

Bachelor Thesis

Degree Program: Information Technology

Specialisation: Information Technology

2016

Kshitij Bhetwal

MULTIMEDIA SECURITY USING ENCRYPTION AND DECRYPTION



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

KSHITIJ BHEWAL

MULTIMEDIA SECURITY USING ENCRYPTION AND DECRYPTION

The importance of multimedia security is becoming more and more important with the continuous increment in digital communication on the internet. The increasing use of audio and video in a wide range of application security and privacy issues to serious attention.

With the advancement of both computer and internet technology, multimedia data, such as images, audio, videos, are being used more and more widely. In order to maintain privacy or security, sensitive data needs to be protected before transmission or distribution. In this thesis, we examine how the Rijndael algorithm helps to protect multimedia content by encrypting multimedia data.

The main focus of this thesis is to research the current methods of multimedia security, their main properties and reflect on the future of multimedia security.

CONTENTS

FIGURES AND TABLES	5
LIST OF ABBREVIATIONS	6
1 INTRODUCTION	7
2 MULTIMEDIA SECURITY	8
2.1 Entity Authentication	9
2.2 Message Authentication	9
3 CRYPTOGRAPHY	10
3.1 Symmetric Key Cryptosystems	11
3.2 Public Key Cryptosystems	12
4 RIJNDAEL ALGORITHM	13
5 HISTORY OF MULTIMEDIA SECURITY	15
5.1 Rijndael History	17
5.1.1 Algebraic Properties	18
5.1.2 Finite Field	18
5.1.3 Euclidean Algorithm	18
5.1.4 Finite Field Arithmetic	19
5.2 Algorithm Specification	19
5.2.1 Rijndael Byte and State	19
5.2.2 The Rounds	20
5.2.2.1 Byte Substitution	20
5.2.2.2 Shift Rows	21
5.2.2.3 Mix Columns	22
5.2.2.4 Add Round Keys	22
5.2.3 Key Schedule	23
6 COMPARISON OF AES AND DES	24
7 CLASSIFICATION OF CRYPTOGRAPHY TECHNIQUES	26
7.1 Optical Encryption	26
7.2 Selective Encryption	26
7.3 Chaotic Encryption	28
Mixing Property	28
Robust Chaos	28
Parameter Set	28

7.4 NonChaotic Encryption	29
8 VARIOUS METHODS	30
8.1 JPEG Encryption	31
8.2 SCAN	32
8.3 Hash Function	33
8.4 Visual Cryptography	33
9 SECURITY ANALYSIS	35
9.1 Exhaustive Key Search	35
9.2 Key Sensitive Analysis	35
9.3 Histogram Analysis	36
9.4 Information Entropy Test	36
9.5 UACI and NPCR Test	37
9.6 Correlation Coefficient Analysis	38
CONCLUSION	39
REFERENCES	40

LIST OF FIGURES

Figure 1. Symmetric Encryption	11
Source: Performance Analysis of Data Encryption Algorithms, Abdel-Karim Al Tamimi	
Figure 2. Asymmetric Encryption	12
Source: Performance Analysis of Data Encryption Algorithms, Abdel-Karim Al Tamimi	
Figure 3. Outline of Rijndael Operation	14
Source: Description of the Advanced Encryption Standard, Roger Fischlin	
Figure 4. Byte Substitution	21
Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001	
Figure 5. Transform Matrix of S-column	21
Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001	
Figure 6. Transform Matrix of Mix Column	22
Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001	
Figure 7. Transform Matrix of AddRoundKeys	22
Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001	
Figure 8. Selective Encryption Mechanism	27
Source: http://www.telecom.ulg.ac.be/publi/publications/mvd/sps-2004/	
Figure 9. Jpeg Encryption Example	31
Source: http://202.38.64.11/~whli/lab/imse.html	
Figure 10. Scan Image Example	32
Source: http://ethesis.nitrkl.ac.in/6456/1/E-57.pdf	
Figure 11. Visual Cryptography Example	34
Source: http://citeseerx.ist.psu.edu/viewdoc10.1.1.457.50771&type=pdf	

LIST OF TABLES

Table 1. Comparison between AES and DES	24
Source: Milind Mathur, Ayush. "COMPARISON BETWEEN DES, 3DES, RC2, RC6, BLOWFISH AND AES." on New Horizons in IT - NCNHIT 2013	

