



Sudan University of science and technology
College Of Graduate Studies
College of Computer Science and Information Technology



Preservation of Multimedia Confidentiality using Elliptic Curve

الحفاظ على سرية الوسائط المتعددة باستخدام المنحنى الإهليلجي

**Thesis submitted in partial fulfillment of the academic requirements for
the degree of Master in Information Technology**

Prepared by:

Zahraa Altayeb Mohammed sileman.

Supervision by:

Dr. Faisal Mohammed Abdalla Ali.

July 2019

الآيه

﴿ أَلَمْ يَأْنِ لِلَّذِينَ آمَنُوا أَنْ تَخْشَعَ قُلُوبُهُمْ لِذِكْرِ اللَّهِ وَمَا نَزَلَ مِنَ الْحَقِّ وَلَا يَكُونُوا كَالَّذِينَ أُوتُوا

الْكِتَابَ مِنْ قَبْلُ فَطَالَ عَلَيْهِمُ الْأَمَدُ فَقَسَتْ قُلُوبُهُمْ ۖ وَكَثِيرٌ مِّنْهُمْ فَاسِقُونَ (16) سورة الحديد (16)

صدق الله العظيم

Dedication

This thesis is dedicated, with deepest love and everlasting respect, to numerous

precious persons.

To my parents for their continuous love, support and encouragement which

helped me to achieve my dream.

To my family and all my friends, for their support and patience throughout

these stressful years.

To the principles of each and every ambitious person who knows that patience

and hard work make the dreams.

Acknowledgment

Firstly, all praise is due to Allah, without his immeasurable blessings and favors none of this could have been possible.

before beginning any thing you should have a good determination , will desire and the motivation I would like to thanks all the people who give me all that and encourage me to move on. I indebted to My Mather, father, all the family, my friend altoma alzain and my helpful my supervisor Dr. Fiasal Mohamed Abdalla Ali .I hope that I will be in their good forestation

Abstract

Today data security over the network is a serious concern as the amount of multimedia data is increasing at an exponential rate due to evolution of internet. Video encryption has various fields including internet communication, multimedia systems, medical imaging and military communication. To secure video, the data must be encrypted before transmission. Cryptographic algorithms are used to encrypt the video data and to achieve high confidentiality.

In this thesis Elliptic curve cryptography (ECC) method is used to encrypt video with line _cut scrambling techniques to provide the real time encryption. In order to reduce the video size Discrete Cosine Transform (DCT) is used. The proposed method increases video encoding speed and can be used in real time application. The results obtained are analyzed using standard metrics such as PSNR and MSE gives optimum results.

المستخلص

في يومنا هذا يعد أمن البيانات المارة عبر الشبكة مصدر قلق كبير كما أن كمية بيانات الوسائط المتعددة تتزايد بمعدل هائل بسبب تطور الإنترنت. يستخدم تشفير الفيديو في العديد من المجالات بما في ذلك الاتصالات عبر الإنترنت وأنظمة الوسائط المتعددة والتصوير الطبي والاتصال العسكري ولتأمين الفيديو يجب تشفير البيانات قبل الإرسال و تستخدم خوارزميات لتشفير بيانات الفيديو لتحقيق سرية عالية.

في هذا البحث ، تم استخدام طريقة تشفير المنحى الاهليجي مع تقنية ترميز الخط المتقطع لتشفير الفيديو في الوقت الفعلي واستخدام Discrete Cosine Transform (DCT) لتقليل حجم بيانات الفيديو. الطريقة المقترحة زادت من سرعة التشفير كما انها قللت من حجم بيانات الفيديو ويمكن استخدامها في الوقت الفعلي للتطبيقات. تم تحليل النتائج التي تم الحصول عليها باستخدام مقاييس قياسية مثل MSE PSNR التي اظهرت ان الطريقة المستخدمة اعطت نتائج جيدة .

Table of Content

الآيه	I
Dedication	III
Acknowledgment	IV
Abstract	V
المستخلص	VI
List of Tables	X
List of Figures	XI
List of Abbreviations	XII
Chapter I	1
Introduction.....	1
1.1 Introduction	1
1.2 Problem statement	1
1.3 Research Objective.....	2
1.4 Research Methodology.....	2
1.5 Research Organization	2
Chapter II.....	4
Literature Review	4
2.1 Introduction	4
2.2 Introduction to Multimedia	4
2.3.1 History of Multimedia	4
2.3.2 Types of Multimedia	6
2.3.3 The Basic Elements of Multimedia	6
2.3 Image and Video Data	7
2.4 Image Compression	7
2.5 JPEG Compression.....	9

2.5.1	Discrete Cosine Transform	9
2.5.1.1	Properties of DCT	11
2.5.2	Quantization	11
2.5.3	Entropy Encoding	12
2.6	Cryptography	13
2.6.1	Types of Cryptographic Algorithms.....	13
2.7	Elliptic Curve Cryptography (ECC).....	16
2.8	Multimedia Compression and Encryption.....	20
2.8.1	Requirements of multimedia encryption	21
2.8.2	Classification of Video Encryption Algorithms	21
2.9	Related Works	22
Chapter III.....		26
Research Methodology And Tools		26
3.1	Introduction	26
3.2	Proposed Work.....	26
3.3	Algorithm of Encryption and Decryption	27
3.4	Tools.....	29
Chapter IV.....		30
Implementation And The Results		31
4.1	Introduction	31
4.2	The Implementation	31
4.3	Quality Measurement and Evaluation	35
4.3.1	Mean Square Error (MSE):	35
4.3.2	Peak Signal to Noise Ratio (PSNR)	35
4.3.3	Histogram	36
4.4	Experimental Results.....	36

4.5	1-Result of quality analysis	37
4.6	Result of execution time.....	39
	Chapter V.....	41
	Conclusion And Future Work.....	42
	Reference:	43

List of Tables

Table 2. 1 : Comparison of the equivalent security level are used cryptographic key sizes.	17
Table 4. 1 : characteristics of the tested video	36
Table 4. 2 : objective fidelity criteria (PSNR, MSE) for the tested videos	37
Table 4. 3 : Execution Time.....	39

List of Figures

Figure 2. 1: DCT coefficients of 8x8 image block	11
Figure 2. 2 : symmetric-key encryption.....	14
Figure 2. 3 : public key cryptography	15
Figure 2. 4 : Hash Function process	16
Figure 2. 5 : (a) Point addition; (b) Point doubling; (c) Point at infinity when y coordinates are both 0; (d) Point at infinity when the coordinates are mirror image of each other. And will be explained as follows:	18
Figure 2. 6 : possible positions of multimedia encryption algorithms.....	21
Figure 3. 1 : Block Diagram for Encryption and Decryption	27
Figure 4. 1 : Extract frame and audio from video.....	31
Figure 4. 2 : Example of original video and extracted frame	32
Figure 4. 3 : Image compression.....	32
Figure 4. 4 : Example for image compression	33
Figure 4. 5 : plots in curve and calculate the ke	33
Figure 4. 6 : Encryption process	34
Figure 4. 7 : Convert frames into video	34
Figure 4. 8 : Example of convert frames into video	35
To evaluate the quality of this work, used the objective fidelity criteria measurements (peak signal to noise ratio (PSNR)), (mean square error (MSE)), PSNR and MSE are tested between the original video and the encrypted video as shown on table (4.2) and figures (4.9) and (4.10). The histogram of the original and encrypted video in shown in figure (4.11) the figure also show that the frames could be recover correctly.	37
Figure 4. 9 : Result of PSNR	37
Figure 4. 10 : Result of MSE	38
Figure 4. 11 : shows some of the original and encrypted of tested video and the histogram of each one.	39
Figure 4. 12 : Results of the execution time	40

List of Abbreviations

Abbreviation	Meaning
B-VOP	Bi-Directional Video Object Plane
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DVI	Digital Video Interface
ECC	Elliptic Curve Cryptography
FDCT	Forward Discrete Cosine Transform
I-VOP	Intra-Video Object Plane
JPEG	Joint Photographic Experts Group
MPEG	Moving Picture Experts Group
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
P-VOP	Predictive- Video Object Plane

Chapter One
Introduction

Chapter I

Introduction

1.1 Introduction

Advances in digital content transmission have increased in the past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology this advances in multimedia technologies have popularized applications like video conferencing, pay-per-view, video on demand (VOD), video broadcast, etc. In such applications, confidentiality of the video data during transmission is extremely important. This rise necessitates to secure video by encryption algorithms [1],the most important challenges facing multimedia encryption are data size which is usually very large , real time applications which are need fast processing and the cost of encryption in terms of computation resource : The proportion of information in multimedia applications is very large but the quantity of information is small .

Classical encryption schemes are designed for encryption of textual (or numeric) data. In general, video data is huge (a frame can have 40, 000 bits and there would be 25-30 frames per second). The information value of video data is far less than that of an equal amount of text data. For secure, video data is encrypted by using classical algorithms (DES, AES, and RC5 etc.). But this causes delay in processing and is not suitable for real-time applications [1].

1.2 Problem statement

A variety of video encryption algorithms have been proposed to meet the specific requirements of visual communication privacy , these algorithms take long time for encoding which is not suitable for multimedia application. Also these algorithms were

mainly designed for textual encryption and therefore it would have been better to find a suitable algorithm for multimedia encryption.

1.3 Research Objective

The main objective of this research is to secure video using a proposed encryption method to provide data confidentially. Other Objective:

- i. Reduce video size
- ii. Increase video encoding speed.

1.4 Research Methodology

In this thesis the securing of Moving Picture Experts Group (MPEG-4) video is based on the use of elliptic curve cryptography for encryption key and line_ cut scrambling to scramble pixel of frames using random matrix after compression using Discrete Cosine Transform (DCT), to decrease video size.

1.5 Research Organization

Chapter two is the Theoretical Background beside the previous studies, chapter three Proposed Research Methodology and Tools, chapter four introduce Implementation of the system and the Result discussion, the last chapters include the Conclusion and Future Work.

Chapter two
Literature Review

chapter II

Literature Review and Related works

2.1 Introduction

This chapter provides brief overview about Multimedia, cryptography and video compression. The next part discusses some related studies in the field of video encryption.

2.2 Introduction to Multimedia

When different people mention the term multimedia, they often have quite different, or even opposing, viewpoints. Personal computer (PC) vendor would like us to think of multimedia as a PC that has sound capability, a DVD-ROM drive, and perhaps the superiority of multimedia-enabled microprocessors that understand additional multimedia instructions. A consumer entertainment vendor may think of multimedia as interactive cable television (TV) with hundreds of digital channels, or a cable-TV-like service delivered over a high-speed Internet connection. A computer science student likely has a more application-oriented view of what multimedia consists of: applications that use multiple modalities, including text, images, drawings (graphics), animation, video, sound including speech, and interactivity[2]. So the definition of multimedia is "concerns the representation of mixed modes of information – text, data, image, audio and video – as digital signals"[3].

