Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD)

Dr.AbdulMonem S. Rahma
Computer Science Department, University of Technology/Baghdad
Email:monemrahma@yahoo.com
Basima Z.Yacob
Science College, University of Zakho /Dhok

Received on: 28/9/2011 & Accepted on: 5/1/2012

ABSTRACT

In recent years, as digital video technologies have been broadly used in TV, communication and multimedia. Security and privacy issues of the transmitted data have become an important concern in multimedia technology.

Digital video stream is quite different from traditional textual data because inter-frame dependencies exist in digital video. Special digital video encryption algorithms are required because of their special characteristics, such as coding structure, large amount of data and real-time constraints.

This paper presents a real-time partial encryption to digital video technique based on Symmetric Dynamic Dual (SDD) keys algorithm which is fast enough to meet the real-time requirements with high level of security.

This approach uses dual key for encryption with variable (dynamic) block bits size, each block bits size (3 or 4 bits) are interpreted as an element of a finite field.. The first key is called control key determines the length of bits block (3 or 4 bits block) size to encrypt, and the second key is used for encryption by using a equation:

$Y = X \ast A + B$WhereX is bits block, AandB are the encryption keys.

The mathematical operations addition and multiplication in this equation are based on mathematical theory of Galois field $GF(2^n)$.

In this technique the I-frame (Intra-frame) of the digital video scene is extracted and decomposed the color picture into its three color channels:luma channel (Y) and two chrominance channels Cb and Cr,with note that the frames of digital video is in YCbCr color system, the SDD algorithm is applied to the Y channel.

The encryption algorithm achieves best timing results, and it provides high level of security by its great resistant against brute force attacks, because it uses dual key and dynamic block cipher, hence it will be very difficult to guess the key. To decrypt the ciphertext with 128 bits, the attacker needs 8.86569157e+188 of possibilities of keys as minimum and 7.91569097e+253 as maximum.

Keywords: Dynamic block encryption, Dual keys for encryption , Encryption digital video, partial encryption for Digital video, Digital video encryption in real time.

https://doi.org/10.30684/etj.30.5.2
2412-0758/University of Technology-Iraq, Baghdad, Iraq

التشفير الجزئي في الزمن الحقيقي للفديو الرقمي باستخدام خوارزميت SDD

الخلاصة

في السنوات الأخيرة ، استخدمت تقنيات الفيديو الرقمية على نطاق واسع في مجال الاتصالات و التلفزيون و الوسائط المتعددة . اصبحت قضايا امن وخصوصية البيانات المنقولة شاغلاً هاماً في مجال تكنولوجيا الوسائط المتعددة.

ان سيل الفيديو الرقمي يختلف تماماً عن البيانات النصية التقليدية. يتطلب تشفير الفيديو الرقمي خوارزميات خاصة و استثنائية بسبب خصائصه المميزة ، مثل هيكل الترميز ، واحتوائه على كميات كبيرة من البيانات و بالاضافة الى القيود التي يفرضها الزمن الحقيقي.

هذا البحث يقدم تقنية التشفير الجزئي في الزمن الحقيقي للفيديو الرقمي اعتماداً على خوارزمية المفاتيح الثنائية الديناميكية المتناظرة (SDD) التي لها السرعة الكافية لتلبية متطلبات الزمن الحقيقي مع امتلاكها مستوى عالٍ من الامن.

هذا الاسلوب يستخدم مفتاحين ثنائيين للتشفير و كذلك كتلة من البت ذو حجم متغير (ديناميكي) ، و يتم تغيير حجم كتلة البت (3 او 4 بت) كعنصر ينتمي الى نطاق الحقول المنتهية. يسمى المفتاح الاول مفتاح التحكم يحدد حجم الكتلة المراد تشفيرها بالبت (3 او 4 بت) ، اما المفتاح الثاني يستخدم في التشفير و ذلك باستخدام المعادلة التالية :

حيث ان X يمثل الكتلة بالبت و Aو B يمثلان مفاتيح التشفير.

و تستند العمليات الحسابية الجمع و الضرب في هذه المعادلة على نظرية جالويس الرياضية للحقول المنتهية $GF(2^n)$.

في هذه التقنية يتم استخراج الصورة I-frame من مشهد الفيديو الرقمي و تحليلها الى قنواتها اللونية الثلاثة YCbCr ، ثم يتم تطبيق الخوارزمية ال SDD على القناة Y . ان خوارزمية التشفير تحقق أفضل نتائج الوقت ، و أنها توفر مستوى عالٍ من الامان لمقاومتها الكبيرة للهجمات ، وذلك لاستخدامها المفتاح الثنائي و كذلك الكتل الديناميكية للتشفير ، وبذلك سيكون من الصعب للغاية تخمين المفتاح . فمثلاً لفك رسالة مشفرة متكونة من 128 بت فالمهاجم يحتاج الى 8.86569157e+188 من احتمالات المفاتيح كحد ادنى و 7.91569097e+253 كحد أقصى .