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
PDA	Personal Digital Assistant
FIPS	Federal Information Processing Standard
NIST	National Institute of Standard and Technology
GCD	Greatest Common Divisor
DCT	Discrete Cosine Transform
RGB	Red Green Blue
LSIC	Large Scale Integrated Circuit
SE	Selective Encryption
CFB	Cipher Feedback
NPCR	Number Of Pixels Change Rate
UACI	Unified Average Changing Intensity

1 INTRODUCTION

Multimedia data security is becoming increasingly important along with the increase of digital form of communication on the internet. The use of a wide range of images and videos in various types of application brings huge attention towards security and privacy issues nowadays. Multimedia data encryption helps to prevent unwanted and unauthorized disclosure of confidential information in transit or storage.

With respect to multimedia information security, there are three major objectives of cryptography i.e. confidentiality, data integrity, and authentication. Although the AES and Rijndael encryption algorithms are used interchangeably, they still have only one difference, the range of supported values and cipher key length. Rijndael is a block cipher having both a variable block and a key length. The block length and the key length can be specified independently as long as it is a multiple of 32 bits and has a value between 128 and 256 bits. Although the version of Rijndael can be defined to have a larger block or key length, it is not likely to be required right now. While the AES fixes the block length of 128 bits and the only key lengths supported are 128, 192, and 256 [1]. The extra block and the key length in Rijndael were not taken into consideration during the AES selection, so they are also not used in the current FIPS standard.

With the advancement of both computer and internet technology, the use of multimedia data is increasing fast. So the need of securing sensitive data before it is transmitted or distributed is high. So, in this thesis, the Rijndael algorithm, which helps to protect the multimedia content by encryption method, is studied and a theoretical report is written based on the studied material.

2 MULTIMEDIA SECURITY

Almost all digital services, such as online-TV, video conferencing, governmental (medical, military) digital services, require strong security in storage and transmission of data (audio/video). In the rapidly growing digital world of today, the internet has been growing at a tremendous speed so the security of the data has become more and more vital. As of the recent years, more and more consumer electronic services (mobile and PDA) have also started to add the functionality of storing and exchanging multimedia messages [2].

Due to the advancement of technology in our society digital images and videos are playing a major role than just plain and simple text, thus demanding a serious protection of user privacy. In order to make everything secure, the encryption of audio and video is very important as it helps to minimize malicious attacks from unauthorized parties. The recent advancement in science and technology, mainly in the computer and communication industry, allows potentially a huge market for distributing digital multimedia content through the internet. However, the rapid increase of digital document, multimedia processing tools and the availability of internet access throughout the world have given birth to a perfect environment for copyright fraud and uncontrollable distribution of multimedia content. One of the major challenges currently is the protection of intellectual content in multimedia networks.

In order to deal with the technical challenges, there are two major security technologies being developed:

1. Multimedia encryption technology providing end-to-end security while the digital content is being distributed over a huge number of distribution systems.

2. Watermarking technology is being used to prevent copyright fraud, ownership trace, and authentication.

Confidentiality means protecting of personal information from unauthorized access. An unwanted party known as adversary should not be able to access the material. Data integrity makes sure that the information has not been tampered in any kind of unwanted way. Therefore, the authentication methods are being studied in two groups:

2.1 Entity Authentication

Entity authentication makes sure that the receiver of the message receives both the identity of the sender and his active participation during the transmission time.

2.2 Message Authentication

Message authentication provides verification of the identity of the message sender. It also holds all evidence of data integrity if it is modified during the transmission period, then the sender is not the originator of the message.

3 CRYPTOGRAPHY

Cryptography is an important tool for the protection of multimedia content. All the multimedia files are encrypted before being distributed over the internet. Due to the encryption of the file, it is useless to all the persons who do not have access to the keys. So the key for the decryption of the content should not be disclosed to anyone else other than the content provider.

Encryption is a way to protect information from unwanted attacks by changing it into a form that cannot be recognized by any attackers. Data encryption mainly is changing of the data, such as text, image, audio, etc. so that it is unreadable, invisible or impenetrable during the transmission. So in order to recover the original data the receiver just inverses data encryption known as data decryption.