2.3.1 History of Multimedia

A brief history of the use of multimedia to communicate ideas might begin with newspapers, which were perhaps the first mass communication medium, using text, graphics, and images. Motion pictures were originally conceived of in the 1830s to observe motion too rapid for perception by the human eye. Thomas Alva Edison 'commissioned the invention of a motion picture camera in 1887. Silent feature films appeared from 1910 to 1927; the silent era effectively ended with the release of the Jazz Singer in 1927. In 1895, Guglielmo Marconi sent his first wireless radio transmission at Polltechio, Italy. A few years later (1901), detected radio waves beamed across the Atlantic. Initially invented for

telegraph, radio is now a major medium for audio broadcasting. In 1909, Marconi shared the Nobel Prize for physics. (Reginald A. Fessenden, of Quebec, beat Marconi to human voice transmission by several years, but not all inventors receive due credit. Nevertheless, Fessenden was paid \$2.5 million in 1928 for his purloined patents.) Television was the new medium for the twentieth century. It established video as a commonly available medium and has since changed the world of mass communication. The connection between computers and ideas about multimedia covers what is actually only a short period [2]:

1960 Ted Nelson started the Xanadu project and coined the term "hypertext." Xanadu was the first attempt at a hypertext system - Nelson called it a "magic place of literary memory."

1967 Nicholas Negroponte formed the Architecture Machine Group at MIT.

1968 Douglas Engelbart, greatly influenced by Vannevar Bush's "As We May Think," demonstrated the "On-Line System" (NLS), another early hypertext program. Engelbart's group at Stanford Research Institute aimed at "augmentation, not automation," to enhance human abilities through computer technology. NLS consisted of such critical ideas as an outline editor for idea development, hypertext links, teleconferencing, word processing, and e-mail, and made use of the mouse pointing device, windowing software, and help systems[5].

1969 Nelson and van Dam at Brown University created an early hypertext editor called FRESS [6]. The present-day Intermedia project by the Institute for Research in Information and Scholarship (IRIS) at Brown is the descendant of that early system.

1976 The MIT Architecture Machine Group proposed a project entitled "Multiple Media". This resulted in the *Aspen Movie Map*, the first hypermedia videodisc, in 1978.

1985 Negroponte and Wiesner cofounded the MIT Media Lab, a leading research institution investigating digital video and multimedia.

1989 Tim Berners-Lee proposed the World Wide Web to the European Council for Nuclear Research (CERN).

1990 Kristina Hooper Woolsey headed the Apple Multimedia Lab, with a staff of 100. Education was a chief goal.

1991 MPEG-1 was approved as an international standard for digital video. Its further development led to newer standards, MPEG-2, MPEG-4, and further MPEGs, in the 1990s.

1991 The introduction of PDAs in 1991 began a new period in the use of computers in general and multimedia in particular. This development continued in 1996 with the marketing of the first PDA with no keyboard.

1992 JPEG was accepted as the international standard for digital image compression. Its further development has now led to the new JPEG2000 standard.

1992 The first Mbone audio multicast on the Net was made.

1993 The University of Illinois National Center for Supercomputing Applications produced NCSA Mosaic, the first full-fledged browser, launching a new era in Internet information access.

1994 Jim Clark and Marc Andreessen created the Netscape program.

1995 The JAVA language was created for platform-independent application development.

1996 DVD video was introduced; high-quality, full-length movies were distributed on a single disk. The DVD format promised to transform the music, gaming and computer industries.

1998 XML 1.0 was announced as a W3C Recommendation.

1998 Handheld MP3 devices first made inroads into consumer tastes in the fall, with the introduction of devices holding 32 MB of flash memory.

2000 World Wide Web(WWW) site was estimated at over 1 billion pages [7].

2.3.2 Types of Multimedia

- i. Linear active content progresses often without any navigational control for the viewer such as a cinema presentation[8].
- ii. Non-linear uses interactivity to control progress as with a video game or self-paced computer based training. Hypermedia is an example of non-linear content [8].

2.3.3 The Basic Elements of Multimedia

The basic elements of multimedia are four elements first text is characters that are used to create words, sentences, and paragraphs. Second graphics is a digital representation of non-text information, such as a drawing, chart, or photograph. Third animation is flipping through a series of still images. It is a series of graphics that create an illusion of motion; Audio is music, speech, or any other sound. And last video is photographic images that are

played back at speeds of 15 to 30 frames per second and that provide the appearance of full motion.

2.3 Image and Video Data

Digital visual data is usually organized in rectangular arrays denoted as frames, the elements of these arrays are denoted as pixels (picture elements). Each pixel is a numerical value, the magnitude of the value specifies the intensity of this pixel. The magnitude of the pixels varies within a predefined range which is classically denoted as “bit depth”, i.e. if the bit depth is 8 bit, the magnitude of the pixel varies between 0 and $2^8 - 1$ (8 bpp means 8 bits per pixel). Typical examples are binary images (i.e. black and white images) with 1 bpp only or gray value images with 8 bpp where the gray values vary between 0 and 255. Color is defined by using several frames, one for each color channel. The most prominent example is the RGB representation, where a full resolution frame is devoted to each of the colors red, green, and blue. Color representations closer to human perception differentiate among luminance and color channels (e.g. the YUV model). Video adds a temporal dimension to the purely spatially oriented image data. A video consists of single frames which are temporally ordered one after the others. A single video frame may again consist of several frames for different color channels.

2.4 Image Compression

The basic idea of compression is to exploit (in fact, remove) redundancy in data. Compression can be broken down into two broad categories. In lossless compression, from the compressed data one is able to reproduce the original data exactly. In lossy compression, the original data cannot be reproduced exactly. Rather allow some degradation in the reproduced data. In a sense, sampling and quantization can be considered as forms of compression. Sampling is lossless if sample above the Nyquist rate, and is lossy otherwise. Quantization is lossy compression. Clearly there is a tradeoff between the quality and amount of data. In sampling and quantization, the signal is converted from an analog to a digital signal. This “compression” has the dramatic effect of converting infinitely many samples each of which requires infinite precision to a finite number of

samples that each have finite precision[9] .There are many compression standard. As explained in the next paragraph.

2.4.1 JPEG

Stands for “Joint Photographic Experts Group ”. JPEG is a popular image file format. It is commonly used by digital cameras to store photos since it supports 2^{24} or 16,777,216 colors. The format also supports varying levels of compression, which makes it ideal for web graphics. The 16 million possible colors in a JPEG image are produced by using 8 bits for each color (red, green, and blue) in the RGB color space. This provides 2^8 or 256 values for each of the three colors, which combined allow for $256 \times 256 \times 256$ or 16,777,216 colors. Three values of 0 produce pure black, while three values of 255 create pure white.

The JPEG compression algorithm may reduce the file size of a bitmap (BMP) image by ten times with almost no degradation in quality. Still, the compression algorithm is lossy, meaning some image quality is lost during the compression process. For this reason, professional digital photographers often choose to capture images in a raw format so they can edit their photos in the highest quality possible. They typically export the pictures as JPEG (.JPG) images when they are shared or published on the web.

2.4.2 MPEG

Stands for “ Moving Picture Experts Group”. MPEG is an organization that develops standards for encoding digital audio and video. It works with the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) to ensure media compression standards are widely adopted and universally available.

The MPEG organization has produced a number of digital media standards since its inception in 1998. Examples: MPEG-1,MPEG_2 , MPEG-4, MPEG-7 and MPEG-DASH . MPEG compression is so ubiquitous that the term "MPEG" is commonly used to refer to a video file saved in an MPEG file format rather than the organization itself. These files usually have a ".mpg" or ".mpeg" file extension. And types of frame in MPEG-4 describe are following:

- i. 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”.
- ii. 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.
- iii. 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 propagates because it is not used as a reference frame to any other form.

2.4.3 DVI

Stands for "Digital Video Interface" . DVI is a video connection standard created by the Digital Display Working Group (DDWG). Most DVI ports support both analog and digital displays. If the display is analog, the DVI connection converts the digital signal to an analog signal. If the display is digital, no conversion is necessary.

2.5 JPEG Compression

Image compression going many stages describe as following :

2.5.1 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) attempts to decorrelate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency [10]. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain. JPEG makes use of transform coding techniques. Transform coding techniques compress the transform of a signal i.e. an image, and not the image directly. The DCT is the most commonly used transform technique for image coding [11].

The energy compaction property of the DCT results in transform coefficients with only a few of the coefficients having significant values, thus making it a popular technique. Each

color component of a continuous tone image can be represented as a series of amplitudes in the two dimensional space. The DCT is used to discard higher frequency information that has minimal visual effect on the image. The DCT is related to the Discrete Fourier Transform (DFT) but can approximate linear signals well with few coefficients.

An image consists of many pixels arranged in an $m \times n$ array. The first step in the Forward Discrete Cosine Transform (FDCT) transformation of the image is to divide the picture array into 8×8 blocks of pixels.

The size of the blocks has been chosen as a compromise of complexity and quality. If the number of rows or columns is not a multiple of 8, the closest multiple of 8 rows or columns is considered when dividing the image into 8×8 blocks. A comparison of the color data but not the intensity level of each pixel to its neighbors is performed [12].

The DCT produces large discrete coefficients for a pixel if the differences between the pixels are large. Otherwise, the differences are little, small DC coefficients are produced. The large amplitudes signify a large color difference. The pixels have thus been mapped from the spatial domain to the frequency domain.

This is in essence where the fundamental principle of JPEG lies, in eliminating the subtle color changes that the human eye cannot detect. In the frequency domain, this map to the smaller coefficients and thus these coefficients can be eliminated or rounded to zero. The data which contains the significant information is then retained by keeping the medium and larger coefficients [13].

Before computing the DCT of the 8×8 block, its values are shifted from a positive range to one centered around zero. For an 8-bit image, each entry in the original block falls in the range $[0, 255]$. The mid-point of the range (in this case, the value 128) is subtracted from each entry to produce a data range that is centered around zero, so that the modified range is $[-128, 127]$. This step reduces the dynamic range requirements in the DCT processing. In computing the DCT of each sub array, 64 DCT coefficients are generated. $F(0, 0)$ is known as the DC component and the remaining components are referred to as AC components

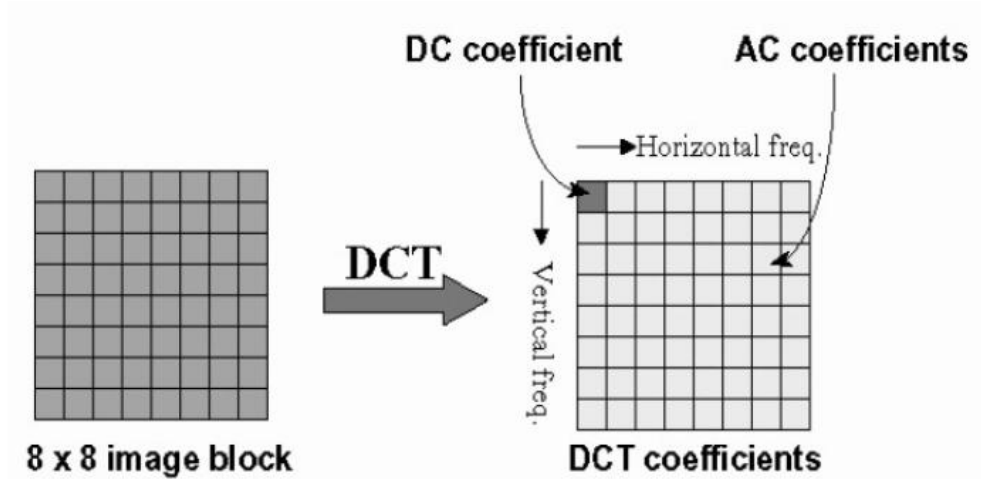


Figure 2. 1: DCT coefficients of 8x8 image block

2.5.1.1 DCT Properties

There are some properties of the DCT which are of particular value to image processing applications [10]. First decorrelation is the principle advantage of image transformation is the removal of redundancy between pixels. This leads to uncorrelated transform coefficients which can be encoded independently. Second energy compaction efficacy of a transformation scheme can be directly gauged by its ability to pack input data into as few coefficients as possible. This allows the quantization to discard coefficients with relatively small amplitudes without introducing visual distortion in the reconstructed image. DCT exhibits excellent energy compaction for highly correlated images

2.5.2 Quantization

In digital signal processing, quantization is the process of approximating a continuous range of values (or a very large set of possible discrete values) by a relatively-small set of discrete symbols or integer values.