INTRODUCTION

Multimedia applications such as Video on-Demand, video broadcast, multimedia mail and video-conferencing must be provided with secure transmission. Secure video transmission is a method in which video can be sent to a receiver with the assurance that any unapproved eavesdroppers along the way will not be able to get any information from video i.e. it is desirable that only those who have paid for the services can view their videos or movies. The high amount of redundancy in the video gives an attacker more clues to reconstruct the original video. Normal data, such as program code or text, has much less redundancy in its structure. These factors make providing secure digital video a challenge. Various encryption algorithms have been proposed in recent years as possible solutions for the protection of the video data. Large volume of the video data makes the encryption difficult using traditional encryption algorithms. Often, we need the encryption to be done in real-time [1]

The naive approach for video encryption is to treat video data as text and encrypt it using standard encryption algorithms like AES (Advanced Encryption Standard) or DES (Data Encryption Standard). The basic problem with these encryption algorithms is that they have high encryption time making them un-suitable for real-time applications like PAY-TV, Pay-Per Viewand Video On Demand (VOD) etc. A unique characteristic of video data is that, even though information rate is very high, information value is very low. Exploiting this fact, to decrease the encrypted video time, many encryption algorithms have been proposed which encrypt only selected parts of the data.Meyer and Gadegast [2] have designed an encryption algorithm named SECMPEG which incorporates selective encryption and additional header information. In this encryption selected parts of the video data like Headers information, I-blocks in P and B frames are encrypted based on the security requirements. Qiao and Nahrstedt [3] proposed a special encryption algorithm named video encryption algorithm in which one half of the bit stream is XORed with the other half. The other half is then encrypted by standard encryption algorithm (DES). The speed of this algorithm is roughly twice the speed of naive algorithm, but that is arguably still the large amount of computation for high quality real-time video applications that have high bit rates [4]. Some of the other encryption algorithms are based on scrambling the DCT coefficients. Tang's [5] scrambling method is based on embedding the encryption into the MPEG compression process. The basic idea is to use a random permutation list to replace the zig-zag order of the DCT coefficients of a block to a 1 × 64 vector. Zeng and Lie [6] extended Tang permutation range from block to segment, with each segment consisting of several macroblocks. Within each segment, DCT coefficients of the same frequency band are randomly shuffled within the same band. Chen, et. al [7] further modified this idea by extending the permutation range from a segment to a frame. Within a frame, DCT coefficients are divided into 64 groups according to their positions in 8 × 8 size blocks, and then scrambled inside each group. Apart from shuffling of the I frames, they also permuted the motion vectors of P and B frames.In order to meet the real-time requirements, Shi,et. al [8] proposed a light-weight encryption algorithm named Video Encryption Algorithm (VEA). It uses simple XOR of sign bits of the DCT coefficients of an I frame using a secret m-bit binary key. The algorithm was extended as Modified Video Encryption Algorithm (MVEA) [9] wherein motion vectors of P and B frames are also encrypted along with I frames.

This paper present an efficient partial encryption technique based on SDD algorithm for real-time video transmission.

The SDD algorithm considered as a stream of bits and the technique uses dual key, first key (control key) to determine the length of bits block and the second one is used for encryption a according to the equation that used addition and multiplication based on mathematical theory of Galois field $GF(2^n)$.

Each block bits size (3 bits block or 4 bits block) in this algorithm are interpreted as finite field elements using a representation in which a 3 or 4 bits with bits b0 b1 b2 or b0 b1 b2 b3 represents the polynomial.

The encryption algorithm was applied on a part of I-frames of video, exclusively on Y Channel of YCbCr color vector.

DIGITAL VIDEO PRELIMINARIES

Digital video consists of a stream of images captured at regular time intervals, where the digital image is a discrete two-dimensional function, $f(x,y)$ which has been quantized over its domain and range [10]. Without loss of generality, it will be assumed that the image is rectangular, consisting of Y rows and X columns. The resolution of such an image is written as $X \times Y$. Each distinct coordinate in an image is called a pixel color space andeach color pixel is a vector of color components.

The Color spaces provide a standard method of defining and representing colors. Each color space is optimized for a well-defined application area [11]. The most popularcolor models are RGB (used in computer graphics); and YCrCb (used invideo systems). Processing an image in the RGB color space, with a set of RGB values for eachpixel is not the most efficient method. To speed up some processing steps manybroadcast, video and imaging standards use luminance and color difference videosignals, such as YCrCb, this color space is widely used for digital video. In this format, luminance information is stored as a single component (Y), and chrominance information is stored as two color-difference components (Cb and Cr).

In the RGB representation the channels are very correlated, as all of them include a representation of brightness, in which the brightness information can be recognized from R, G and B channels shown separately. But in YCbCr representation the luminance information of (Y) component is more thanchrominance information of (Cb and Cr) components[12].

A color in the RGB color space is converted to the YCrCb color space using the following equation [13]:

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \quad \text{........ (1)}$$

While the inverse conversion can be carried out using the following equation:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.164 & 0.000 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.017 & 0.000 \end{bmatrix} \begin{bmatrix} Y-16 \\ C_b-128 \\ C_r-128 \end{bmatrix} \quad \text{..... (2)}$$

Digital video stream is organized as a hierarchy of layers called: Sequence, Group of Pictures (GOP), Picture, Slice, Macroblock and Block. The Sequence Layer consists of a sequence of pictures organized into groups called GOPs.Each GOP is a series of I, P and B pictures[14].I pictures are intraframe coded without any reference to other pictures. P pictures are predicatively coded using a previous I or P picture. B pictures are bidirectionally interpolated from both the previous and following I and/or P pictures[7].
Each picture is segmented into slices, where a picture can contain one or more slices. Each slice contains a sequence of macroblocks where a macroblock consists of four luminance blocks (Y) and two chrominance blocks (Cb and Cr). Each block is organized into a matrix of 8x8 pixel samples with a macroblock covering a 16 x 16 pixel area, Figure (1) shows the Structural hierarchy of digital video.

