USING DYNAMIC DUAL KEYS ENCRYPTION ALGORITHM AS PARTIAL ENCRYPTION FOR A REAL-TIME DIGITAL VIDEO

Abdul Monem S. Rahma[1] and Basima Z.Yacob[2]
[1]Computer Science Department, University of Technology, Baghdad, Iraq
[2]Computer Science Department, University of Duhok, Duhok, Kurdistan Iraq

ABSTRACT

Advances in digital video transmission have increased in the past few years. 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 interframe 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 depends on Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields which is fast enough to meet the real-time requirements with high level of security. 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 Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields is applied to the Y channel. The encryption technique achieves best timing results, and it provides high level of security by its great resistant against brute force attacks.

KEYWORDS: *Encryption digital video, partial encryption for Digital video, Digital video encryption in real time.*

I. INTRODUCTION

In the digital world nowadays, the security of digital images/videos becomes more and more important since the communications of digital products over network occur more and more frequently. In addition, special and reliable security in storage and transmission of digital images/videos is needed in many digital applications, such as pay-TV, broadcasting, confidential video conferencing and medical imaging systems, etc. 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. The naïve 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 View and 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.

This paper presents an efficient partial encryption technique depends on Dynamic Dual Key Encryption algorithm Based on joint Galois Fields for real-time video transmission.

The Dynamic Dual Key Encryption algorithm Based on joint Galois Fields is 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 (3, 4, 5, or 6) bits size in this algorithm are interpreted as finite field elements using a representation In which a 3, 4, 5 or 6 bits with bits $b_0\, b_1\, b_2$, $b_0\, b_1\, b_2\, b_3$, $b_0\, b_1\, b_2\, b_3\, b_4$ or $b_0\, b_1\, b_2\, b_3\, b_4\, b_5$ represents the polynomial consecutively, this algorithm is existing and introduced in details in[1]

We apply the encryption algorithm to a part of I-frames of video, exclusively on Y Channel of YCbCr color vector. This technique is fast enough to meet the real-time requirements, in addition it provides high level of security by its great resistant against brute force attacks. To decrypt the ciphertext with 128 bits, the attacker needs $1.86285884e+204$ of possibilities of keys as minimum and $1.80032832e+399$ as maximum [1].

The paper is organized as follows. Section 2 presents related work, Section 3 introduces digital video preliminaries. Section 4 and 5 present the methodology of partial encryption and decryption algorithm video consecutively. In Section 6 the suggested technique for partial video encryption is presented. Section 7 shows the experimental results for proposed technique of partial video encryption, Discussion the proposed technique for partial video encryption is presented in section8. Finally, conclusions are provided in Section 9.

II. RELATED WORK

Many video 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.

III. 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 and each 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 popular color models are RGB (used in computer graphics); and YCrCb (used in video systems). Processing an image in the RGB color

space, with a set of RGB values for each pixel is not the most efficient method. To speed up some processing steps many broadcast, video and imaging standards use luminance and color difference video signals, 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 than chrominance 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.

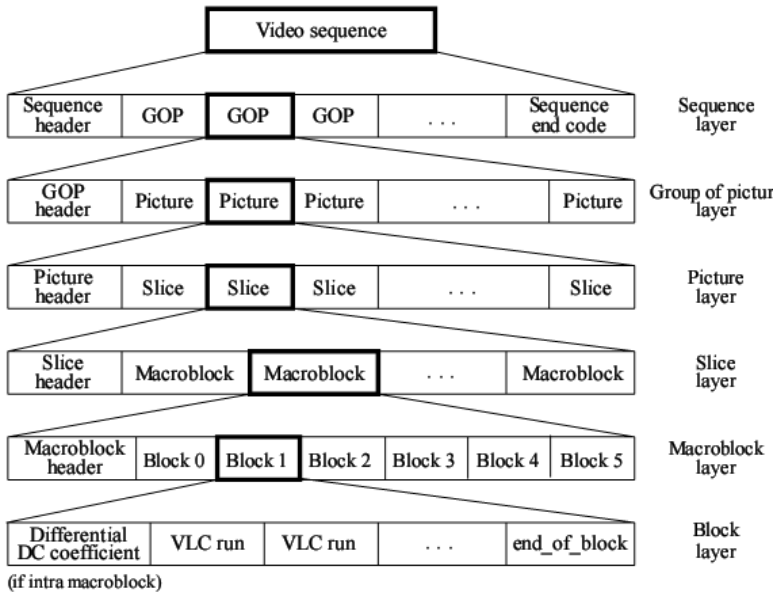


Figure 1: Structural hierarchy of Digital video.

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.

IV. 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 as Ciphertext
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 , 4 ,5 or 6 bits) from plaintext.
Read from KeyTwo A and B Keys.
Perform the following Encryption Equation :

$$Y = X * A + B$$

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 Dynamic Dual Key Encryption 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 3,4,5 or 6 bits [1].