A common use of quantization is in the conversion of a discrete signal (a sampled continuous signal) into a digital signal by quantizing. Both of these steps (sampling and quantizing) are performed in analog-to-digital converters with the quantization level

specified in bits. A specific example would be compact disc (CD) audio which is sampled at 44,100 Hz and quantized with 16 bits (2 bytes) which can be one of 65,536 (i.e. 2¹⁶) possible values per sample.

2.5.3 Entropy Encoding

Entropy coding is a reversible mapping from one data representation to another more compact representation. In picture and video coding applications and standards the original source data are first mapped onto so-called coding symbols such as motion vectors and transform coefficient levels and these coding symbols are then entropy coded. The entropy coding stage of today coding applications and standards is dominated by Huffman coding and arithmetic coding [14].

In information theory an entropy encoding is a lossless data compression scheme that is independent of the specific characteristics of the medium. One of the main types of entropy coding creates and assigns a unique prefix-free code to each unique symbol that occurs in the input. These entropy encoders then compress data by replacing each fixed-length input symbol with the corresponding variable-length prefix-free output codeword. The length of each codeword is approximately proportional to the negative logarithm of the probability. Therefore, the most common symbols use the shortest codes [15].

2.5.3.1 Coding Techniques

There are many Coding Techniques describe as following :

i. Huffman Coding

In computer science and information theory, a Huffman code is a particular type of optimal prefix code that is commonly used for lossless data compression [15].

ii. Arithmetic coding

Arithmetic coding is a data compression technique that encodes data (the data string) by creating a code string which represents a fractional value on the number line between (0) and (1). The coding algorithm is symbol wise recursive; i.e., it operates upon and encodes (decodes) one data symbol per iteration or recursion. On each recursion, the algorithm successively partitions an interval of the number line between 0 and 1, and retains one of the partitions as the new interval. Thus, the algorithm successively deals with smaller

intervals, and the code string, viewed as a magnitude, lies in each of the nested intervals. The data string is recovered by using magnitude comparisons on the code string to recreate how the encoder must have successively partitioned and retained each nested subinterval. Arithmetic coding differs considerably from the more familiar compression coding techniques, such as prefix (Huffman) codes. Also, it should not be confused with error control coding, whose object is to detect and correct errors in computer operations [16].

iii. Unary coding

Unary coding, sometimes called thermometer code, is an entropy encoding that represents a natural number, n , with n ones followed by a zero (if natural number is understood as non-negative integer) or with $n - 1$ ones followed by a zero (if natural number is understood as strictly positive integer). For example 5 is represented as 111110 or 11110. Some representations use n or $n - 1$ zeros followed by a one. The ones and zeros are interchangeable without loss of generality. Unary coding is both a Prefix-free code and a Self-synchronizing code [15].

2.6 Cryptography

Cryptography is the ability to send information between participants, in a mangled format, that prevents others from reading it. In the late 20th century, this picture of cryptography radically changed. study of cryptography- as a science.[17]

2.6.1 Types of Cryptographic Algorithms

The three types of cryptographic algorithms, conventional, Public key cryptography and Hash Functions.

2.6.1.1 Conventional cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the U.S. government and Advanced Encryption Standard (AES) NIST initially selected Rijndael in October 2000 and formal adoption as the AES standard came in December 2001. The following figure is an illustration of the conventional encryption process.

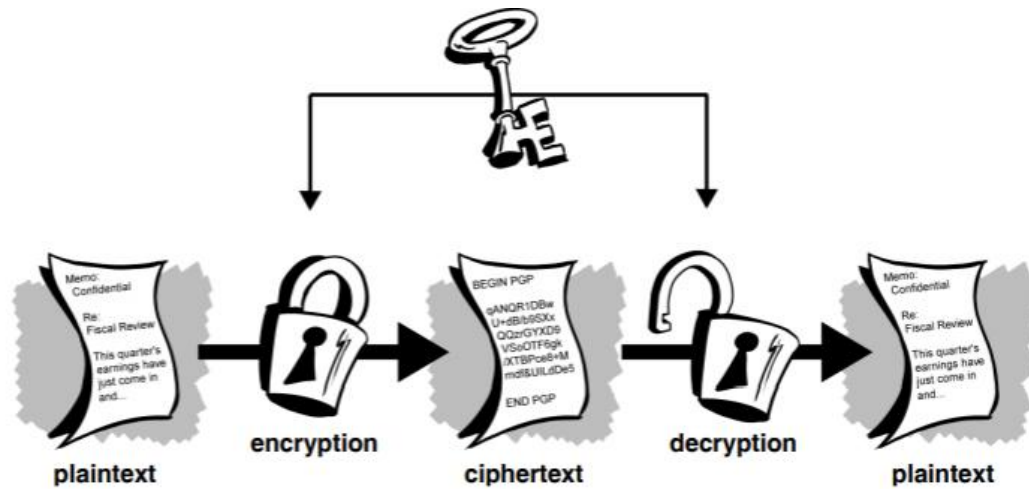


Figure 2. 2 : symmetric-key encryption

Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution [18].

2.6.1.2 Public Key Cryptography

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. (There is now evidence that the British Secret Service invented it a few years before Diffie and Hellman, but kept it a military secret—and did nothing with it.)[17]

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private key (secret key) for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information. The following figure is an illustration of the public key encryption process.

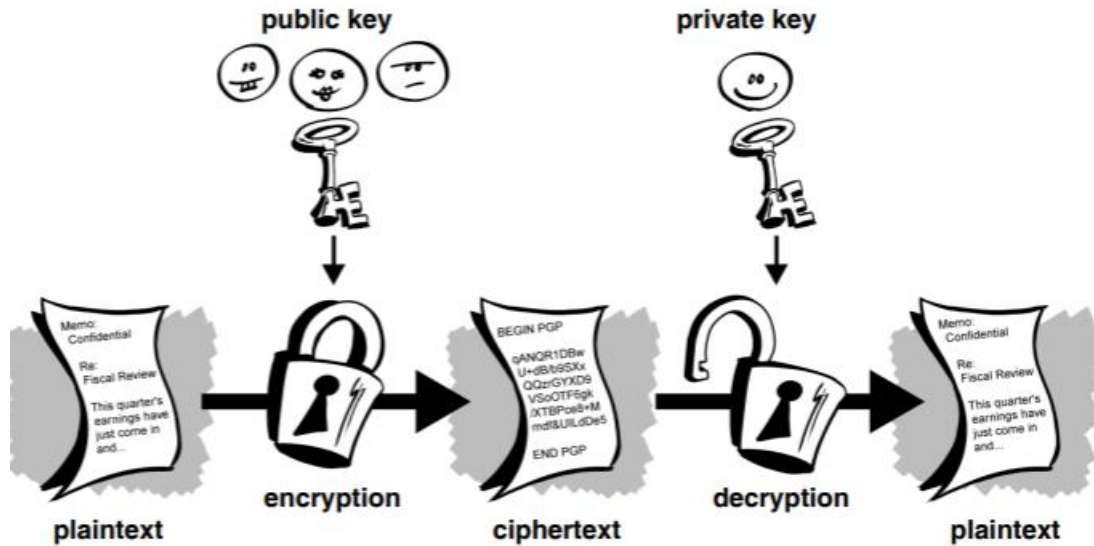


Figure 2. 3 : public key cryptography

The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal, RSA, Diffie-Hellman, and DSA, the Digital Signature Algorithm. Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings). Public-key encryption is the technological revolution that provides strong cryptography to the adult masses. Remember the courier with the locked briefcase handcuffed to his wrist? Public-key encryption puts him out of business (probably to his relief).

2.6.1.3 Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also

commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file[18]. The Message Digest (MD) algorithms is an example of Hash functions cryptosystem .The MD is a series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. and Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value and was originally published as FIPS 180-1 and RFC 3174. FIPS 180-2 (aka SHA-2) [19]. The following figure is an illustration of the Hash Function process.

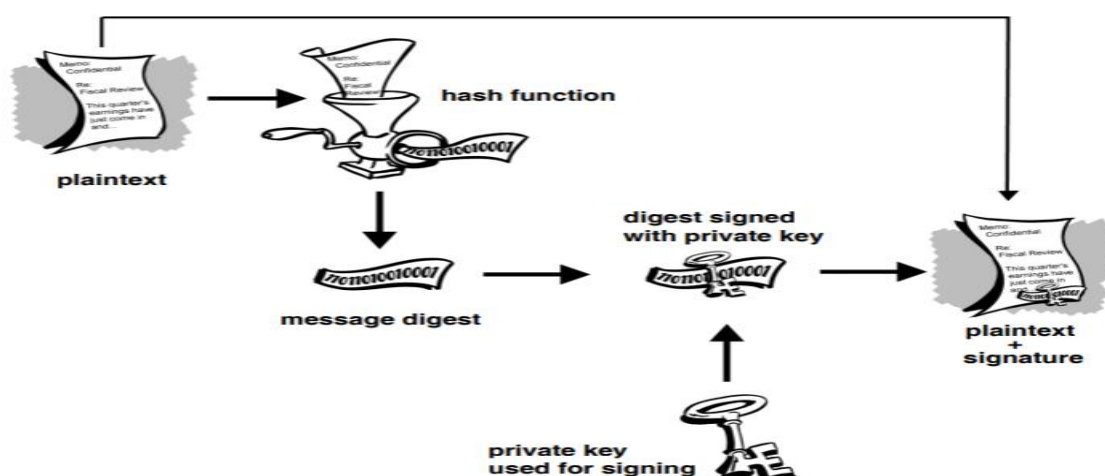


Figure 2. 4 : Hash Function process

2.7 Elliptic Curve Cryptography (ECC)

Elliptic curves (EC) were suggested for cryptography by Victor Miller [20] and Neal Koblitz [21] in 1985 in the form of Elliptic Curve Cryptography (ECC). ECC follows Public Key encryption technique and the security provided is based on the hardness of Discrete Logarithm Problem (DLP) and since then, a lot amount of work has been done on Elliptic Curve Cryptography. One main advantage of ECC is that similar level of security can be achieved with considerably smaller keys size. Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. In ECC it is normally to start with an affine point called $P_m(x,y)$. These points may be the Base point (G) itself or some other point closer to the Base point. Base point

implies has the smallest (x ,y) co-ordinates, which satisfy the EC. Today, RSA is the powerhouse crypto security of choice for E-commerce transaction. The RSA is too slow compared to ECC because ECC required smaller key size. The IT connectivity provides will be able to utilize fewer crypto-server securities for providing secure network connections [22]. Table 1 compares the security level for some commonly considered crypto-graphics Key size.

Table 2. 1 : Comparison of the equivalent security levels using cryptographic key sizes.