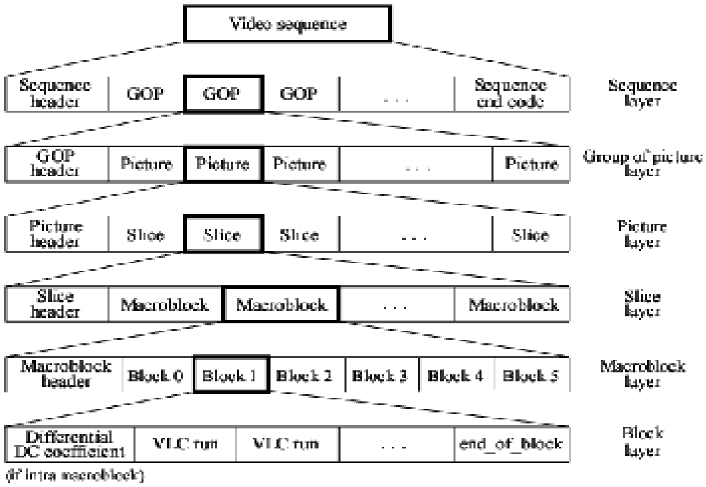


Figure (1) Structural hierarchy of Digital video.

The properties of the I, P, and B frames can help further improve the encryption and decryption performance. Since B frames depend on I or P frames, and P frames depend on the closest preceding I frame, we need only encrypt the I frames while leaving the P and B frames untouched. Without I frames, one cannot decode P and B frames.

MATHEMATICAL PRELIMINARIES BASED ON GALOIS FIELD

A field is a commutative ring (with unity) in which all nonzero elements have a multiplicative inverse [15]. For a given prime p, the finite field of order p, $\mathrm{GF}\,(\mathrm{p})$ is defined as the set $\mathrm{Z_p}$ of integers $\{0, 1, \dots, \mathrm{p}-1\}$, together with the arithmetic operations modulo p[16]. The finite field of order $\mathrm{p^n}$ is generally written $\mathrm{GF}\,(\mathrm{p^n})$.
Arithmetic in a finite field is different from standard integer arithmetic. There are a limited number of elements in the finite field; all operations performed in the finite field result in an element within that field.

A polynomial f(x) in $\mathrm{GF}\,(2^{\mathrm{n}})$ is represented as:

$$\mathrm{f(x)} = \mathrm{a_{n-1}x^{n-1}} + \mathrm{a_{n-2}x^{n-2}} + \dots + \mathrm{a_1x} + \mathrm{a_0} = \sum_{\mathrm{i=0}}^{\mathrm{n-1}} \mathrm{a_i\,x^i}$$

Can be uniquely represented by its n binary coefficients $(\mathrm{a_{n-1}a_{n-2}\dots a_0})$. Thus, every polynomial in $\mathrm{GF}\,(2^{\mathrm{n}})$can be represented by an n-bit number. In this paper we are concerned with the finite field $\mathrm{GF}\,(2^3)$and $\mathrm{GF}\,(2^4)$.

The addition of two finite field elements is achieved by adding the coefficients for Corresponding powers in their polynomial representations, this addition being performed in $\mathrm{GF}(2)$, that is, modulo 2, so that $1 + 1 = 0$. Consequently, addition and subtraction are both equivalent to an exclusive-or operation on the n-bits that represent the field elements of $\mathrm{GF}\,(2^{\mathrm{n}})$ .Tables 1 and 2 represent the addition and addition inverse in $\mathrm{GF}\,(2^4)$ consecutively.

Finite field multiplication is more difficult than addition and is achieved by multiplying the two polynomials for the two elements concerned and collecting like powers of x in the result, if a multiplication result in a polynomial of degree greater than n-1, then the polynomial is reduced modulo some irreducible polynomial m(x) of degree n. That is, divided by m(x) and keep the remainder. The definition of irreducible polynomial is a polynomial f(x) over a field F is called irreducible if and only if f(x) cannot be expressed as a product of two polynomials, both over F, and both of degree lower than that of f(x) [16].

Since each polynomial for 3 bits block can have powers of x up to 3, the result can have powers of x up to 6 and will no longer fit within a 3bits, and for 4 bits block can have powers of x up to 4, the result can have powers of x up to 8 and will no longer fit within a 4 bits. This situation is handled by replacing the result with the remainder polynomial after division by a special order irreducible polynomial; irreducible polynomial of degree 3 there are only two such polynomials:

$(x^3 + x^2 + 1)$ and $(x^3 + x + 1)$, and of degree 4, there are three:

$$(x^4 + x + 1), (x^4 + x^3 + x^2 + x + 1) \text{ and } (x^4 + x^3 + 1)$$

To construct the multiplication finite filed $GF(2^n)$ requires choosing an irreducible polynomial of degree n.

Table 3 represents multiplication in finite field $GF(2^4)$ with irreducible polynomials $m(x) = x^4 + x + 1$.

Each element of the finite field set other than 0 has a multiplicative inverse [16]. Just as the Euclidean algorithm can be adapted to find the greatest common divisor (gcd) of two polynomials, the extended Euclidean algorithm can be adapted to find the multiplicative inverse of a polynomial. Specifically, the algorithm will find the multiplicative inverse of b(x) modulo m(x) if the degree of b(x) is less than the degree of m(x) and gcd[m(x), b(x)] = 1. If m(x) is an irreducible polynomial, then it has no factor other than itself or 1, so that gcd[m(x), b(x)] = 1. Suppose two polynomials a(x), b(x), and m(x) is an irreducible polynomial, a(x) and b(x) are mutual inverses If a(x).b(x) mod m(x) =1. Table 4 represents multiplication inverse in finite field $GF(2^4)$ with irreducible polynomials $m(x) = x^4 + x + 1$Theaddition, Addition inverse, Multiplication and Multiplication inverse tables for $GF(2^3)$are existent in [16].