The encryption process can be described as $C = E (P, K)$

Where, P = Original data

E = Encryption Algorithm

K = Encryption Key

C= Cipher message, which is transmitted and can be subject to attack

The decryption procedure can be described as $P= D (C, K)$

Where, C = Cipher message; D= Decryption Algorithm

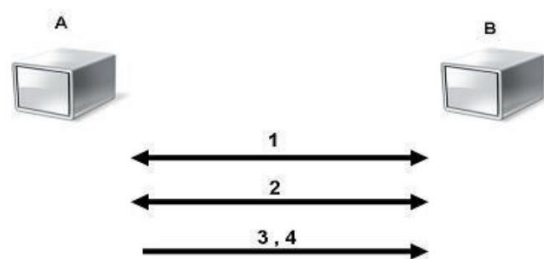
K= Decryption Key; P= Recovered data

3.1 Symmetric key cryptosystems

All the classical cryptosystems that were developed before 1970 are an example of symmetric key cryptosystems. Besides that, most of the cryptosystems developed after 1970 are symmetric [3]. Some of the very popular examples of modern symmetric key include:

1. AES (Advanced Encryption Standard)
2. DES (Data Encryption Standard)

All symmetric keys have a common interest, they depend on a secret shared between communicating parties. The secret can be used as both encryption and decryption key. The disadvantage of symmetric key is that it is not able to handle a large network of communication. On the other hand, the symmetric key requires a smaller size for the same level of security as public key cryptosystems, thus, making the communication faster and memory required smaller.



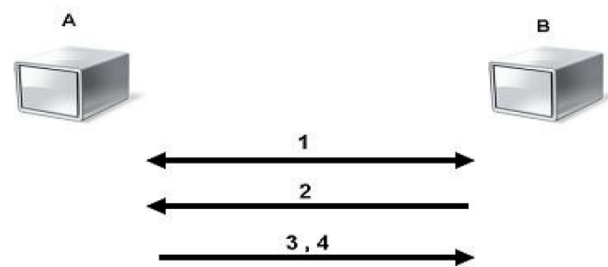
1. A and B agree on cryptosystems.
2. A and B agree on the key to be used.
3. A encrypts message using the shared key.
4. B decrypts the cipher message using the shared key.

Figure 1. Symmetric Encryption

(Source: Performance Analysis of Data Encryption Algorithms, Abdel-Karim Al Tamimi)

3.2 Public key cryptosystems

In this type of cryptosystems, there are two separate keys: a public key, which is known publicly and the secret key, which is only known to the owner. This type of system is known as 'asymmetric' for the reason of using a different key for decryption and encryption (the public and private key). The data is encrypted using a public key and it can be only decrypted using the private key.



1. A and B agree on cryptosystems.
2. B sends its public key to A.
3. A encrypts the message using the negotiated cipher and B's public key.
4. B decrypts the cipher message using its private key and the negotiated cipher.

Figure 2. Asymmetric Encryption

(Source: Performance Analysis of Data Encryption Algorithms, Abdel-Karim Al Tamimi)

4 RIJNDAEL ALGORITHM

The Rijndael algorithm has been selected by the U.S. National Institute of Standards and Technology (NIST) as a proposed AES algorithm. This algorithm was designed by two Belgian cryptologists, namely Dr. Vincent Rijmen and Dr. Joan Daemen. Rijndael is a block cipher, which are the common form of a private key algorithm [4]. The main reasons for NIST to select this algorithm are:

1. The symmetric and parallel structure
2. It gives implementers a lot of flexibility
3. It has not allowed effective cryptanalytic attacks
4. It is well adapted to modern processors
5. Pentium
6. RISC and parallel processors
7. They are suited for Smart cards
8. It is flexible for dedicated hardware

In addition to these reasons, the algorithm can be implemented in a very efficient way on a wide number of processors and hardware. Compared with others, it has a short encryption and decryption time and provides the best performance for both hardware and software being used.