RSA/DSA key Size	ECC key size	RSA/ECC key size ratio
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

In Elliptic Curve Cryptography, the curve equation of the form certain formula is defined for operation with the points.

$$y^2 = x^3 + a x + b \quad (2-1)$$

Which is known as weierstrass equation, where a and b are the constant with

$$4a^3 + 27b^2 = 0 \quad (2-2)$$

2.7.1 Mathematics in elliptic curve cryptography over finite field

Cryptographic operations on elliptic curve over finite field are done using the coordinate points of the elliptic curve. Elliptic curve over finite field equation is given by:

$$y^2 = [23] \text{ mod } p \quad (2-3)$$

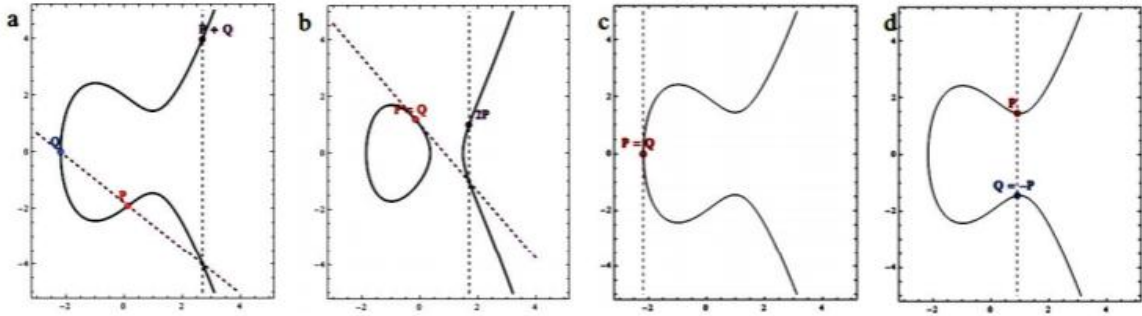


Figure 2. 5 : (a) Point addition; (b) Point doubling; (c) Point at infinity when y coordinates are both 0; (d) Point at infinity when the coordinates are mirror image of each other. And will be explained as follows:

2.7.1.1 Point addition

The two point $P(x_1, y_1)$ and $Q(x_2, y_2)$ are distinct. $P + Q = R(x_3, y_3)$ is given by the following calculation. Figure 1(a) shows graphical representation of Point Addition operation.

$$x_3 = [24] \text{ mod } p \quad (2-4)$$

$$y_3 = \{\lambda(x_1 - x_3) - y_1\} \text{ mod } p \quad (2-5)$$

Where

$$\lambda = y_2 - y_1 / x_2 - x_1 \text{ mod } p \quad (2-6)$$

2.7.1.2 Point Doubling

The two point $P(x_1, y_1)$ and $Q(x_1, y_1)$ overlap. $P + Q = R(x_3, y_3)$ is given by the following calculation. Figure 1(b) shows graphical representation of Point Doubling operation.

$$X_3 = \{\lambda^2 - 2x_1\} \quad \text{mod } p \quad (2-7)$$

$$y_3 = \{\lambda(x_1 - x_3) - y_1\} \quad \text{mod } p \quad (2-8)$$

Where

$$\lambda = 3x_1^2 + a / 2y_1 \quad \text{mod } p \quad (2-9)$$

2.7.1.3 Point multiplication

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition. $kP = P + P + P + \dots + k$ times.

2.7.1.4 Point at Infinity

If $x_1 = x_2$ and $y_1 = y_2 = 0$ or $x_1 = x_2$ and $y_1 = -y_2$, the points is said to intersect at infinity denoted by O. Figure 1(c) and 1(d) shows graphical representation of Point at Infinity.

2.7.1.5 Finding Inverse Modulo

Let us consider an elliptic curve

$$y^2 = x^3 + 2x + 4 \quad \text{mod } 7 \quad (2-10)$$

It has got the following coordinate points. $\{O, \{0, 2\}, \{0, 5\}, \{1, 0\}, \{2, 3\}, \{2, 4\}, \{3, 3\}, \{3, 4\}, \{6, 1\}, \{6, 6\}\}$.

To perform point addition of two points $\{0, 5\}$ and $\{3, 4\}$, it need to find lambda.

$$\lambda = 4 - 5 / 3 - 0 \quad \text{mod } 7 \quad (2-11)$$

$$\lambda = -1 / 3 \quad \text{mod } 7 \quad (2-12)$$

Since ECC is a public key cryptography, we require a public key and a private key. Consider Alice and Bob are the two communicating parties. They agree upon a common Elliptic curve equation and a generator G. Let Alice and Bob private keys be n_A and n_B respectively. Alice and Bob public keys are given by

$$P_A = nAG \quad (2-13)$$

And

$$P_B = nBG \quad (2-14)$$

Respectively . If Alice want to send a message ‘P_m’ to Bob, Alice uses Bob’s public key to encrypt the message. The cipher text is given by

$$P_C = \{kG, P_m + k P_b\} \quad (2-15)$$

Where ‘k’ is a random integer. The random ‘k’ make sure that even for a same message the cipher text generated is different each time. This gives a hard time for someone who is illegally trying to decrypt the message. Bob decrypts the message by subtracting the coordinate of ‘kG’ multiplied by nB from ‘P_m + kP_b’.

$$P_m = \{P_m + k P_b - nBkG\} \quad (2-16)$$

Here multiplied does not mean simple multiplication that we do in algebra, rather it is multiple addition of points using the point addition method stated above in point multiplication. As the multiplier nB is the secret key of Bob, only Bob can decrypt the message sent by Alice [25].

2.8 Multimedia Compression and Encryption

The process of multimedia compression and encryption is associative. There are three ways to combine encryption algorithms with compression as shown in Figure (2-5). The encryption algorithm can be applied before, within or after the multimedia compression [26]. The encryption algorithms that work jointly with the compression algorithms are called joint compression and encryption algorithms, whereas the algorithms that work independently of the compression algorithms are called compression-independent encryption algorithms. In joint compression and encryption algorithms, encryption is performed during compression; it can be within or after transformation [27], quantization

[28] or entropy coding [29]. On the other hand, in compression-independent encryption algorithms, encryption can be before compression [30] or after compression [31].

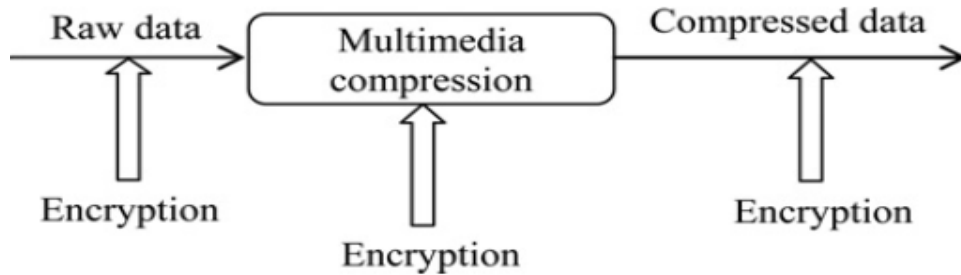


Figure 2. 6 : possible positions of multimedia encryption algorithms

2.8.1 Requirements of multimedia encryption

Multimedia communication has distinguished characteristics such as rich of information, real-time play out, standard compression codec and formats. These peculiarities create several levels of security according to the application requirements. The requirements of multimedia encryption should be considered when designing a cryptographic algorithm. They include compression efficiency, encryption efficiency, codec compliance and security level [26].

2.8.2 Classification of Video Encryption Algorithms

There are many types of video encryption methods the first fully layered encryption in this class, whole content of video and then using standard algorithms like AES and DES encryption. The disadvantage of this method is that it is not suitable for real-time video encryption because there is heavy computation required and the speed is also slow.

Secondly scrambling based encryption the algorithm in this category mainly uses different permutation algorithms to scramble and encrypt the content of video. Scrambling means re-positioning of pixels and not changing its value. In this encryption method, security is low, speed is fast but it is vulnerable to known-plaintext attack.

Third selective encryption the video encryption algorithm in this kind of encryption selects only the needed bytes in the video frames and then encrypts it. The computational capacity

lowers to a great degree because every single byte of video content is not required to be encrypted. Selective encryption algorithm is fast but encryption ratio is low.

Four perceptual encryption the quality of video is partially degraded in perceptual encryption. The low quality video observed in many pirated videos is due to perceptual encryption. Perceptual encryption is not secure against known-chosen plaintext attack.

Five chaotic encryption the chaos based video encryption is best suited for real-time video encryption because of low computational complexity, format-complaint, invariance of compression ratio, real-time, strong transmission error tolerance, multiple levels of security and hence, it is superior over other conventional encryption methods[12].

2.9 Related Works

Brief studies of related work in the area of video encryption is presented in this section.

- i. Narsimha Raju et.al.[1] Proposed a computationally efficient and secure video encryption algorithm and achieved computational efficiency by exploiting the frequently occurring patterns in the DCT coefficients of the video data. Using RC5 algorithm, ECB mode and MPEG video. It succeeds in using text-based algorithms for videos by managing the computational overhead and hence suiting real-time applications. The security level provided is as good as security provided by RC5 or DES, It is selective, i.e., based on the criticality level of the DCT coefficient, the algorithm adjusts to provide optimum security (like CBC mode for DC coefficients), The algorithm succeeds in exploiting the statistical properties of the video for providing better encryption speed. The drawback of these algorithms was used textual encryption and is least secure because the ECB mode of encryption is less secure than all.
- ii. Ghada Mohammed Taher Al – Dabbagh et.al.[32] proposed random scrambling algorithm Which is based on the principle of random scrambling image pixel To reduce the huge calculations and time spent in the encryption and decryption by Read video file information and convert frames to images while reading audio

information if found in the video file, Calculate the image dimensions of each frame and then convert the image data to unsigned 8-bit integer and calculate the sound matrix dimensions, Generate the key used to encrypt images frames while generating the private key for audio encoding and scrambling the image pixels through the use of keys that have been generated. The drawback of these algorithms It is not safe enough because only the encrypted file gets distorted and used textual encryption.

- iii. Fuwen Liu et.al.[33] proposed the video encryption algorithm called puzzle. The Puzzle algorithm was inspired by the children game jigsaw puzzle that splits an entire picture into many small pieces and places them in disorder and it consists of two encryption steps: Puzzling the compressed video data of each frame and Obscuring the puzzled video data. Puzzle inherently makes no impairment on the compression efficiency and is easily to integrate into available multimedia applications Puzzle achieves a sufficiently fast encryption speed to meet the real-time requirements of mostly used multimedia applications, especially for high resolution video streams. It provides a significant increase in the encryption speed compared to the widely used naive algorithm approaches. But this algorithm does not handle all types of cryptanalytic attacks and Complex in the encryption phase.
- iv. Lo'ai Tawalbeh et.al.[20]. They applied ECC to do selective encryption and perceptual encryption along with multimedia compression, and study its effect on the multimedia encryption requirements. Two ECC-based encryption algorithms have been presented: selective encryption of the quantized DCT coefficients and perceptual encryption based on selective bit-plane encryption. The results of applying the ECC-based algorithms showed that ECC has the potential to be used for multimedia encryption; it can meet the real-time constraints of multimedia applications and does not affect the compressed data size. But in this paper it was applied algorithm to encrypt images only.
- v. Giradkar et.al.[23]. Proposed privacy preserving for encrypted media is new topic for growing research field. The used RC4 encryption scheme facilitates the way of encrypting video directly on the compressed domain. RC4 algorithm generates the key stream which is pseudorandom in nature. This Pseudorandom key stream makes

cryptanalytic attacks more difficult. Our research performs encryption of a compressed video stream and thus it preserves the compression & decompression time cycle. Means there is no requirement to encrypt video before compression & if it is already compressed then it is not required to decompress that video for encryption.

- vi. Dr.Abdul-Wahab et.al.[24]. 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.