PARTIAL ENCRYPTION ALGORITHM OF VIDEO (METHODOLOGY)

The encryption scheme can be described by the following steps:

```
Input :
Y-channel as  Plaintext , KeyOne ,
KeyTwo
Output :
Y-channel asCiphertext
          No_K1          //number of
bits from keyOne  that are used in
one round
          No_K2          //number of
bits from keyTwo  that  are used in
one round

 Step 0:
          Round= 0
 -  While Round < 2 do :
Step 1: Read a portion of KeyOne
(Control key)
Step 2: depending  on the value of
          KeyOne's portion    do the
          following:
          Select the block size ( 3 bits or 4 bits) from plaintext.
          Read from KeyTwo A and B Keys.
          Perform the following Encryption Equation :
                 $Y = X \ast A + B$

Step3 : Compute the number of bits for KeyOne and KeyTwo that are used in one round
             Check If Round =0 then
                 No_K1=No_K1 + 2
                 No_k2=No_K2 + block size * 2
             End if
Step 4: Repeat steps 1, 2 and 3 until plaintext is finished.
          Round=Round+1
          End while.
```

The partial encryption of video technique is based on SDD algorithm which uses two keys, the first key is called control key (keyOne) which is used to determine the size of bit block and the second one(KeyTwo) is used for encryption.

The size of bit block is either 3 bits or 4 bits. The first step of the technique is reading the two less significant bits from control key(KeyOne) if the value is odd, the block size will be 3 bits Otherwisewill be 4 bits. Suppose the value of these two bits is odd, then 3bits from plaintext is to be read and stored in X varible. 3bits from KeyTwo is to be read and stored in A variable and the next three bits is also to be read and stored in B variable. Second step, the encryption equation is performed on the 3bits block: $Y = X \ast A + B$.
If two bits' value of KeyOne is even the same steps are applied but with four bits instead ofthree bits.

Third step is used to count the number of bits for KeyOne and KeyTow that are used in one round; these bits are used later in Decryption part of the algorithm.
These steps are applied to the rest plaintext message. Addition and multiplication in the encryption equation are based on a Galois field $GF(2^3)$, and $GF(2^4)$.

PARTIAL DECRYPTION ALGORITHM OF VIDEO

The decryption Technique can be described by the following steps:

```
Input :   Y-Channel asCiphertext  , KeyOne , KeyTwo
Output :  Y-channel as  Plaintext

STEP1. Round=0
-While Round < 2 do
STEP2. apply  a circular left shift of  (No_K1)  bits and
       (No_K2) bits for KeyOne and KeyTwo  consecutively
STEP3. Read a portion of KeyOne(Control key)
STEP4. depending on the value of  KeyOne'sportion  do the
       following
       Select the block size ( 3 bits or 4 bits) from plaintext
       Read from KeyTwo  A and B Keys
       Perform the following Decryption  Equation  :
           $X = (Y + \text{addtion inverse}(B)) * \text{multiplicative inverse}(A)$
STEP5. Repeat steps 1 ,2 and 3 until  Ciphertext  is finished
Round=Round+1
End while
```

For decryption the same steps of encryption are applied but with reverse equation's operations are performed.

PARTIAL ENCRYPTION TECHNIQUE OF VIDEO

The Suggested Technique model consists of two parts; the main stages of the first part are started from reading video file(with note that the frames of digital video is in YCbCr color system), converting it into frames, the output of this stage is frames in YCbCr color representation, the last stage deals with selecting the I-frame. In the second part of system, the Partial Encryption algorithm is applied on Y-channel of I-frame, then reconstructing the video file before broadcasting. At the receiver side, the video file will be converted into frames, andapplying the Partial decryption algorithm on Y-channel of I-frame, Figure 2 illustrates the steps of proposed system.

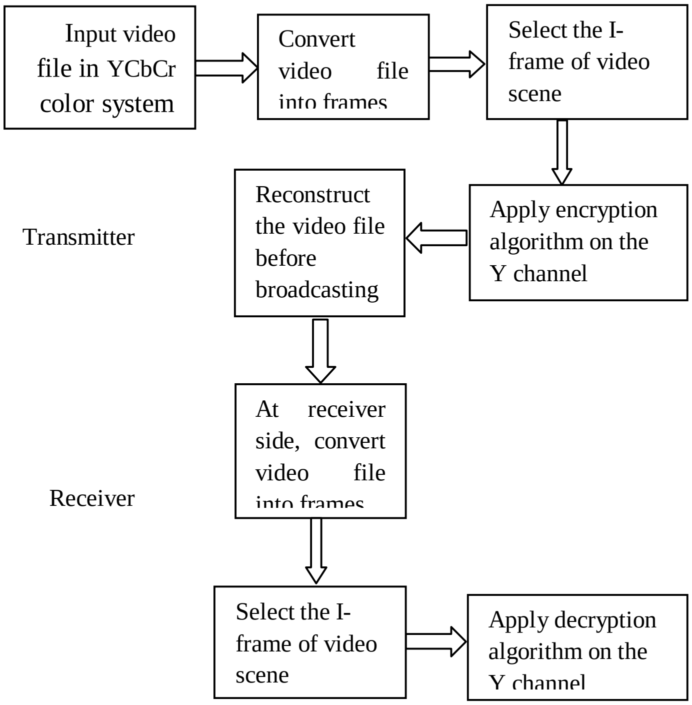

Input video file in YCbCr color system
Convert video file into frames
Select the I-frame of video scene
Apply encryption algorithm on the Y channel
Reconstruct the video file before broadcasting
Transmitter
At receiver side, convert video file into frames
Receiver
Select the I-frame of video scene
Apply decryption algorithm on the Y channel

Figure (2) The steps of partial encryption Technique

SECURITY EVALUATION OF PARTIAL ENCRYPTION TECHNIQUE

Cryptography may be described as the science of secure communication over a public channel. An important area of cryptography is symmetric key cryptography. In symmetric key cryptography, the two parties share a secret piece of information, the key, and a public encryption algorithm.

The message (M) is encrypted by using the encryption half of algorithm $C=E_k(M)$. The message is decrypted by computing:

$$D_k(C) = D_k(E_k(M)) = M.$$

Where M, K, and C may are took to be finite sequencesof bits.

