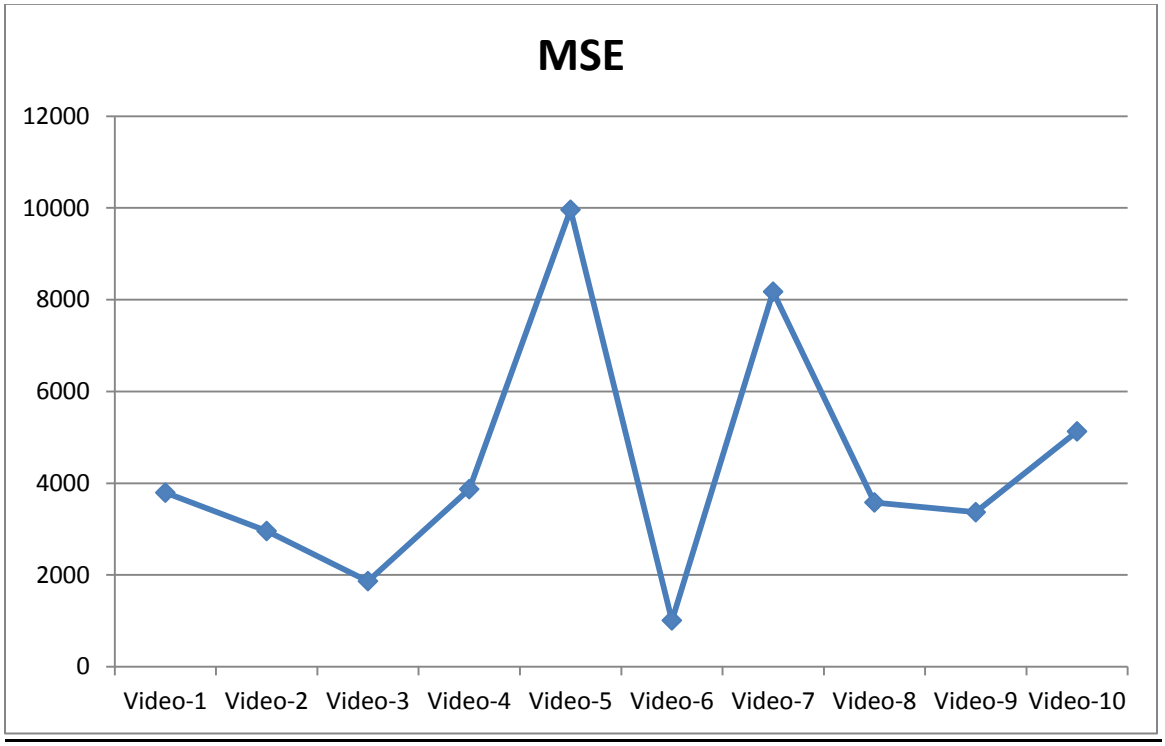
To evaluate the quality of this work, used the objective fidelity criteria measurements (PSNR(peak signal to noise ratio), MSE(mean square error) and SSIM(structure similarity)),PSNR, MSE and SSIM are tested between the original video and the encrypted video shows in figures(6,7,8).