Chapter Three
Research Methodology

Chapter III

Research Methodology and Tools

3.1 Introduction

This chapter explores the conducted methodology in this work. In the naive approach for video encryption, the MPEG stream (bit sequence) is treated as text data, and encrypted using standard encryption algorithms like Data Encryption Standard (DES), Rivest Cipher (RC5), and Advanced Encryption Standard (AES) etc. Though this approach is supposedly the most secure for video encryption, it is computationally infeasible for real-time applications. Arguing that the full content of the video is not critical. Selective encryption algorithms these methods encrypt a selected portion of the video data (for example headers of the video streams, I frames and I-blocks in P and B frames, I frames and motion vectors in P and B frames, etc.) using text-based encryption algorithms. This decreases encryption time. For real-time applications, light-weight encryption algorithms. In this work scrambling encryption is used for encryption video using elliptic curve cryptography.

3.2 Proposed Work

The main idea is based on the DCT for compression of the frames to decreasing size of frames and then encryption process is applied using elliptic curve cryptography and line _cut scrambling for securing video

3.3 Algorithm of Encryption and Decryption

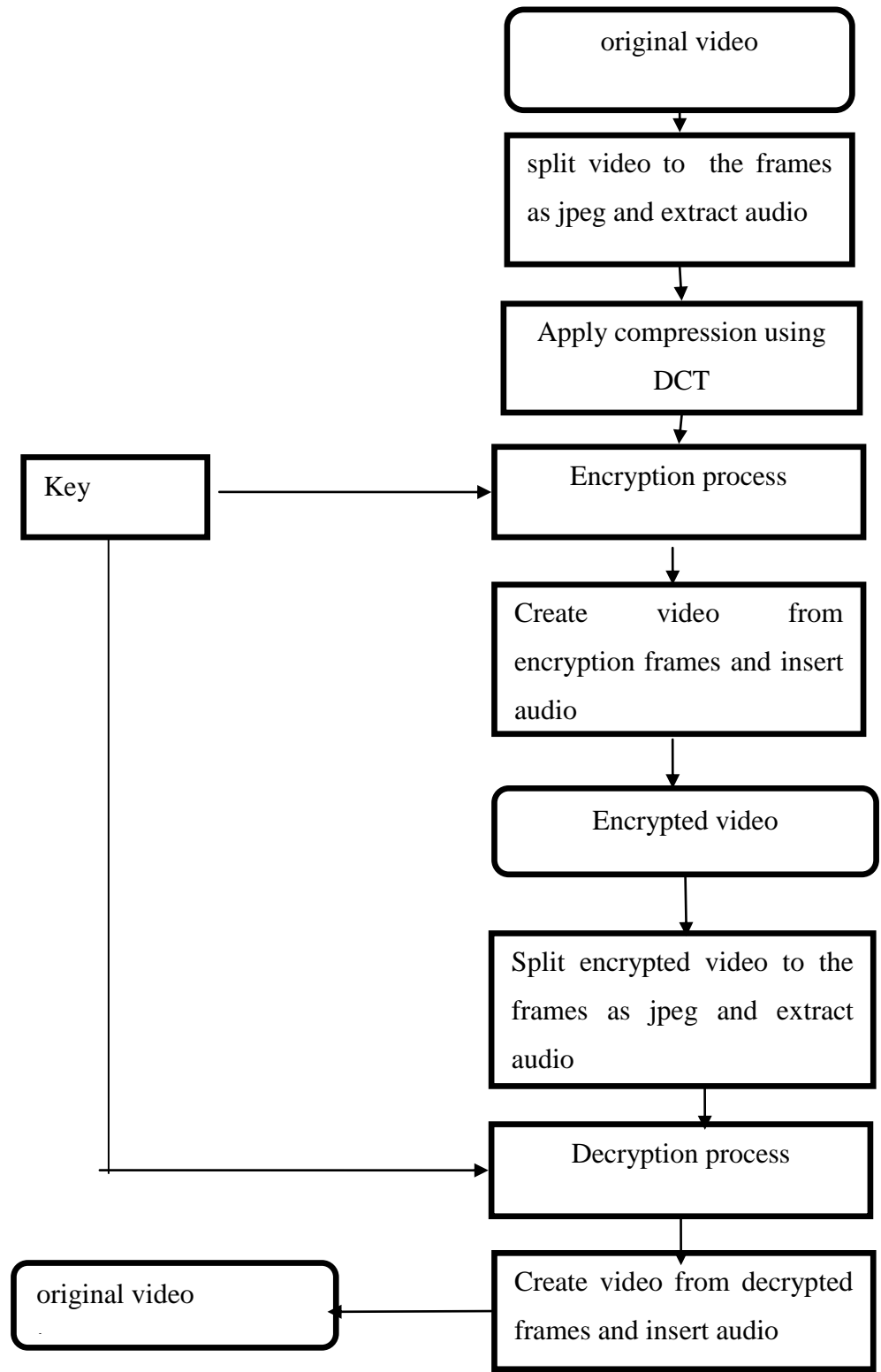


Figure 3. 1 : Block Diagram for Encryption and Decryption

The previous figure describes steps of compression, encryption and decryption process in this research. The steps as a following

Step one: split video into frames as a jpg formatting and extract audio.

Step two: after split video into frames applied DCT .Computing the DCT of the 8×8 block, its values are shifted from a positive range to one centered around zero. For an 8-bit image, each entry in the original block falls in the range [0,255].

Step three: calculate key using elliptic curve cryptography for encryption and decryption process. To calculate the key the first will find and plot all the points on a specific prime curve takes as its inputs, A, B and p and produces two vectors X, Y which contain all the points (x, y) that lie on

$$y^2 = x^3 + Ax + B \pmod{p} \quad (3-1)$$

Second performs the successive doubling algorithm over prime curves takes as its inputs X1, Y 1, k and outputs X2, Y 2

Where $(X2, Y 2) = k(X1, Y 1) = (X1, Y 1) + (X1, Y 1) + \dots + (X1, Y 1)$ (k summands) and addition is performed over the elliptic curve

$$y^2 = x^3 + Ax + B \pmod{p} \quad (3-1)$$

Finally using those points in previous step to create key by multiply last points in the curve modular the large prime number under the row dimension of frame.

Step four: encryption process using line _cut scrambling. Scrambling method each scan line is cut into pieces and re-collected in a varied series.

For example, if a line like 0123456789 Passes the encoder, the output might look like 4567890123 Which every line in the video frames cuts from different points and these cut points are created from a random matrix .

Step five: create video from encryption frame and insert audio in video

Step six: spilt encryption video into frames as jpg formatting and extract audio.

Step seven: decryption process by to find the inverse

Step eight: create video from decryption frames and insert audio.

3.4 Tools

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB stands for Matrix Laboratory, is a complete programming environment that encompasses its own programming language, integrated development environment (IDE), libraries (called toolboxes in MATLAB).

Chapter Four
Implementation & Results

Chapter IV

Implementation and Results

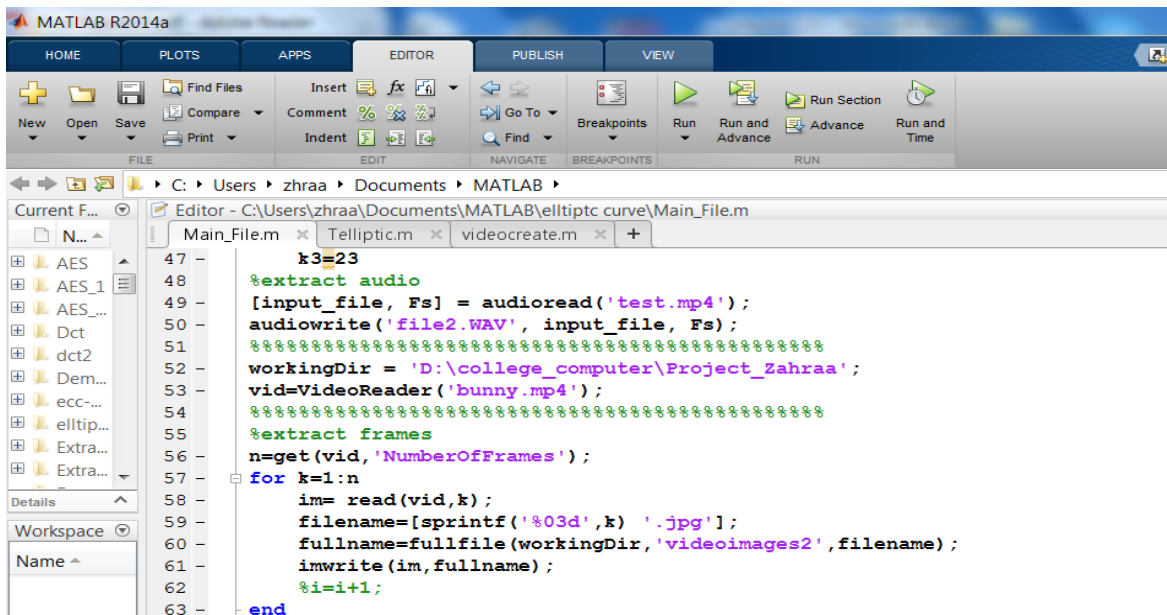
4.1 Introduction

In the previous chapter the details of the proposed method were described and how to perform encryption operations. This chapter shows the implementation of the model in term of a computer program. A detailed description of how the program works by making a number of experiments as well as presenting the final results from the program operation.

4.2 The Implementation

The implementation process was done by using MATLAB language, the MATLAB code is divided into five different parts, each part serving on step of the methodology implementation, the implementation steps are:

Step1: Reading the original video, extract the audio from video in a WAV file, and converting the video into stream of images, shown in figures (4.1) and (4.2)



```
47 - k3=23
48 - %extract audio
49 - [input_file, Fs] = audioread('test.mp4');
50 - audiowrite('file2.WAV', input_file, Fs);
51 - %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
52 - workingDir = 'D:\college_computer\Project_Zahraa';
53 - vid=VideoReader('bunny.mp4');
54 - %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
55 - %extract frames
56 - n=get(vid, 'NumberOfFrames');
57 - for k=1:n
58 -     im= read(vid,k);
59 -     filename=[sprintf('%03d',k) '.jpg'];
60 -     fullname=fullfile(workingDir, 'videoimages2', filename);
61 -     imwrite(im, fullname);
62 -     %i=i+1;
63 - end
```

Figure 4. 1 : Extract frame and audio from video



a) original video



b) extracted frame

Figure 4. 2 : Example of original video and extracted frame

Step2: applying DCT compression on extracted frames. As shown in figure (4.3) and (4.4).