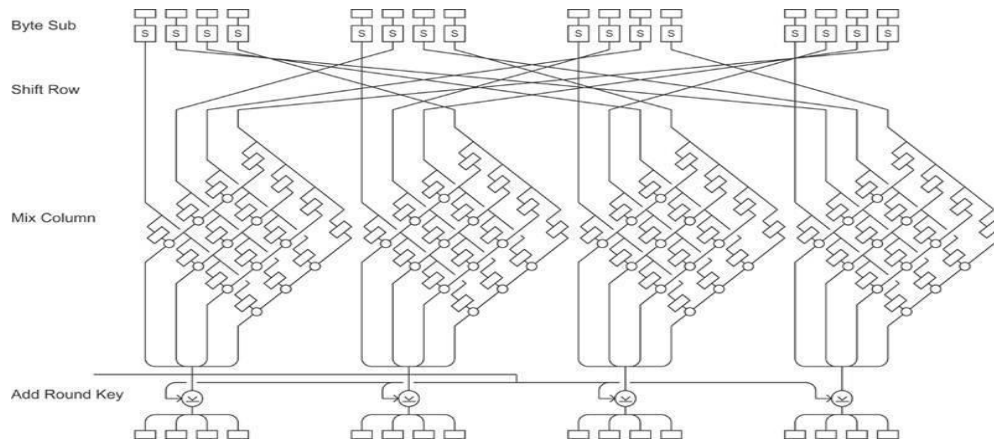


Figure 3. Outline of Rijndael operation

(Source: Description of the Advanced Encryption Standard, Roger Fischlin)

5 HISTORY OF MULTIMEDIA ENCRYPTION

Multimedia encryption technology was first introduced in 1980 and became a hot topic for research during the mid-90s. Its development can be categorized into three stages; raw data encryption, compressed data encryption, and partial encryption.

Before the 90s, only a few multimedia encoding methods were standardized. Most multimedia data (image, video) were transmitted or stored in raw form. Multimedia encryption was mainly based on permutation or scrambling of pixel, i.e., the video/image is modified so that the resulting data is incomprehensible. For example, space-filling curves are used to modify the image/video data, which hence confuses the relation between neighbouring images/video pixels. European TV networks use the Eurocrypt standard to encrypt the signals, which modifies the field line by line. [5] These methods are used for the reason of having low computing complexity and cost. Nevertheless, this type of modification changes the relation between neighbouring pixels, making compression operation not work. Therefore, these encryption algorithms are only useful for an application that does not require compression.

During the early 1990s, with the advancement of multimedia technology, some image and audio/video encoding standards were developed such as JPEG, MPEG, etc. Generally, these types of multimedia data are compressed before being stored or transmitted making raw data encryption not suitable for this application.

After the advancement of internet technology during late 1990, a multimedia application created required more real-time operation and interaction. By only encrypting certain parts of the data, the size of the final encrypted file can be reduced improving the encryption efficiency. Due to the rapid growth of the

network, the advancement in information security becomes vital in order to protect the secrecy and privacy. Encryption algorithms play a vital role in information security. The different algorithms used are AES, DES in order to encrypt and decrypt the data.

The most commonly used encryption algorithms include AES and DES. These algorithms can be used by someone who wants to secure a large quantity of information by making a data file which can be encrypted or decrypted using the AES or DES algorithm.

There was a comparison made between AES, DES and Blowfish by Ashwin Kumar and K.S. Sandha in terms of security and power consumption and they concluded that AES has better performance than any other algorithm. There is more comparison made between AES and DES about which one is better in providing more secure content with better timing [6]. They also show that both the algorithm takes different time depending on the machine.

Encrypting entire files of data can be a practical method for securing a huge quantity of data. However, bulk encryption of files can be ineffective and bulky as it is not possible to access a selective portion of the encrypted data in the file. Even if the application only needs to access a certain portion of the data, the entire file needs to be decrypted. Without the ability to decrypt a part of a file, it is difficult to design a data processing system that is able to provide a different level of data access to different applications.

5.1 Rijndael History

A collection of block ciphers used for cryptography application is known as Rijndael, and three of the ciphers from Rijndael are adopted as the algorithms for AES a symmetric key encryption standard that was endorsed by NIST as US Federal Information Processing Standard on 26th November 2001, and it was later on adopted by US government standard on 26th May 2002. Every Rijndael block ciphers a symmetric key (a secret key, cipher key, encryption key or decryption key), plain or cipher text as input and thus implements a cryptographic procedure that uses four basic transformations in order to convert plain text to cipher text and vice versa for message authentication[6]. The four basic steps are:

- Sub Bytes
- Shift Row
- Mix Column
- Add Round Key

For the same reason as AES, some variants of Rijndael are being widely accepted for better performance of a cryptographic function for data containing voice or other media types.

Mathematical Background

The mathematical concepts useful in understanding the Rijndael algorithm are as follows :

- Algebraic Properties
- Finite Field
- Euclidean Algorithm
- Finite field Arithmetic

5.1.1 Algebraic Properties

All the integers denoted by Z are closed under the operation of subtraction, addition, and multiplication. However, algebraic properties cannot be closed under the division operation as the remainder is not always an integer.