Table (2) objective fidelity criteria(PSNR,mse,SSIM) for the tested videos

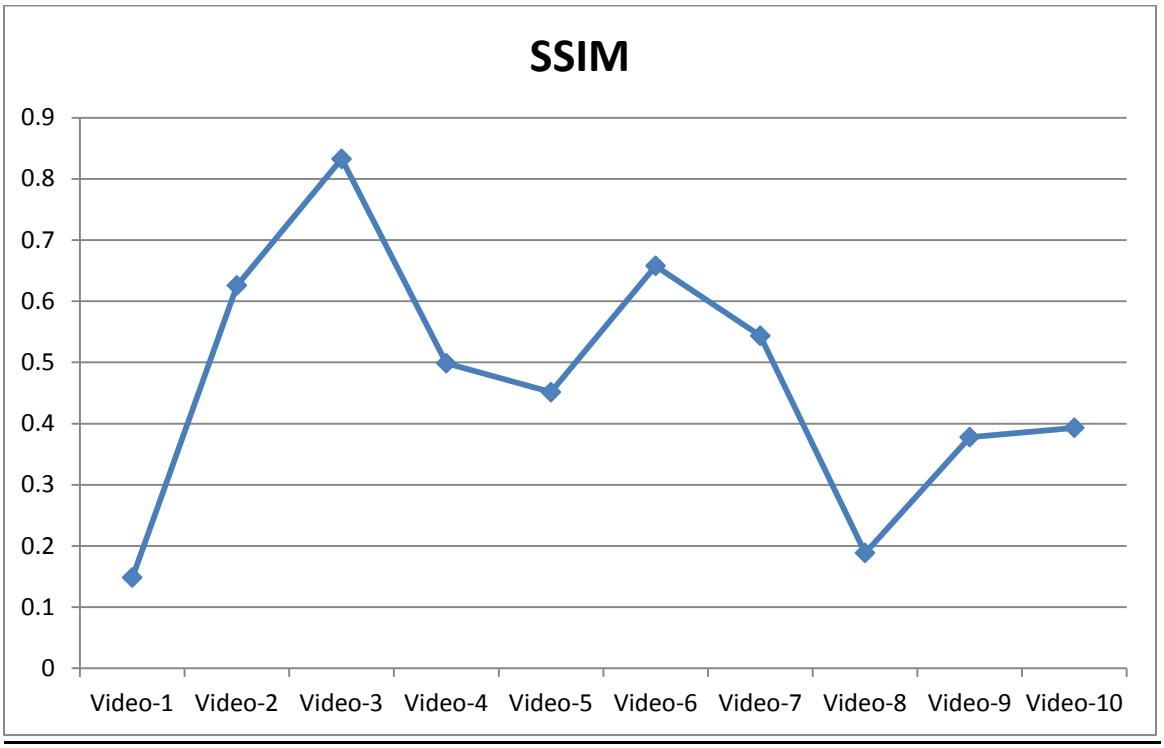
File name	*PSNR*	*MSE*	*SSIM*
Video-1	*12.34199*	*3793.26147*	*0.1484*
Video-2	*13.42348*	*2956.9707*	*0.62579*
Video-3	*15.42454*	*1864.83325*	*0.83264*
Video-4	*12.25449*	*3869.25366*	*0.49864*
Video-5	*8.14771*	*9958.44043*	*0.45129*
Video-6	*18.09057*	*1008.58154*	*0.65786*
Video-7	*9.00652*	*8173.43408*	*0.54341*
Video-8	*12.59102*	*3580.52441*	*0.18858*
Video-9	*12.85767*	*3367.47437*	*0.37781*
Video-10	*11.03075*	*5128.26367*	*0.39318*