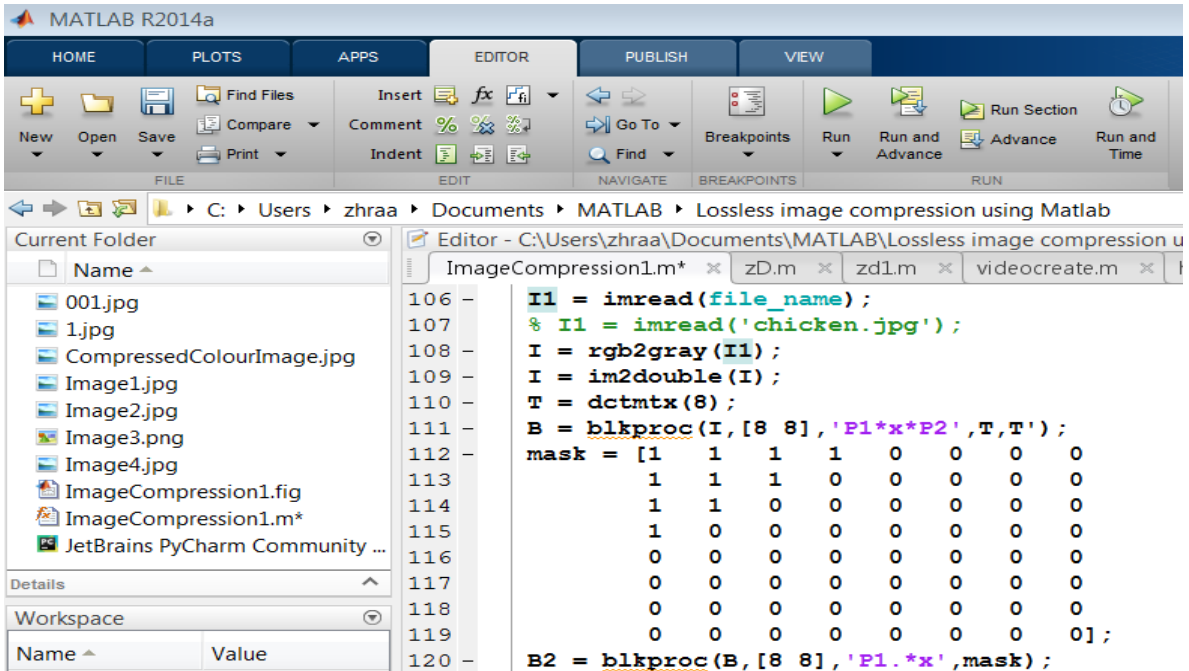


Figure 4. 3 : Image compression

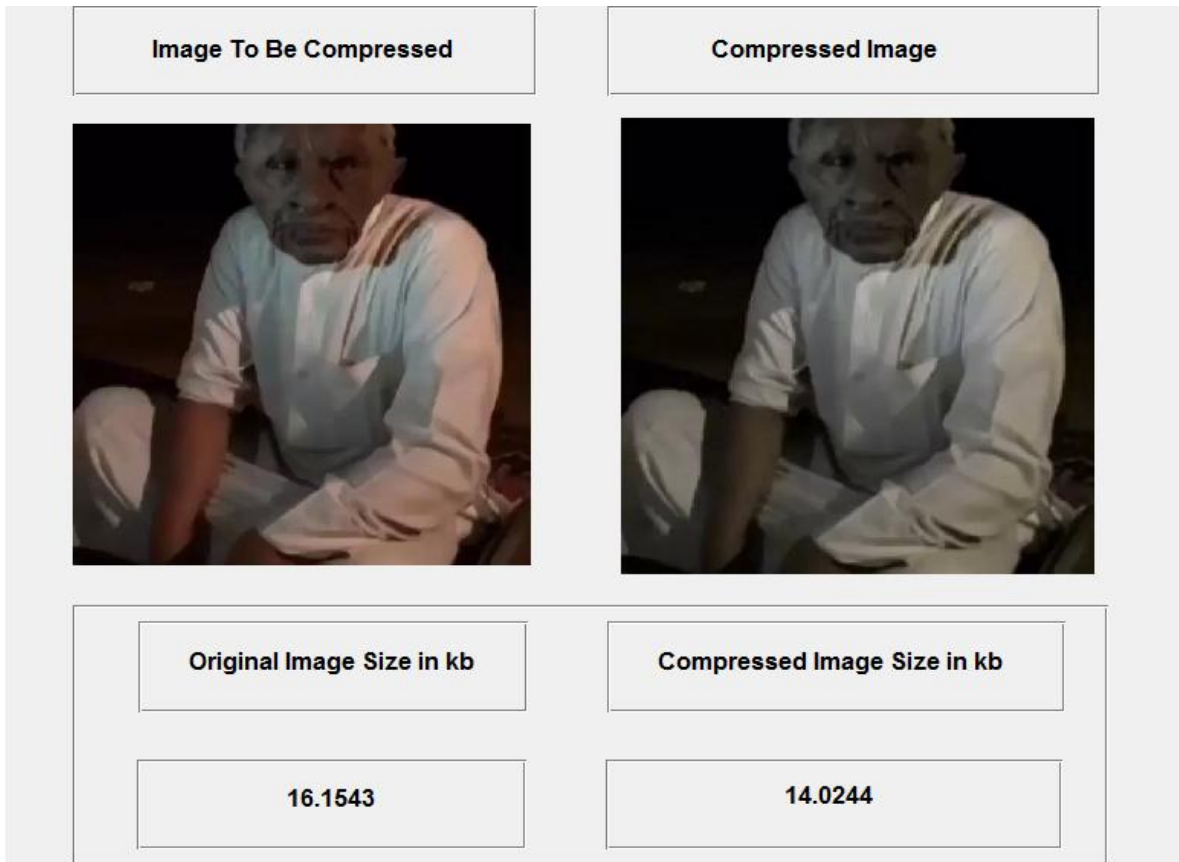


Figure 4. 4 : Example for image compression

Step3: Calculate the key using point of elliptic curve after the find all plots in the curve and select two point. Shown in figure (4.5) .

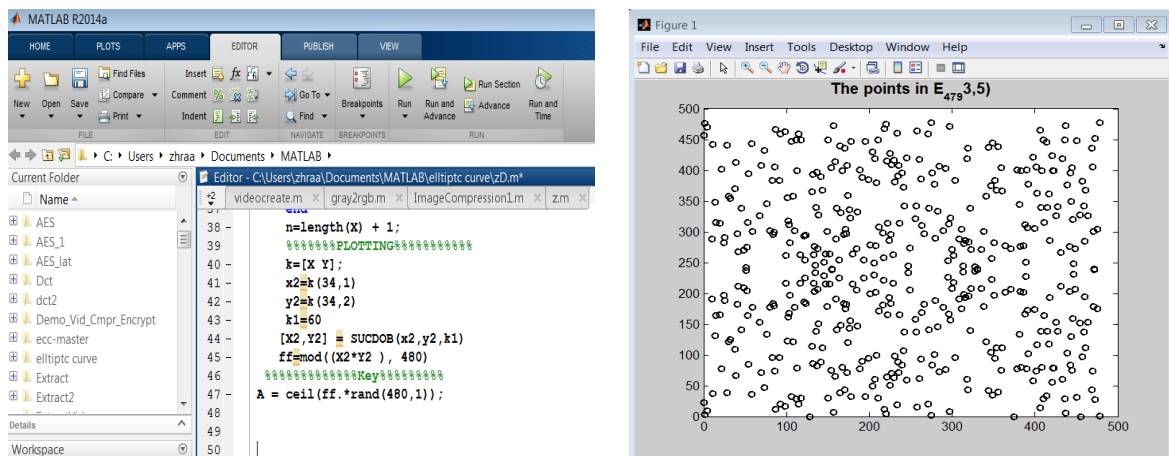


Figure 4. 5 : plots in curve and calculate the ke

Step4: Encryption process using line _cut scrambling, shown in figure (4.6)

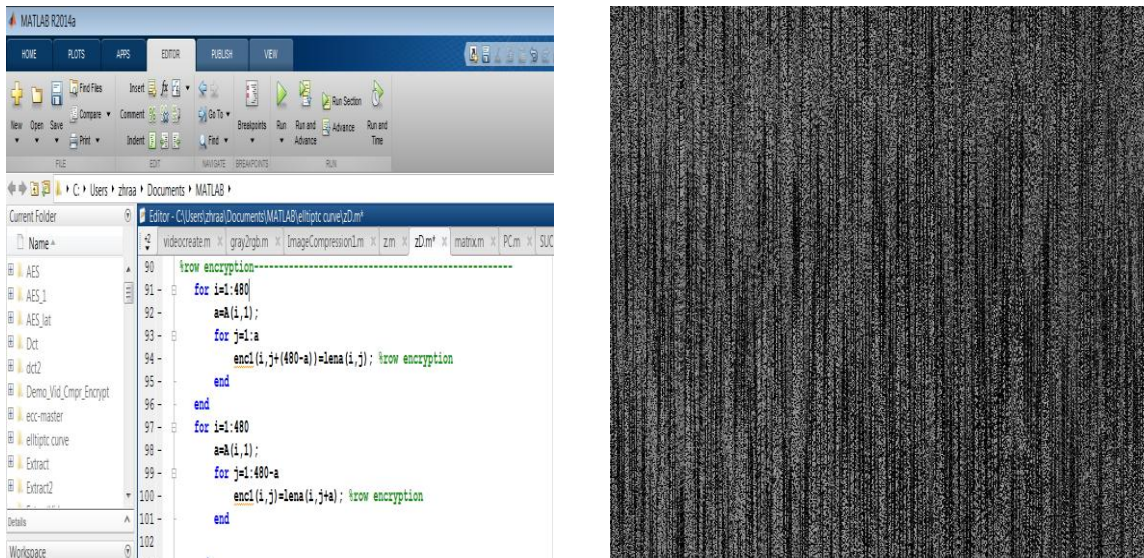


Figure 4. 6 : Encryption process

Step5: Convert the frames into video, shown in figures (4-7) and (4-8);