Without knowing K, an attacker cannot compute M from C. A more common assumption in modern cryptography is to assume that an attacker may have several pairs M_i,C_i from which to try to recover the key (a known plaintext attack), or may even be able to pick M’s or C’s to have encrypted or decrypted. (a chosen plaintext or chosen ciphertext attack, or, if both are allowed, a chosen text attack). In these cases, simply by trying all possible keys an attacker will eventually recover the key K. This is known as a brute force attack, or exhaustive key search.

The SDD algorithm is resistant against brute force attacks, because it employs dual key and dynamic block cipher, hence it will be very difficult to guess the key.

The following example illustrates the large number of possibilities of keys that the attacker needs to decrypt the small size of ciphertext with 128 bits by using (SDD) technique:

The control key (KeyOne) determines the block size either 3bits or 4bits block size.

To construct $\mathrm{GF}(2^3)$, there are two an irreducible polynomials degree 3, and for construct $\mathrm{GF}(2^4)$, there are three with degree 4.The equation is:

$Y = X \ast A + B$, A and B are keys, the size of both is either 3 bits or 4 bits.

If the block size is 3 bits, the number of possible keys for each key is 2^3.

The number of possibility of keys to decrypt one 3bits block size for each round is:

$2*2^3 * 2^3=2^7$.

The number of possibility of keys to decrypt one 4bits block size for each round is:

$3*2^4 * 2^4=3 *2^8$.

To decrypt only one block, the number of possibility of keys for each round is:

$(2^7 +3 *2^8)=896$.

It is possible to compute the minimum and maximum number of possibility of keys to decrypt 128 bits of ciphertext, first the maximum number of blocks is computed when all blocks are of 3bits size,

128 ÷3=42.6, the result with reminder will be increased by one, thus the maximum number of blocks is 43, and the minimum number of blocks is computed when all blocks are of 4bitssize, 128 ÷4=32.

It can be computed the minimum and maximum number of possibility of keys to decrypt 128 ciphertext bits.

The minimum number of possibility of keys for each round is:

$(2^7 + 3 *2^{8)32}$ = 2.97753112e+94.

The maximum number of possibility of keys for each round is:

$(2^7 + 3 *2^8)^{43}$ = 8.89701700e +126.

The algorithm has two rounds hence the minimum number of possibility of keys is:

$(2^7 + 3 *2^8)^{32} * (2^7 + 3 *2^8)^{32} = 2* (2^7 + 3 *2^8)^{64}$ = 8.86569157e+188

The maximum number of possibility of keys for two rounds is:

$(2^7 + 3 *2^8)^{43} * (2^7 + 3 *2^8)^{43}= (2^7 + 3 *2^8)^{86}$ =7.91569097e+253

EXPERIMENTAL RESULTS

Advanced Encryption Standard (AES) is an algorithm of the first category which is used nowadays in communication and encrypted video broadcasting, and it provides much higher security level than DES and perform it in 3 to 10 less computational power than 3-DES [17], it has better performance than DES, 3DES, and RC2 [18], based on these facts, AES is to be compared with proposed technique.

The following tables represent the experimental results for the speed of the partial video encryption based on SDD, and AES algorithm.

As shown in tables 5and 6, we observed that the SDD algorithm is approximately 13 times faster than AES encryption and 9 times faster than AES decryption.

The sample test video sequences include videos like Car, Wedding, and xylophone. Some of the test videos along with their frame numbers are shown in Figure 3, Figure4 and Figure5.

The designed technique and AES algorithm both has been implemented successfully using visual basic 6 Programming language and also implemented with processor of Pentium IIII (3.40 GHZ) and 3GB of RAM on windows XP.

CONCLUSIONS

In this paper, we have proposed a new partial digital video encryption technique. From the experimental results and security evaluation of partial encryption technique we have come to conclusion the following:

1-The(SDD) algorithm provides high level of security by using dual key, and dynamic tiny block cipher that prevent exhaustive key search and differential attacks.

Non fixed (dynamic) size block cipher avoid replaying in authentication and attacks that can happen on the fixed sized block cipher algorithm, dynamic block length in proposed algorithm leads to maximum cryptographic confusion and consequently makes it difficult for cryptanalysis.

2-because the new technique encrypts only Y-channel from I-frame of the video scene, this will reduce the encryption and decryption time, in addition its high security depending on (SDD) algorithm, these properties make the technique appropriate for real time application.

3-No variation has been made in the digital video structure, because of making use of the present broadcasting technique; whereas a change has been made in the part of complete structure.

REFERENCES

[1] Nehete", J. K.Bhagyalakshmi, M.B. Manjunath, S. Chaudhari, T. R. Ramamohan "A Real-time MPEG Video Encryption Algorithm using AES",NCC-2003.

[2] J. Meyer and F. Gadegast, “Security Mechanisms for Multimedia Data with the Example MPEG-1Video”, Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.

[3] Qiao, L and Klara Nahrstedt, “A New Algorithm for MPEG Video Encryption”, In Proc. of First International Conference on Imaging Science System and Technology, Las Vegas, pp 21–29, 1997.

[4] Furht, B. and D. Kirovski, “Multimedia Encryption Techniques", Multimedia Security Handbook, CRC Press LLC, Dec. 2004.

[5] Tang, L. “Methods for Encrypting and Decrypting MPEG Video Data Efficiently”, In Proc. of ACM Multimedia, Boston, pp 219-229, 1996.

[6] Zeng,W. and Sh. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video", In Proc. of the IEEE Transactions on Multimedia, pp 118-129, 2002.

[7] Chen, Z. Z. Xiong, and L. Tang."A novel scrambling scheme for digital video encryption". In Proc. of Pacific-Rim Symposium on Image and Video Technology (PSIVT), pp 997–1006, 2006.