5.1.2 Finite Field (Galois Field)

A field consisting of a finite number of elements and having a prime characteristic is known as a finite field or Galois field. The total number of elements in a set is known as the order of the fields and the fields consisting of the same order are known as isomorphic, because they have a similar structure.

5.1.3 Euclidean Algorithm

This algorithm helps to determine the greatest common divisor (GCD) of any two integers. The GCD of two integers is the largest number which divides both the integer in the case of both integers not being zero. For example, the GCD of 12 and 30 is 6. The extended Euclidean algorithm can be called as a version of the Euclidean algorithm; in the case of having two integers a and b as input, then the algorithm computes GCD of the integer as well as the x and y . This works as Euclid's algorithm and deals with the sum of multiples of a and b .

5.1.4 Finite Field Arithmetic

Elements of a finite field can be expressed in various numerical forms, however, in the Rijndael algorithm the polynomial representation was chosen, with each term expressing bits in binary expression. For example: the hexadecimal value {4a} which is {01001010} in binary can be represented as the following polynomial x^6+x^3+x .

5.2 Algorithm Specification

Rijndael is a key-iterated block cipher having both block length and key length, i.e., both the key and block size needs to have 128, 150, 192, 224 or 256 bits. The difference between Rijndael and AES is the range of values supported for both block and cipher length. The AES fixes the block length to be 128 and supports the key length of either 128, 192 or 256 bits. The extra block and key length of Rijndael are not adopted in the current FIPS standard as they were not evaluated during the AES selection process.

5.2.1 Rijndael Byte and State

The input and output of AES (Rijndael) are a sequence of 128 bits, which is the size of the cipher block and the key length can be chosen between 128, 192 or 256 bits. A byte for Rijndael can be defined as: a collection of 8-bit sequences and representing a finite field element. Using the polynomial representation, the byte 'b' can be represented as follows:

$$b_7x^7 + b_6x^6 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0$$

Where; $b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0$ are either 0 or 1 given that Rijndael uses a finite field.

5.2.2 The Rounds

Rijndael consists of a variable number of rounds depending on the cipher block and key length which are as follows:

- i. 10 for both block and key length being 128 bits long.
- ii. 12 if either one of the block or keys is 192 bits, but neither of them is larger than 192 bits.
- iii. 14 if either the block or the key is 256 bits.

Rijndael is an algorithm consisting of an initial key addition, the Add Round Keys step which is followed by routine rounds, but the final round omits the Mix Columns step. Each round is a sequence of four-byte transformation known as steps. So, when Rijndael algorithm is being used for the encryption the steps that are being followed are:

5.2.2.1 Byte Substitution

Every 8-bit byte is reversely mapped into another byte. Each byte in the block is changed by its substitute in an S-box (a box that maps 'n' bits to 'm' bits). Being the only part of the cipher that is nonlinear, it is considered the most vital part of the algorithm.

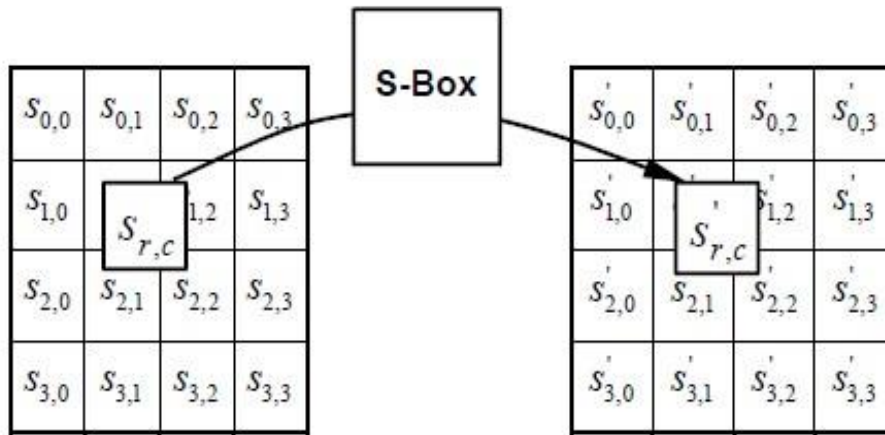


Figure 4. Byte Substitution

(Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001)

5.2.2.2 Shift Rows

In this step, the rows are shifted over four different ways. Row 0 is not touched; row1, row2, and row3 are rotated left respectively. In the Shift Rows transformation, the bytes in the last three rows are cyclically shifted over a different number of bytes the first row, $r=0$ not being touched.