Figure(6) Result of PSNR

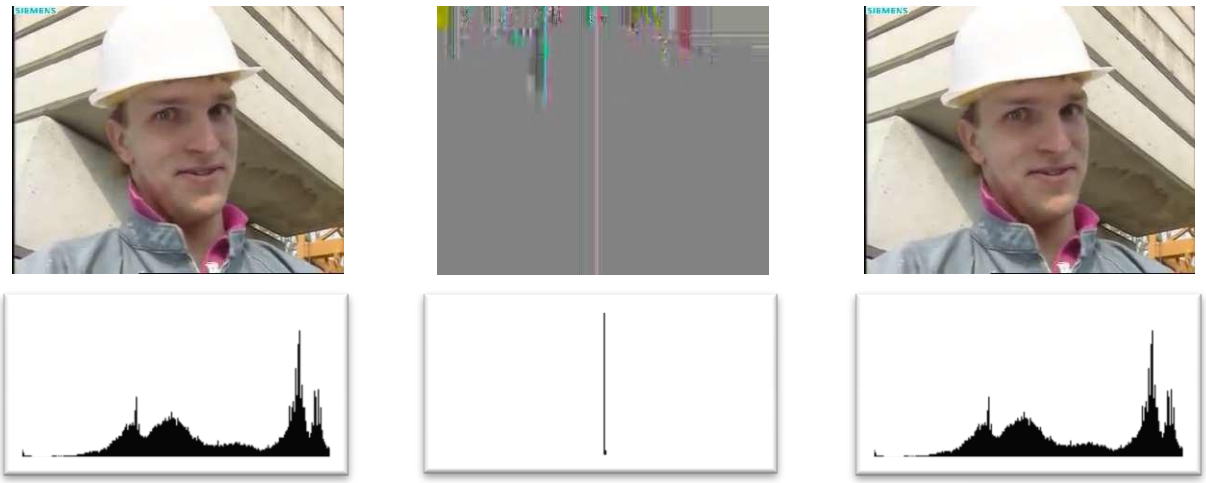


Figure(7) Result of MSE

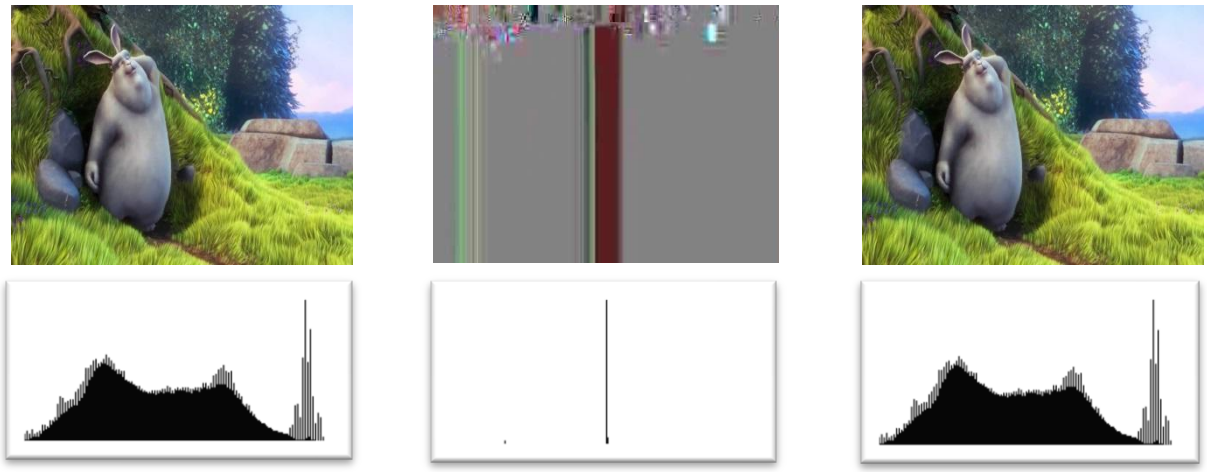


Figure(8) Result of SSIM

The results of PSNR(peak signal to noise ratio) ranging between(8.14771 and 18.09057), the MSE(mean square error) ranging between(9958.44043 and 1008.58154) and the SSIM(structure similarity) ranging between(0.14840 and 0.83264) from this result mean good destroyed of the visual data.



a) Original frame b)Encryption frame c) Decrypted video



a) Original frame b)Encryption frame c) Decrypted video

Figure (9) shows some of the original and encrypted of tested video and the histogram of each one