[8] Shi,C. S. Wang, and B. Bhargava,"MPEG Video Encryption in Real time Using Secret Key Cryptography", In Proc. of International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, NV ,1999.

[9] Shi, C. and B. Bhargava, "A Fast MPEG Video Encryption Algorithm", In Proc. of ACM Multimedia,Bristol,UK, pp 81-88, 1998.

[10] Robert Gray, M. and L. David Neuhoff. "Quantization". IEEE Transactions on Information Theory, 44(6):1.63, October 1998.

[11] Gonzalez, R. C. and R. E. Woods, "Digital Image Processing", Second Edition, Printice Hall Inc, (2002)

[12] Iain Richardson.,E. G. "H.264 and MPEG-4 Video Compression ",The Robert Gordon University, Aberdeen, John Wiley & Sons Ltd ,UK, 2003.

[13] Drew, Li &,"Fundamentals of Multimedia", Chapter 5, Prentice Hall 2003.

[14] Tudor, P. N. "MPEG-2 video compression", In Electronics and Communication Engineering Journal, Dec.1995.

[15] Nakahara Jr, J. and E. Abrah˜ao, "A New Involutory MDS Matrix for the AES", International Journal of Network Security, Vol.9, No.2, PP.109–116, Sept. 2009.

[16] Stallings,W. "Cryptography and Network Security", 4th edition, Prentice-Hall, 2005.

[17] J. Dray, "Report on the NIST Java^{TM} AES Candidate Algorithm Analysis", NIST ,1999.

[18] Abd Elminaam, D. S. H. M. Abdual Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3,PP.216–222, May 2010.

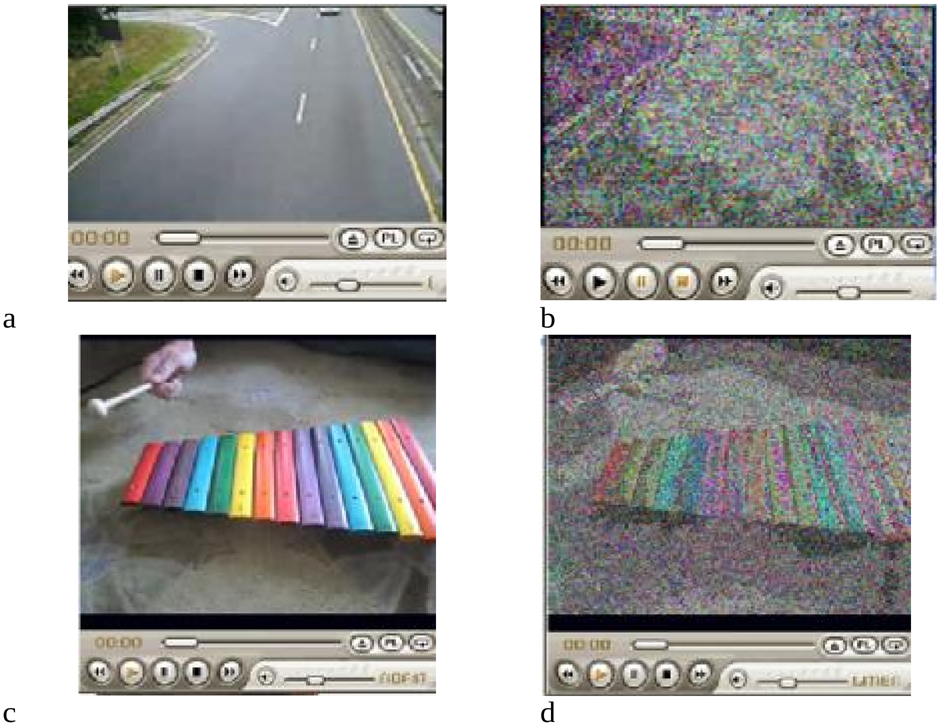


Figure (3): The encryption results after applying partial encryption based on SDD algorithm for the 1st frame in "Car" and xylophone video. a) Original I-frame of car video b) car I-frame after encryption c) Original I-frame Of xylophone video d) xylophone I-frame after encryption.

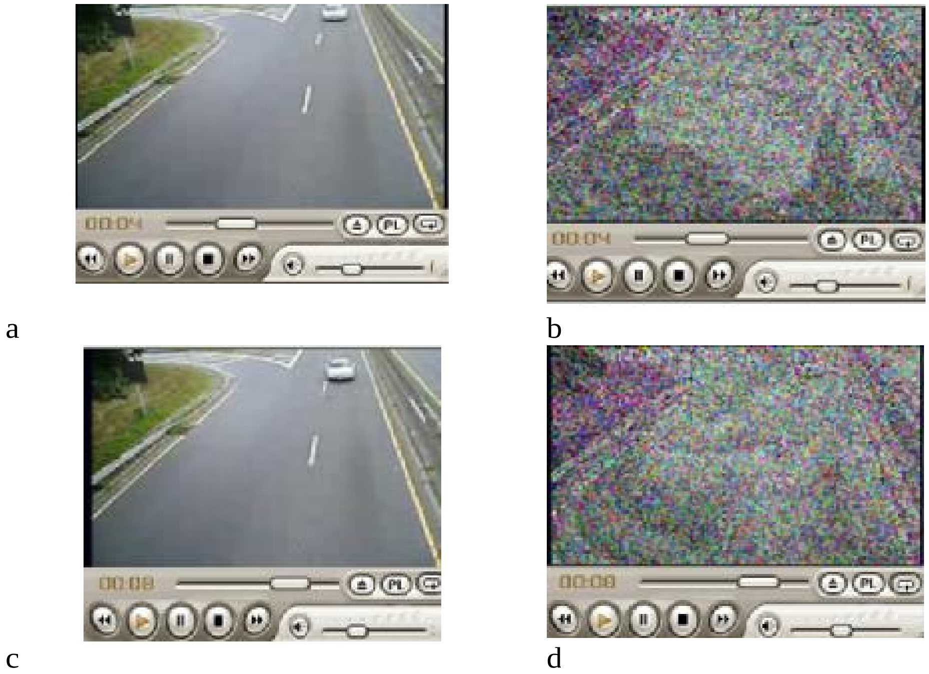


Figure (4): The effect of the partial encryption based on SDD algorithm on Car Video Frames is used as test object. (a)Original car film after 4 seconds (b) Encryption car film after 4 seconds (c) Original car film After 8 seconds (d) Encryption car film after 8 seconds