V. PARTIAL DECRYPTION ALGORITHM OF VIDEO (METHODOLOGY)

The decryption Technique can be described by the following steps:

Input : Y-Channel as Ciphertext , 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 ,4,5 or 6 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 [1].

VI. PARTIAL VIDEO ENCRYPTION TECHNIQUE

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 Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields 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, and applying the Dynamic Dual Key decryption Algorithm Based on joint Galois Fields on Y-channel of I-frame, Figure 2 illustrates the steps of proposed system.

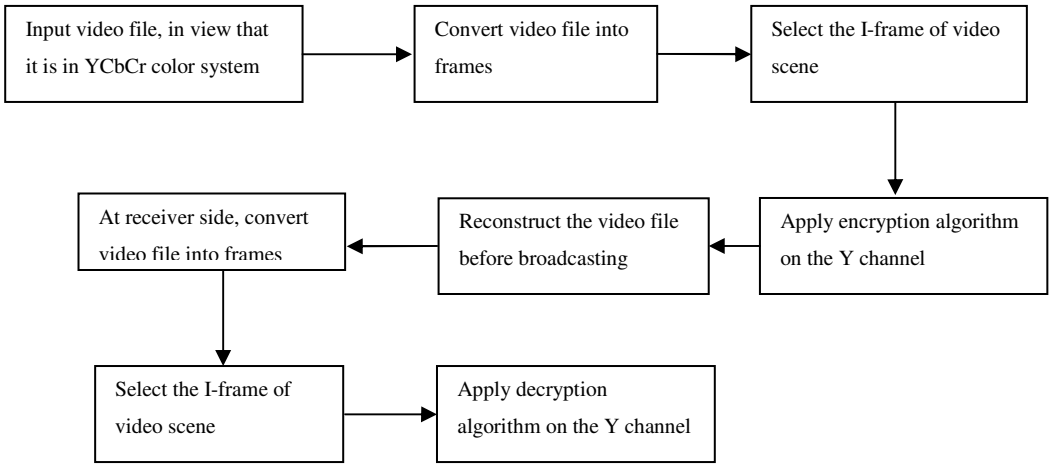


Figure (2): The steps of partial encryption Technique

VII. 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 [15], it has better performance than DES, 3DES, and RC2 [16], 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 Dynamic Dual Key Encryption algorithm, and AES algorithm.

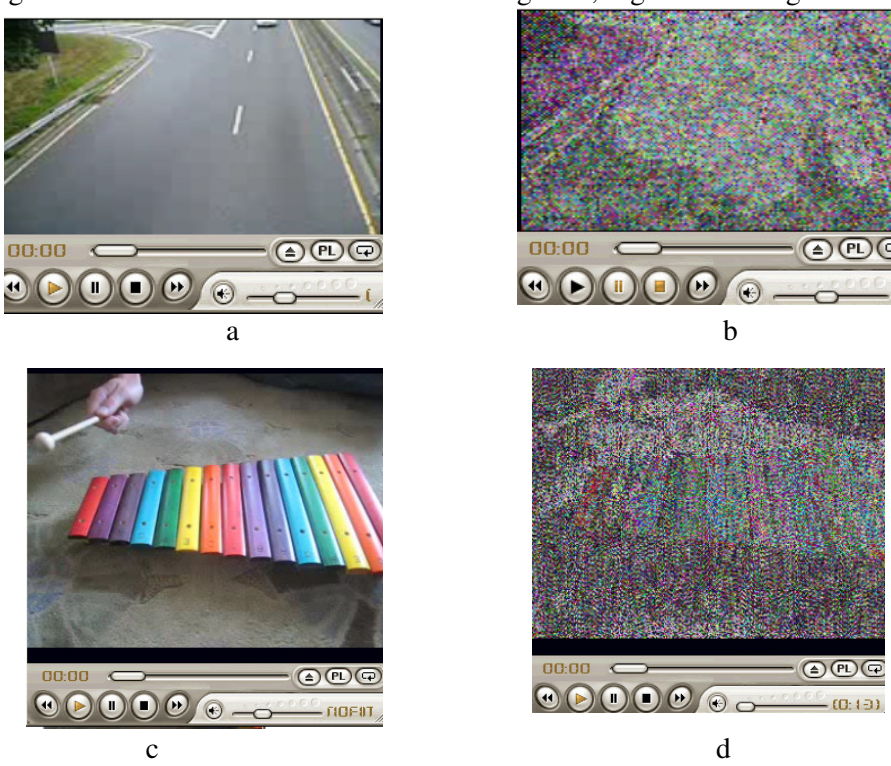
Table 1: The encryption and decryption times for AES algorithm using key size 128 bit on I-frame

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 2: The encryption and decryption times for Dynamic Dual Key Encryption algorithm on I-frame.