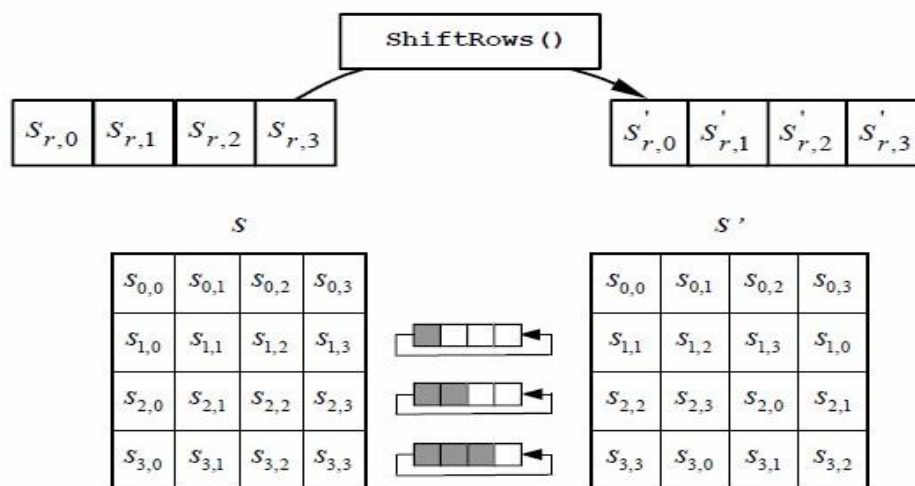


Figure 5. Shift rows cyclically shifts the last three rows in the state

(Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001)

5.2.2.3 Mix Columns

In this process the bytes in columns are combined linearly, after matrix multiplication is performed.

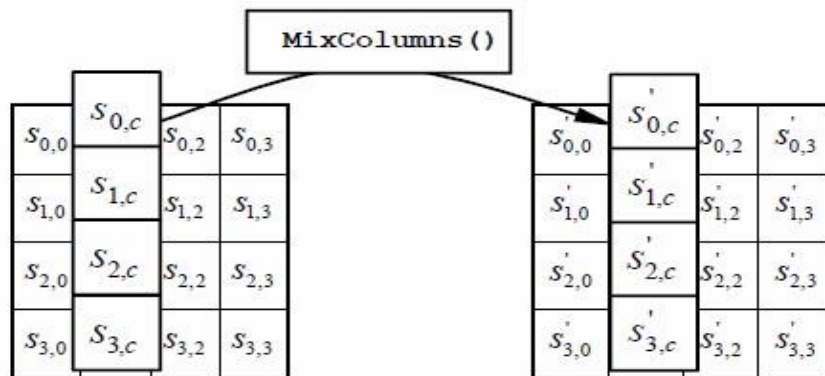


Figure 6. Transform matrix of mix column

(Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001)

5.2.2.4 Add Round Keys

In this final stage, the subkey is added by combining each byte with the corresponding byte of the subkey using XOR (logical operation given true output when both inputs are different).

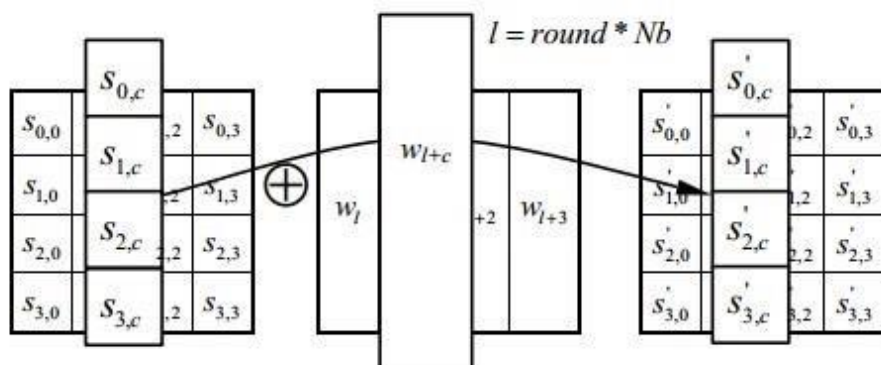


Figure 7. AddRoundKey () XORs each column of the State with a word from the key schedule.