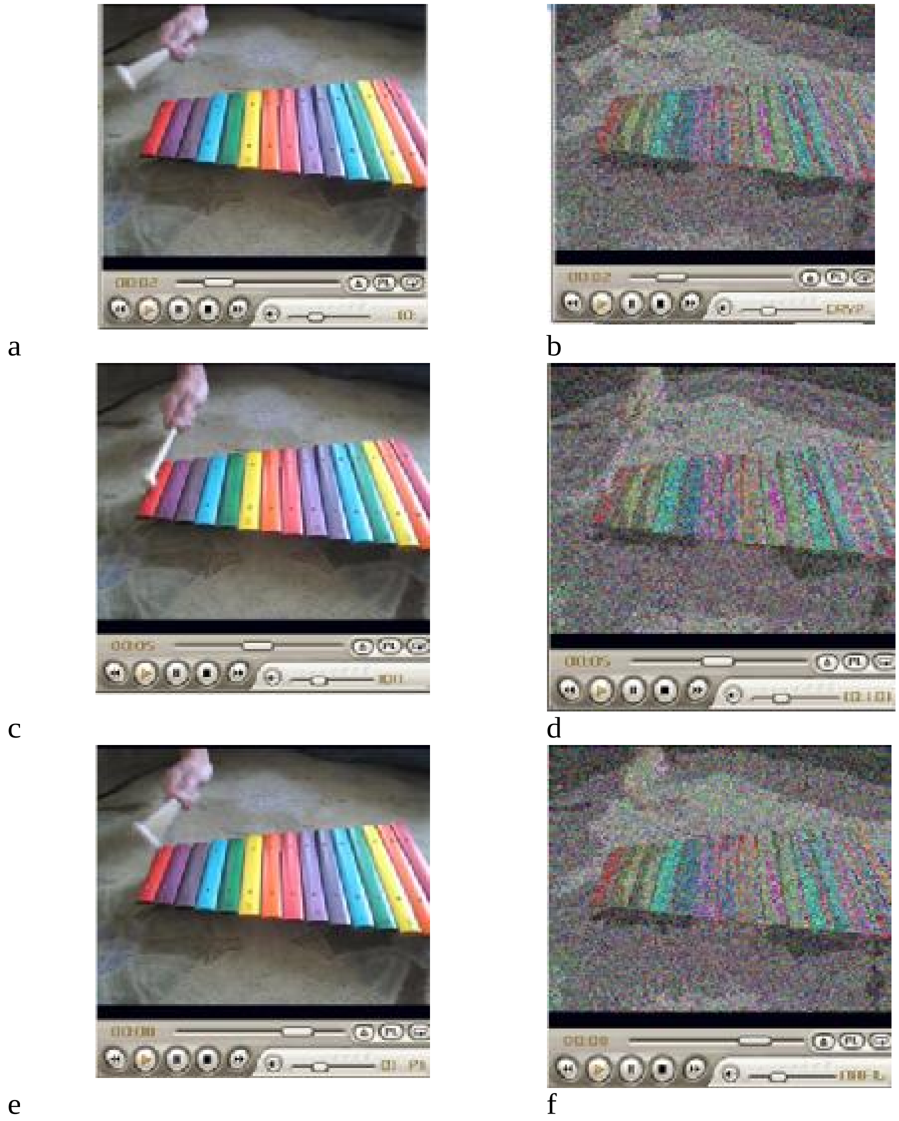
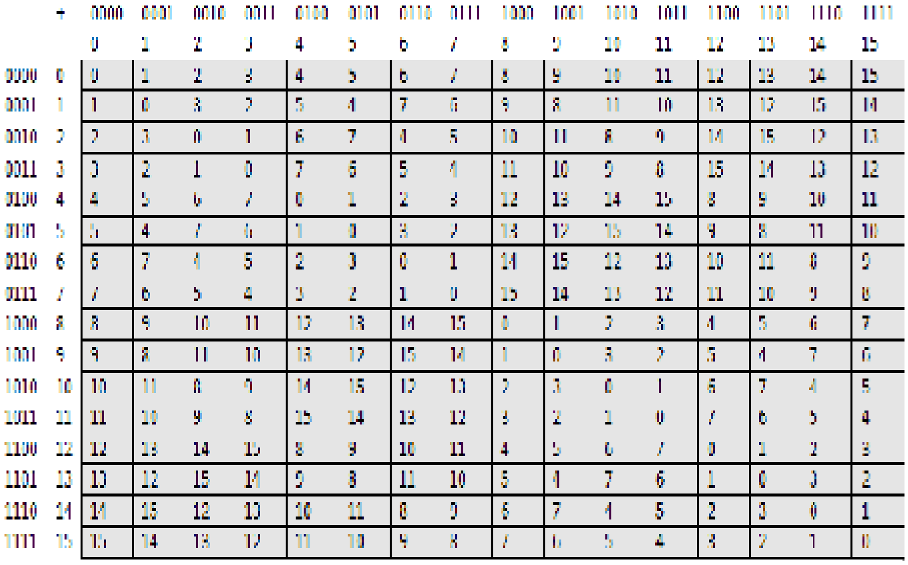