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

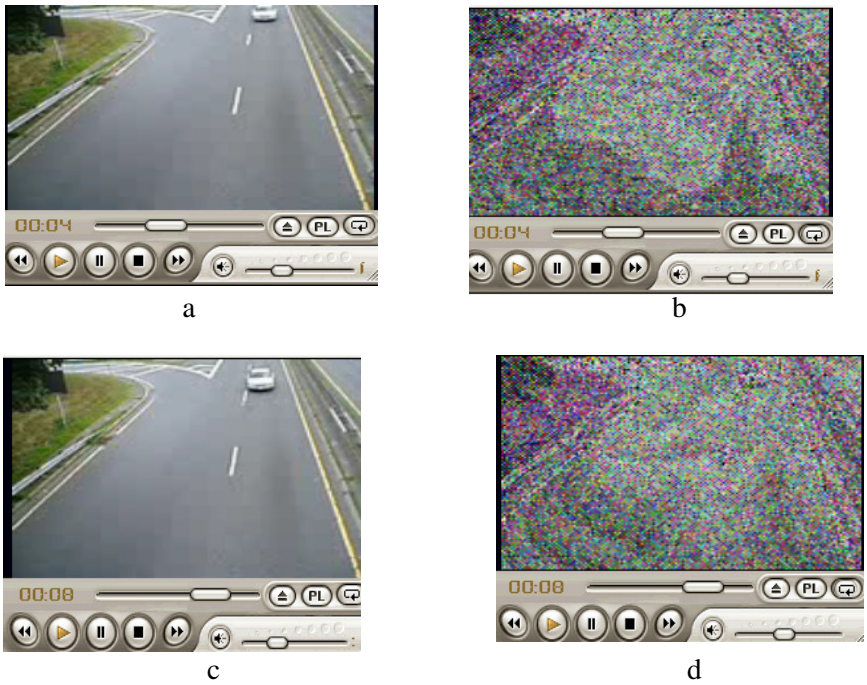
From Tables 1 and 2, Can be observed that the Dynamic Dual encryption algorithm is approximately 13 times faster than AES encryption and 9 times faster than AES decryption.
The sample test video sequences include videos like Car, Wedding, and xylophone. Some of the test videos along with their frame numbers are shown in Figure 3, Figure 4 and Figure 5.



a b

c d

Figure (3): The encryption results after applying partial encryption based on Dynamic Dual keys 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.



a b

c d

Figure (4): The effect of the partial encryption based on Dynamic Dual keys 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