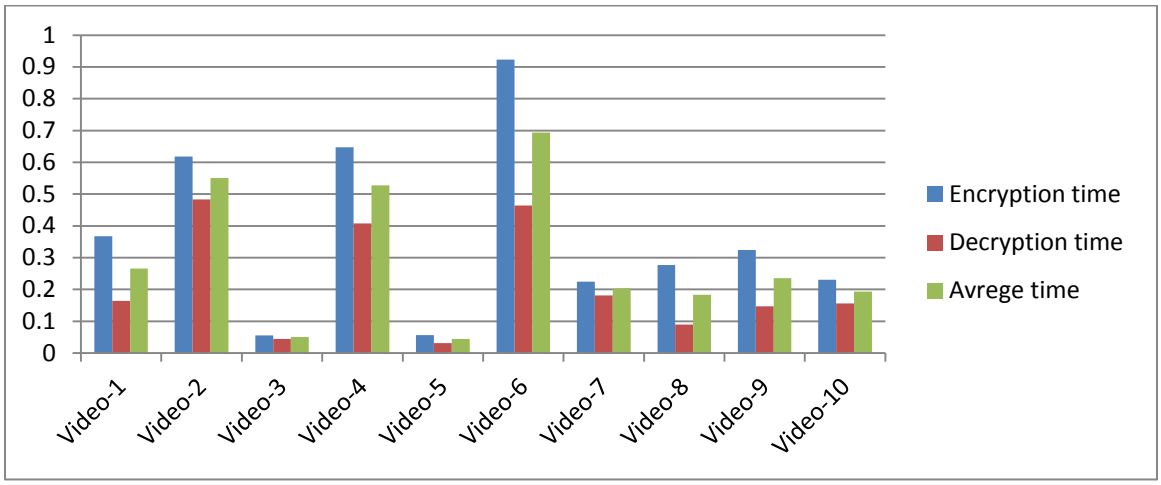
2-Result of execution time

The execution time of encryption shown in the table (2):-

Table(2)execution Time

File name	*Encryption time of one frame in sec*	*Decryption time of one frame in sec*	*Averege Time*
Video-1	*0.367*	*0.164*	*0.2655*
Video-2	*0.618*	*0.483*	*0.5505*
Video-3	*0.056*	*0.044*	*0.05*
Video-4	*0.647*	*0.408*	*0.5275*
Video-5	*0.057*	*0.0314*	*0.0442*
Video-6	*0.923*	*0.464*	*0.6935*
Video-7	*0.225*	*0.181*	*0.203*
Video-8	*0.277*	*0.090*	*0.1835*
Video-9	*0.324*	*0.147*	*0.2355*
Video-10	*0.231*	*0.156*	*0.1935*

From the result of execution time can notify that the time of the frame increased when the frame size, number of frames in Sec and bitrate are increased.



Figure(10) Reesults of the execution time

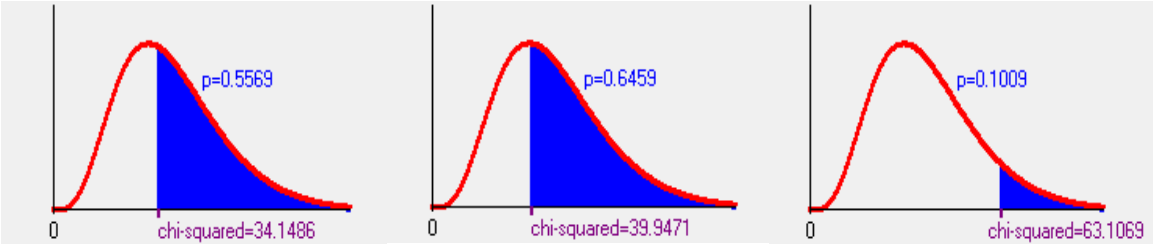
3-Result of security analysis

To measure the security of the proposed schema , CRYPT-X used as a testing tool to detect the deviation of binary sequence for randomness, some tested was preformed ,to experiment the hypothesis that say the plaintext could produce a random ciphertext block the following tests was preformed on block size (128)bit:-

A. Frequency test: Test the distribution of the number of ones in the block, the frequency test applying on different number of blocks , the result of the frequency test shows in table(3) and figure(10).

Table(3)frequency test results

Number of blocks	*Number of ones*	*Expected ones(mean)*	*Proportion of ones*	*Significance probability (p)*	*Satisfy*
10000	*2752*	*10000*	*1*	*0.5569*	*Yes*
100000	*3136*	*100001*	*1.0002*	*0.6459*	*Yes*
1000000	*3707*	*999998*	*0.9996*	*0.1009*	*Yes*