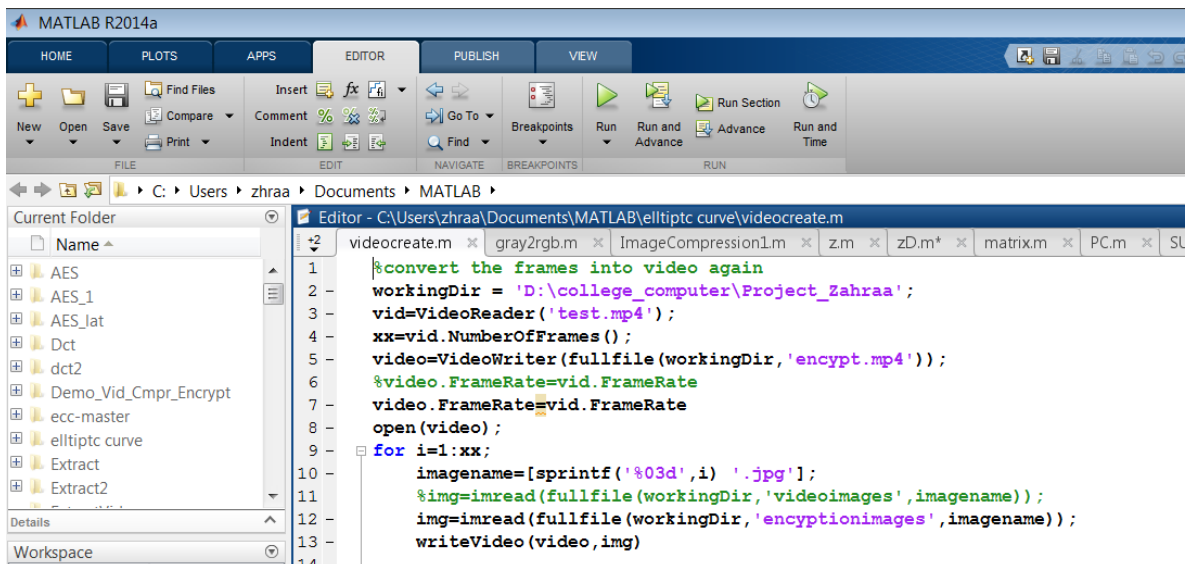


Figure 4. 7 : Convert frames into video

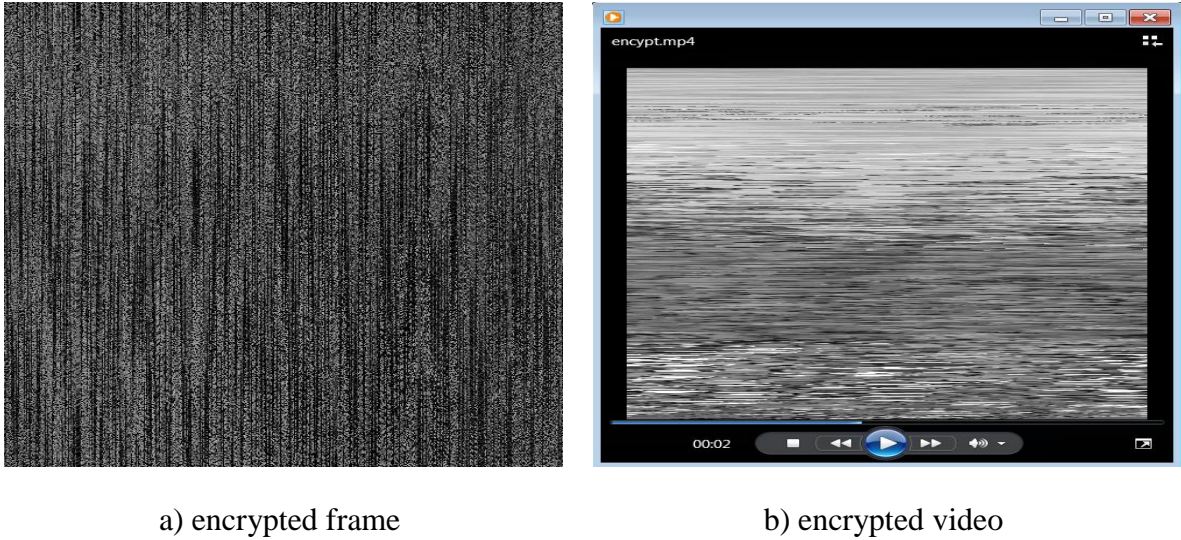


Figure 4. 8 : Example of convert frames into video

4.3 Quality Measurement and Evaluation

4.3.1 Mean Square Error (MSE):

The Mean Square Error is obtained by calculating the average squared difference between a original frame and a modified frame (encrypted frame). It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count, MSE is calculated using equation (4-1):

$$\text{MSE}(f, g) = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (f_{ij} - g_{ij})^2 \quad (4-1)$$

Where, MSE is Mean Square error, H and W are height width and $f(i, j)$ represents original frame and $g(i, j)$ represents corresponding encrypted frame.

4.3.2 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio is most commonly used as a measure of the quality of reconstruction for lossy compression. It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. A higher PSNR would normally indicate that the reconstruction is of higher quality. A small

value of PSNR indicates poor quality; the PSNR is calculated using equation (4-2):

$$\text{PSNR}(f, g) = 10 \log_{10} (255^2 / \text{MSE}(f, g)) \quad (4-2)$$

PSNR is peak signal to noise ratio, L is peak signal level of an image and MSE is calculated in the previous equation.

4.3.3 Histogram

A histogram is a plot that lets discover, and show, the underlying frequency distribution of a set of continuous data. This allows the inspection of the data for its underlying distribution (e.g., normal distribution), outliers, etc. An example of a histogram, and the raw data it was constructed from.

4.4 Experimental Results

To evaluate the performance of the proposed method, different MPEG-4 videos were tasted, each video was different in size, display time, frame per seconds and data rate, the characteristics of each video are shown in table(4-1):

Table 4. 1 : characteristics of the tested video

File name	File Size	Length	Frames /Sec	Data rate (kbps)	Frame height	Frame width	Number of frames
Video-1	0.525MB	00:00:05	29	738	480	480	169
Video-2	0.246MB	00:00:03	23	502	360	640	92
Video-3	15.1MB	00:05:39	25	243	240	426	8484
Video-4	6.78MB	00:01:35	29	367	720	1280	3388
Video-5	1.80MB	00:00:15	25	873	1080	1920	375

4.5 1-Result of quality analysis

To evaluate the quality of this work, used the objective fidelity criteria measurements (peak signal to noise ratio (PSNR)), (mean square error (MSE)), PSNR and MSE are tested between the original video and the encrypted video as shown on table (4.2) and figures (4.9) and (4.10). The histogram of the original and encrypted video in shown in figure (4.9) the figure also show that the frames could be recover correctly.

Table 4. 2 : objective fidelity criteria (PSNR, MSE) for the tested videos

File name	File Size	PSNR	MSE
Video-1	0.525MB	55.1082	0.2006
Video-2	0.246MB	56.7260	0.1382
Video-3	15.1MB	54.0203	0.2577
Video-4	6.78MB	63.6844	0.0278
Video-5	1.80MB	60.5201	0.0577

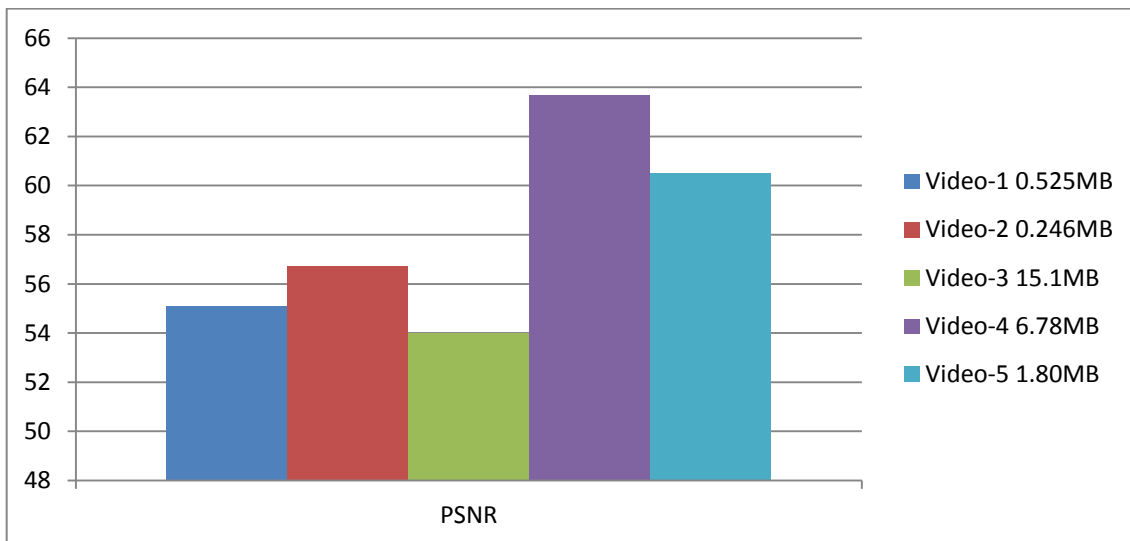


Figure 4. 10 : Result of PSNR

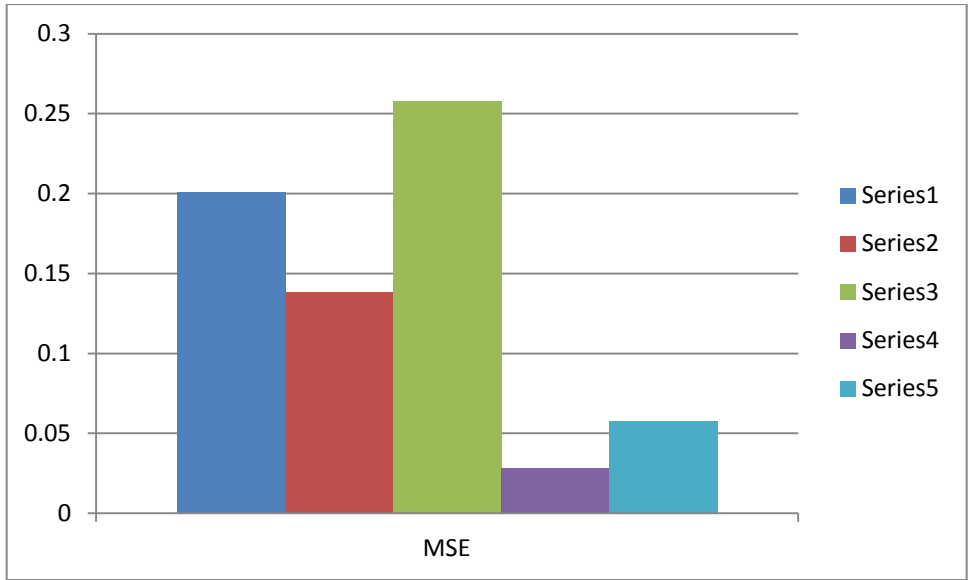
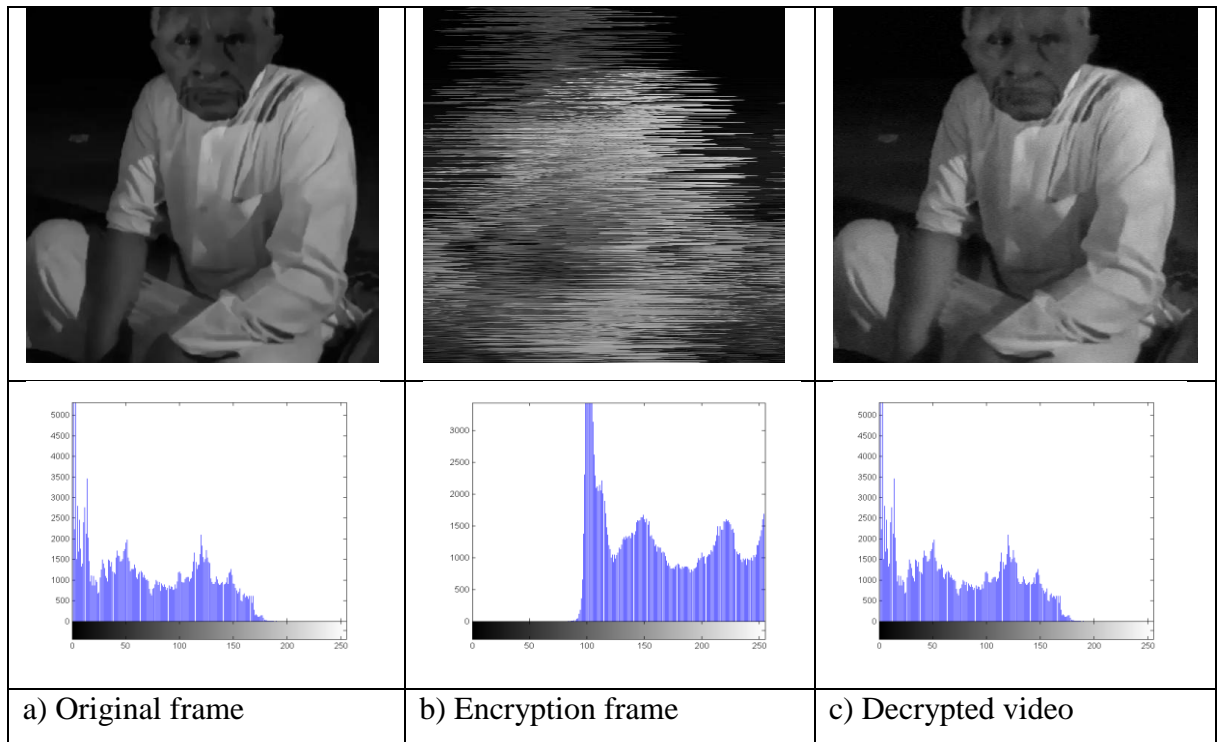


Figure 4. 11 : Result of MSE

The results of peak signal to noise ratio (PSNR) ranging between(54.0203 and 60.5201) and the mean square error (MSE) ranging between(0.0278 and 0.2006) from this result show reasonable destroyed of the visual data.