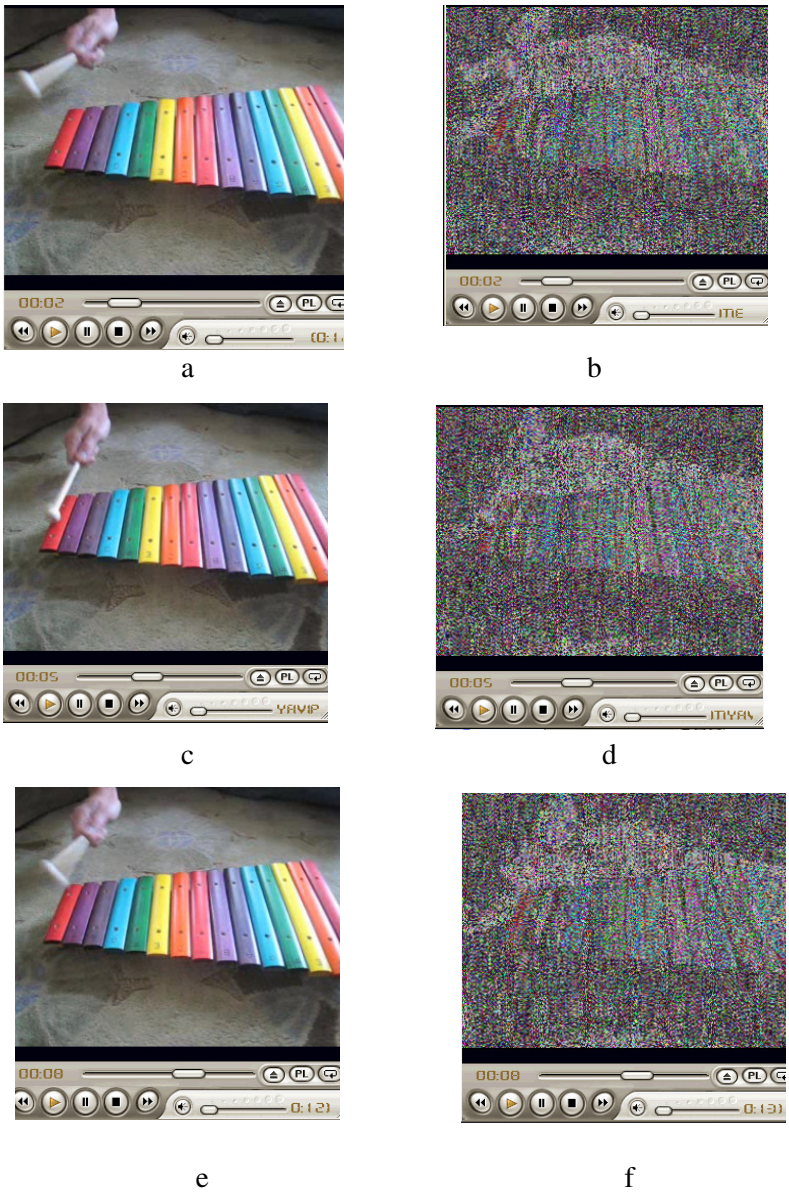


Figure (5) The effect of the partial encryption based on Dynamic Dual keys algorithm on xylophone Video Frames is used as test object (a) Original xylophone film after 2 seconds (b) Encryption xylophone film after 2 seconds (c) Original xylophone film after 5 seconds (d) Encryption xylophone film after 5 seconds (e) Original xylophone film after 8 seconds (f) Encryption xylophone film after 8seconds.

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.

VIII. DISCUSSION

The comparison between the speed of partial encryption digital video technique which uses AES algorithm, and the partial encryption digital video technique which uses Dynamic Dual Keys algorithm ,it can be seen from tables 1and 2 that the speed of the technique which uses Dynamic Dual Key Encryption algorithm is faster than the technique which uses AES algorithm, whereas the technique which uses Dynamic Dual Keys algorithm gets the best results , and it is approximately 13 time faster than AES encryption and 9 times faster than AES decryption. Because of the high security obtained by Dynamic Dual Key Encryption algorithm this will make the proposed technique high security.

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

IX. CONCLUSION

In this paper, we have proposed a new partial digital video encryption technique. The proposed technique which encrypts only Y-channel from I-frame of the digital video scene will reduce the encryption and decryption time, in addition to its high security depending on Dynamic Dual Key Encryption algorithm which uses dynamic block cipher and dual keys. All these properties will make the proposed technique suitable for Real-Time Application RTA.

REFERENCES

[1] Abdul Monem S. Rahma , and Basima Z.Yacob"The Dynamic Dual Key Encryption Algorithm Based on joint Galois Fields", International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.
[2] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video", Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.
[3] L. Qiao and Klara Nahrstedt, "A New Algorithm for MPEG Video Encryption", In Proc. of First International Conference on Imaging Science System and Technology, pp 21–29, 1997.
[4] Borko Furht and Darko Kirovski, "Multimedia Encryption Techniques, Multimedia Security Handbook," CRC Press LLC ,Dec. 2004 .
[5]L.Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", In Proc. of ACM Multimedia, Boston, pp 219-229, 1996.
[6] W. Zeng and Sh. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video", In Proc. of the IEEE Transactions on Multimedia, pp 118-129, 2002.
[7] Z. Chen, 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] C. Shi, 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] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm", In Proc. of ACM Multimedia, Bristol,UK, pp 81-88, 1998.
[10] Robert M. Gray and David L. Neuhoff. "Quantization", IEEE Transactions on Information Theory, 44(6):1.63, October 1998.
[11] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Second Edition, Printice Hall Inc, 2002.
[12] Iain E. G. Richardson. "H.264 and MPEG-4 Video Compression" The Robert Gordon University, Aberdeen, John Wiley & Sons Ltd, UK, 2003.
[13] Li & Drew," Fundamentals of Multimedia ", Chapter 5, Prentice Hall 2003.
[14] P. N. Tudor. "MPEG-2 video compression". In Electronics and Communication Engineering Journal, December - 1995.
[15] J. Dray, "Report on the NIST Java AES Candidate Algorithm Analysis", NIST ,1999.
[16] D. S. Abd Elminaam, 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.

Authors

Abdul Monem Saleh Rahma awarded his MSc from Brunel University and his PhD from Loughborough University of technology United Kingdom in 1982, 1985 respectively. He taught at Baghdad university department of computer science and the Military Collage of Engineering, computer engineering department from 1986 till 2003.He fills the position of Dean Asst. of the scientific affairs and works as a professor at the University of Technology Computer Science Department .He published 82 Papers in the field of computer science and supervised 24 PhD and 57 MSc students. His research interests include Cryptography, Computer Security, Biometrics, image processing, and Computer

graphics. And he Attended and Submitted in many Scientific Global Conferences in Iraq and Many other countries.

Basima Zrkqo Yacob received the B.Sc. degree in Computer Science from Mosul University, Iraq, in 1991, The MSc. Degree in computer science from University of Duhok ,Iraq in 2005. Currently she is a PhD student at faculty of computer science at Duhok University