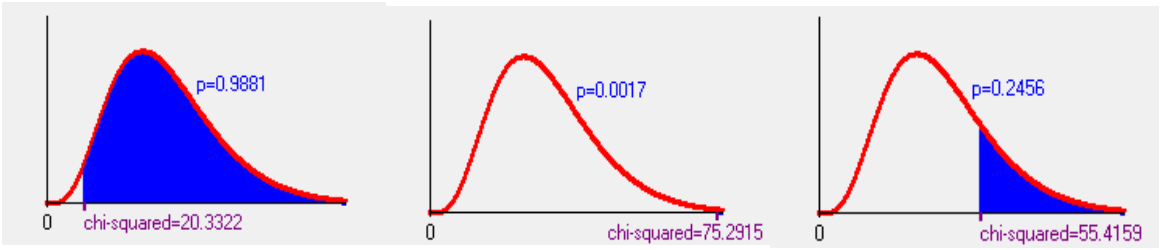
Figure(11)frequency test

- All the sequences satisfy the frequency test because the Significance probability (p) is all greater than (0.001).
- It indicates that there is an equal Proportion of 1s and 0s in each stream, therefore the sequence are considered balanced and randomness.

B. Binary Derivative test: show if the distribution of the number of bit changes in each block,the Binary test applying on different number of blocks , the result of this test shows in table(4) and figure(11).

Table(4) results of Binary Derivative test

Number of blocks	*Number of ones*	*Expected ones(mean)*	*Proportion of ones*	*Significance probability (p)*	*Satisfy*
10000	*2793*	*10002*	*1*	*0.9881*	*Yes*
100000	*3303*	*99998*	*1.0001*	*0.0017*	*Yes*
1000000	*3520*	*999998*	*0.9999*	*0.2456*	*Yes*



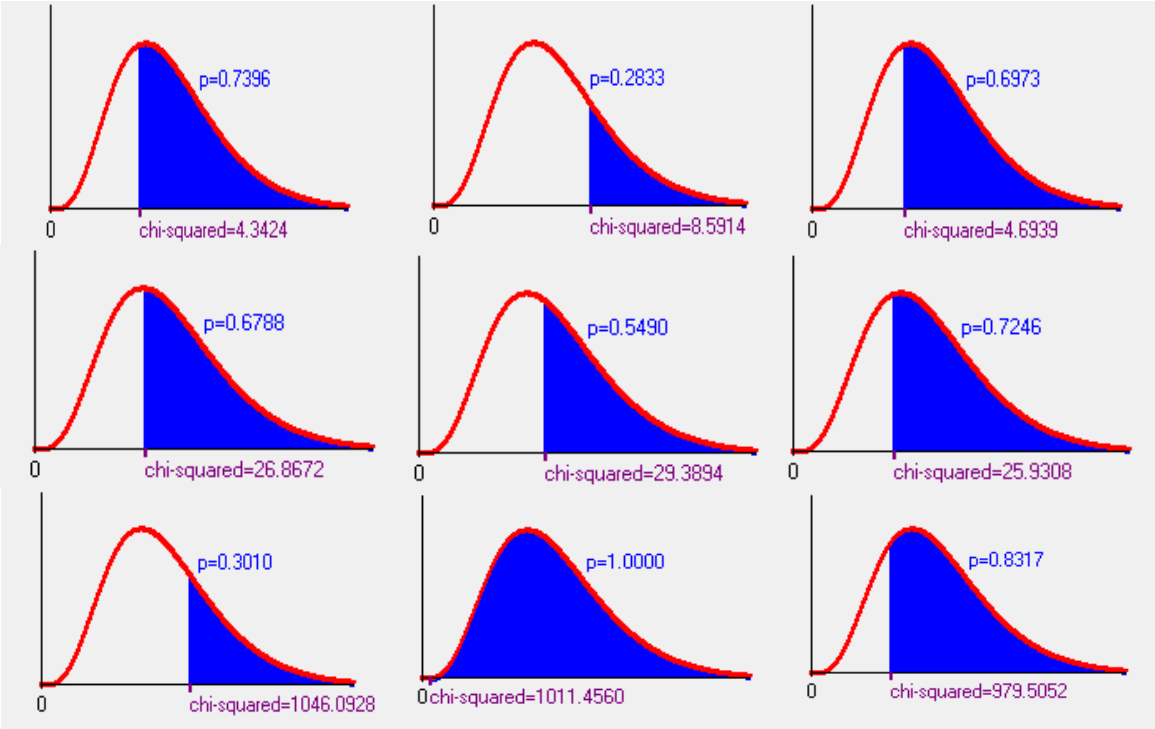
Figure(12) results of Binary Derivative test

- All the sequences satisfy the Binary Derivative test because the Significance probability (p) is all greater than (0.001).
- It indicates that the distribution of the numbers of bits changes in each block therefore the sequences is considered randomnes.