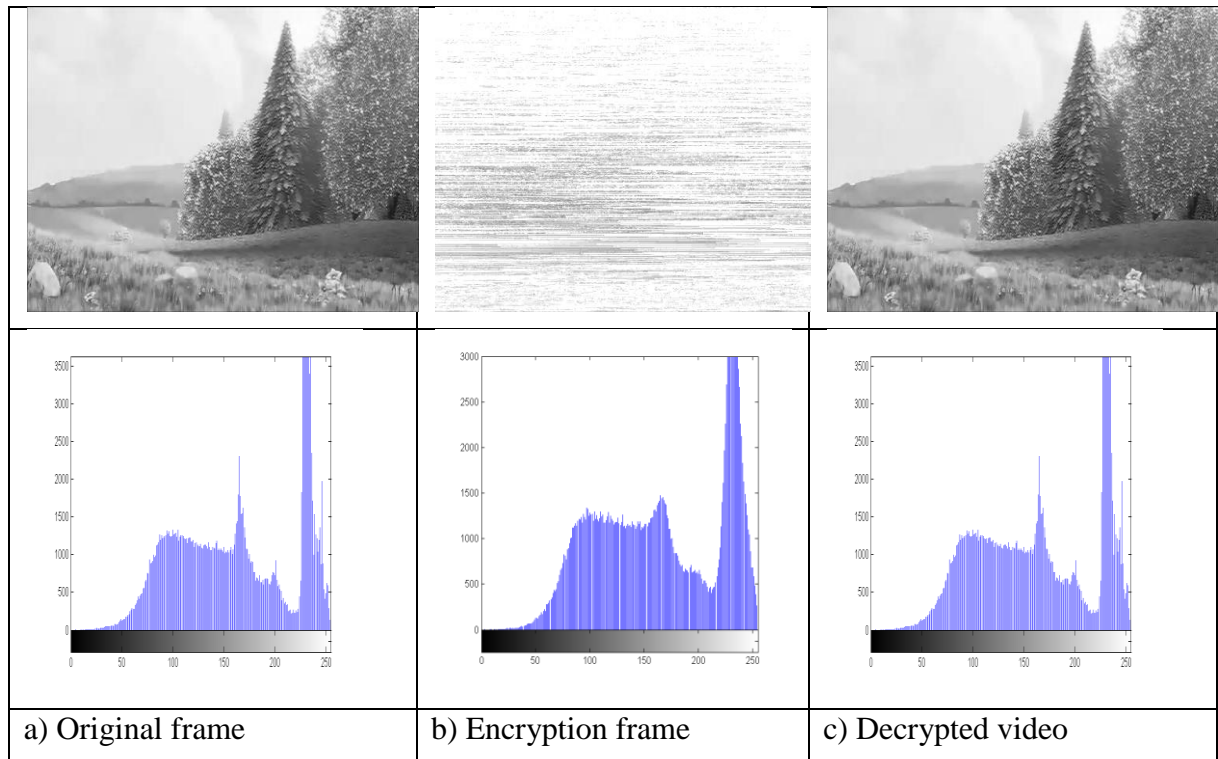


Figure 4. 12 : shows some of the original and encrypted of tested video and the histogram of each one.

4.6 Result of execution time

The execution time of encryption shown in the table (4.3) and figure (4.12).

Table 4. 3 : Execution Time

File name	File Size	Encryption time of one frame in sec	Decryption time of one frame in sec	Average Time
Video-1	0.525MB	0.166	0.046	0.106
Video-2	0.246MB	0.621	0.027	0.321
Video-3	15.1MB	0.126	0.004	0.065
Video-4	6.78MB	0.274	0.070	0.172
Video-5	1.80MB	0.423	0.104	0.263

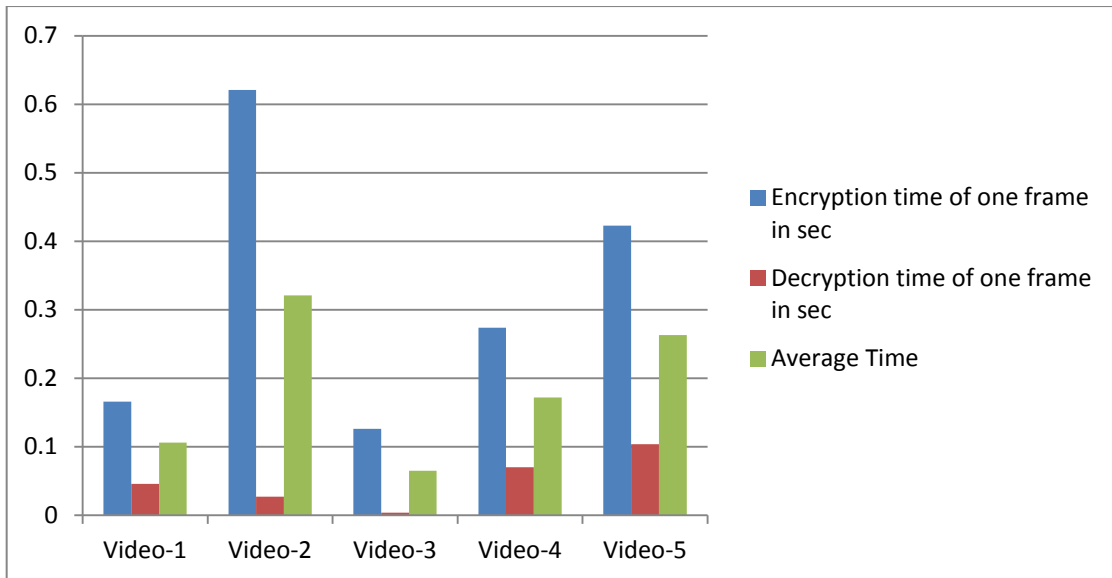


Figure 4. 13 : Results of the execution time

Chapter Five
Conclusion & Future Work

Chapter V

Conclusion and Future Work

5.1 Conclusion

The encryption algorithms developed to secure text data are not suitable for multimedia application because of the large data size in real time constraint. This research, introduces elliptic curve cryptography with line _cut scrambling for video encryption after compression by DCT. Used ECC for encryption key generation , the encryption key done by select the points in curve and prime number under the demission of frame and multiply in the random matrix and scrambles the lines of the image. This takes less time to encrypt the video than other encryption method like (AES, DEA etc) so can be used in real time applications and It supplies a proper video signal, gives an amount of obscurity in great quality, as well as good decode quality and steadiness. The proposed method is implemented on MATLAB.

5.2Future work

This study can provide the base for several future researches, the following points are suggested for further study:

1. Encrypted RGB color video
2. Using elliptic curve for audio encryption.

Reference:

- [1] C. N. Raju, G. Umadevi, K. Srinathan, and C. Jawahar, "Fast and secure real-time video encryption," in *Computer Vision, Graphics & Image Processing, 2008. ICVGIP'08. Sixth Indian Conference on*, 2008, pp. 257-264.
- [2] Z.-N. Li, M. S. Drew, and J. Liu, *Fundamentals of multimedia*: Springer, 2004.
- [3] F. F. Kuo, W. Effelsberg, and J. J. Garcia-Luna-Aceves, *Multimedia communications protocols and applications*: Prentice-Hall, Inc., 1997.
- [4] G. Lu, *Multimedia database management systems*: Boston, MA: Artech House, 1999.
- [5] N. J. Castellan, *Individual and group decision making: current issues*: Psychology Press, 2013.
- [6] N. Yankelovich, N. K. Meyrowitz, and A. v. Dam, "Reading and writing the electronic book," *IEEE computer*, vol. 18, pp. 15-30, 1985.
- [7] Z.-N. Li, M. S. Drew, and J. Liu, : Springer, 2004.
- [8] I. Petelycky, M. Harris, S. Northmore, G. Elliot, D. Staheli, J. Smith, *et al.*, "Non-timeline, non-linear digital multimedia composition method and system," ed: Google Patents, 2001.
- [9] P. Billingsley, *Ergodic theory and information* vol. 1: Wiley New York, 1965.
- [10] S. A. Khayam, "The discrete cosine transform (DCT): theory and application," *Michigan State University*, vol. 114, 2003.
- [11] P. Yip and C. Patrick, *Discrete cosine transform: algorithms, advantages, applications*: Boston; Toronto: Academic Press, 1990.
- [12] P. G. Howard and J. S. Vitter, "New methods for lossless image compression using arithmetic coding," *Information processing & management*, vol. 28, pp. 765-779, 1992.
- [13] W. Pennebaker and J. M. J. S. I. Data, "Compression Standard," *New York, NY, Vanl Nostrand Reinhold I*, vol. 993, 1993.
- [14] D. Marpe, H. Schwarz, and T. Wiegand, "Entropy coding in video compression using probability interval partitioning," in *Picture Coding Symposium (PCS), 2010*, 2010, pp. 66-69.
- [15] S. Kaur and S. Singh, "Entropy Coding and Different Coding Techniques," *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org*, vol. 6, 2016.
- [16] G. G. Langdon, "An introduction to arithmetic coding," *IBM Journal of Research and Development*, vol. 28, pp. 135-149, 1984.
- [17] J. Ellis, "The possibility of non-secret digital encryption," ed: Technical report, CESG Report, 1970.
- [18] G. C. Kessler, "An Overview of Cryptography," 2010.
- [19] G. C. Kessler, "An overview of cryptography," *published by Auerbach*, vol. 22, 1998.
- [20] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, 1985, pp. 417-426.
- [21] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, pp. 203-209, 1987.
- [22] R. Singh, R. Chauhan, V. K. Gunjan, and P. Singh, "Implementation of Elliptic Curve Cryptography for Audio Based Application," *International Journal of Engineering*, vol. 3, 2014.
- [23] S. S. Giradkar and A. Bhattacharya, "Securing compressed video streams using RC4 encryption scheme," in *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 640-644.

- [24] R. S. Shaker and A.-W. S. Ibrahim, "partial MPEG-4 video encryption schema using RC6 algorithm," *Iraqi Journal of Information Technology*, vol. 7, pp. 47-62, 2015.
- [25] L. D. Singh and K. M. Singh, "Implementation of text encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 73-82, 2015.
- [26] F. Liu and H. Koenig, "A survey of video encryption algorithms," *computers & security*, vol. 29, pp. 3-15, 2010.
- [27] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Transactions on Multimedia*, vol. 5, pp. 118-129, 2003.
- [28] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, pp. 214-223, 2007.
- [29] C.-P. Wu and C.-C. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, pp. 828-839, 2005.
- [30] D. Socek, S. Magliveras, D. Čulibrk, O. Marques, H. Kalva, and B. Furht, "Digital video encryption algorithms based on correlation-preserving permutations," *EURASIP Journal on Information Security*, vol. 2007, p. 10, 2007.
- [31] L. a. Tawalbeh, M. Mowafi, and W. Aljoby, "Use of elliptic curve cryptography for multimedia encryption," *IET Information Security*, vol. 7, pp. 67-74, 2013.
- [32] غ. م. ط. الدباغ. "استخدام البعثة العشوائية في تشفير الوسائط المتعددة," *مجلة الرافدين لعلوم الحاسوب والرياضيات*, vol. 10, pp. 209-225, 2013.
- [33] F. Liu and H. Koenig, "Puzzle-an efficient, compression independent video encryption algorithm," *Multimedia tools and applications*, vol. 73, pp. 715-735, 2014.