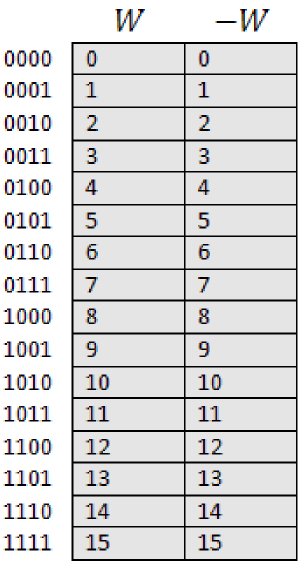
Figure (5): The effect of the partial video encryption based on SDD algorithm on xylophone video frames is used as test object (a)Original xylophone film after 2 seconds b) Encryption xylophone film after 2 seconds (c) Original xylophone film after 5 seconds (d) Encryption xylophone film after 5 seconds (e) Original xylophone film after 8 seconds (f) Encryption xylophone film after 8 seconds.

Table (1) Addition operation in $\mathrm{GF}(2^4)$.



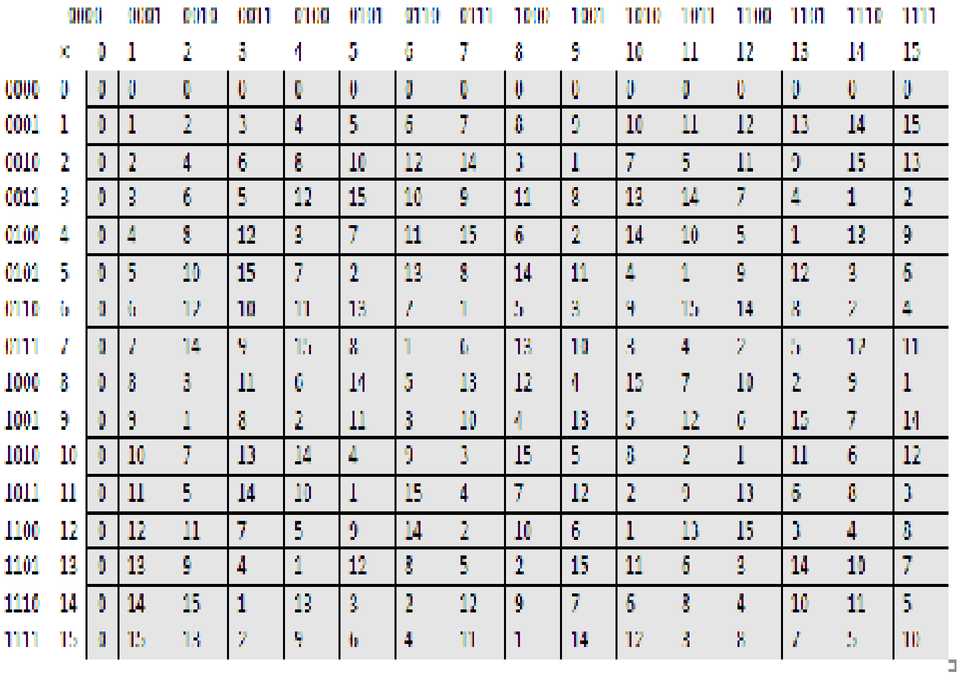
+		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0001	1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
0010	2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
0011	3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
0100	4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
0101	5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
0110	6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
0111	7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
1000	8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
1001	9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
1010	10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
1011	11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
1100	12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
1101	13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
1110	14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
1111	15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Table (2): Addition inverse in $\mathrm{GF}(2^4)$.



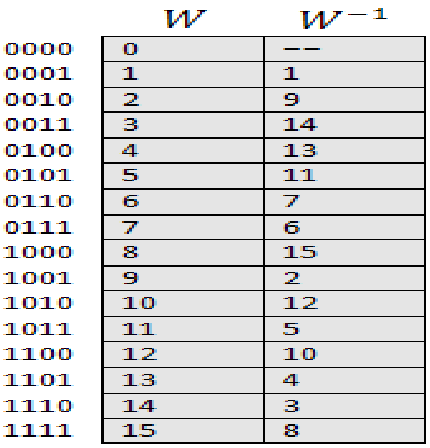
	W	$-W$
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	10
1011	11	11
1100	12	12
1101	13	13
1110	14	14
1111	15	15

Table (3): Multiplication in GF(2^4) with the irreducible polynomial m(x) = x^4 + x + 1



		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
	x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0010	2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
0011	3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
0100	4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
0101	5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
0110	6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
0111	7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
1000	8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
1001	9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
1010	10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
1011	11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
1100	12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
1101	13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
1110	14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
1111	15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Table (4): Multiplication inverse in GF(2^4) with the irreducible polynomial m(x) = x^4 + x + 1



	w	w^{-1}
0000	0	--
0001	1	1
0010	2	9
0011	3	14
0100	4	13
0101	5	11
0110	6	7
0111	7	6
1000	8	15
1001	9	2
1010	10	12
1011	11	5
1100	12	10
1101	13	4
1110	14	3
1111	15	8

Table (5): The encryption and decryption times for AES algorithm using key size 128bit on I-frame.

Security Algorithm	I-Frame Name	Size of Frame KB	Encryption time (Second)	Decryption time (Second)
AES-Rijndael	Car	60	8	12
	Wedding	1180	175	260
	xylophone	225	28	46

Table (6): The encryption and decryption times for (SDD) algorithm on I-frame.

Security Algorithm	I-Frame Name	Size of Frame KB	Encryption time (Second)	Decryption time (Second)
SDD algorithm	Car	60	0.656	1.282
	Wedding	1180	12.468	28.594
	xylophone	225	2.312	5.438