C. Subblock test: choose subblock from the plaintext and ciphertext block then determine these different position subblock are dependent or independent , preform the subblock test on number of subblock (3,10,17), the subblock test applying on different number of blocks , the result of this test shows in table(5,6) and in figures(13,14).

Table (5) result of Subblock test(subblock size=3)

Number of blocks	*Subblock size*	*Chi-squared value*	*Significance probability (p)*	*Satisfy*
10000	*3*	*4.3424*	*0.7396*	*Yes*
100000	*3*	*8.5914*	*0.2833*	*Yes*
1000000	*3*	*4.6939*	*0.6973*	*Yes*
10000	*5*	*26.8672*	*0.6788*	*Yes*
100000	*5*	*29.3894*	*0.5490*	*Yes*
1000000	*5*	*25.9308*	*0.7246*	*Yes*
10000	*10*	*1046.0928*	*0.3010*	*Yes*
100000	*10*	*1011.4560*	*1.0000*	*Yes*
1000000	*10*	*979.5052*	*0.8317*	*Yes*



Figure(13) result of Subblock test(subblock size=3,5,10)

- the value of probability (p) in all number of blocks are graeter than(0.001), thus the sample satify the subblock test when the subblock is (3,5,10)
- sample satisfies the subblock test on the positions selected.

Conclusion

In this paper, we have proposed a computationally efficient,secure video encryption scheme. It uses RC6 for encryption of the(I and P)frames. The proposed scheme is fast, possesses good security, and don't increased the file size ,Partial video encryption techniques are used to significantly reduce the computational overhead associated with encryption while achieving an acceptable level of security. Experimental results from the encryption of the various test video demonstrate the effectiveness of the video encryption scheme.

References

[1] M. Abomhara, Omar Zakaria and et.al, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, (2010).

[2] Andreas Uhl and Andreas Pommer, "Image and Video Encryption From Digital Rights Management to Secured Personal Communication" ,Springer Science + Business Media, Inc., eBook ISBN: 0-387-23403-9 (2005).

[3] A Massoudi, F Lefebvre and et.al," Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Journal on Information Security , 2008:179290,doi:10.1155/2008/179290,(2008).

[4] Borok Furht ,Darko Kirovski , "multimedia security handbook",CRC press ,London,(2005).

[5] Tom Lookabaugh, "Selective Encryption, Information Theory and Compression", MSC.thesis, Computer Science Department, University of Colorado, (2004).

[6] Iain E. G. Richardson "H.264 and MPEG-4 VideoCompression Video Coding for Next-generation Multimedia", John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England ,(2003).

[7] B. Bhargava, C. Shi and S.-Y. Wang, "MPEG Video Encryption Algorithms", Multimedia Tools and Applications,Vol. 24, No. 1, pp. 57-79, 2004.

[8] INTERNATIONAL STANDARD ISO/IEC(14496-12), Information technology — "Coding of Audio-visual objects-ISO base media file format" Second edition, (2012)

[9] Man Young Rhee ," Internet Security Cryptographic Principles, Algorithms and Protocols" , John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,West Sussex PO19 8SQ, England,(2003).

[10] Ashwaq T. Hashim,et ,al.," A Proposed 512 bits RC6 Encryption Algorithm", IJCCCE, VOL.10, NO.1,(2010).

[11] Sheetal Charbathia and Sandeep Sharma," A Comparative Study of Rivest Cipher Algorithms", International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 17 pp. 1831-1838, (2014).