(Source: Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001)

5.2.3 Key Schedule

The round keys with the help of key schedule are derived from the cipher key. The AES algorithm thereafter performs a key expansion using the cipher key, takes the cipher key, and performs an expansion to generate a total of $N_b(N_r+1)$ 32 bit words (where, N_b is a total number of columns, for AES the value is 4 and N_r are total number of rounds i.e. 10,12 or 14). Each of the rounds in Rijndael having Add Round Keys requires a set of four 32-bit words of key data. The key expansion algorithm expands the input cipher key by changing the first N_k words with the input cipher key (where, N_k is the number of 32 bit words in the cipher key for AES the value are 4, 6 or 8). Then every following word $w[i]$ is equal, to the exclusive OR of the previous word $w[i-1]$, and the word N_k is the word $w[i-N_k]$. For the words in positions that are a multiple of N_k , the previous word $w[i-N_k]$ is first rotated one byte to the left, and then its bytes are transformed using the Sbox from the Byte Substitution step and then is exclusive OR-ed with a round-dependent constant prior to the exclusive OR with $w[i-N_k]$.

6 COMPARISON OF AES AND DES

AES and triple DES (TDES OR 3DES) are the most commonly used block ciphers. By design, AES is faster in term of rounds, i.e., switching between the hardware is simpler than switching between software. However, DES encrypts data in 64 bit and uses a 56 bit key, as a result of which it has an approximate possibility of 72 quadrillion [7]. Even though the number is huge, due to the computing power of current technology, it is not sufficient and can be exposed to attacks. So, as a result of DES not being able to keep up with the technology advancement, it is not an appropriate security. Because of the vast use of DES, the fastest solution was to update to 3DES, which is secure enough for current technology. The Rijndael algorithm has been chosen to replace 3DES. The main reason for Rijndael to be chosen as the next gen AES are:

- i. Security
- ii. Software and Hardware Performance
- iii. Suitability in restricted-space environments
- iv. Resistance to power analysis and other implementation attacks

AES works fast even on small electronics and devices (smart phones, smart cards). It is able to provide more security as it has a larger and longer block size and key. It also uses a 128-bit block size and works with 128,192 and 256-bit keys. Rijndael being flexible is able to work with any key and block size which is the multiple of 32bit and is between 128 and 256 bits. AES is a replacement for 3DES, and both of the cipher keys will coexist until 2030 for a smooth and gradual transition. The detailed comparison of AES and DES is shown in the table below:

Table 1. Comparison of AES and DES

Factors	AES	DES
Key length	128, 192 or 256 bits	56 bits
Cipher type	Symmetric block cipher	Symmetric block cipher
Block size	128, 192, or 256 Bits	64 bits
Cryptanalysis resistance	Strong against differential, linear, interpolation and square attacks.	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	Proven inadequate
Possible keys	$2^{128}, 2^{192}$ or 2^{256}	256
Times required checking all possible keys 50 billion Keys per second	For a 128-bit key 5×10^{21} years	For a 56-bit 400 days
Rounds	10,12 and 14 for 128, 192 And 256-bits respectively	16

(Source: Milind Mathur, Ayush."COMPARISON BETWEEN DES, 3DES, RC2, RC6, BLOWFISH AND AES." on New Horizons in IT - NCNHIT 2013)

7 CLASSIFICATION OF CRYPTOGRAPHY TECHNIQUES

The high growth in the networking technology leads to a common culture for interchanging of the data very drastically. Hence, it is more vulnerable to duplicate and be re-distributed by hackers. Therefore, the information has to be protected while being transmitted. Many encryption techniques exist which are used to prevent information theft. Different cryptography techniques used to protect the confidential data include:

7.1 Optical Encryption

Optical encryption uses optical instruments in order to build physical systems for image encryption, which mostly relies on optics for changing the frequency component of an image. The colour images are first changed into indexed image formats before being encoded. During that encoding process, the image is encoded to motionless white noise with two phase masks: one being on the input plane and the other on the Fourier plane. In the decryption process, the coloured image can be recovered by changing the indexed image back to the RGB composition. This method is more solid and powerful than any other currently.

7.2 Selective Encryption

Selective encryption mostly aims at avoiding the encryption of all the bits of a digital image while still being able to provide secure encryption. The key point is only to encrypt a small part for fast encryption. Selective encryption includes five methods:

- i. DCT-based Methods
- ii. Fourier-based Methods
- iii. Scan-based Methods

- iv. Chaos-based Methods
- v. Quad-tree based Methods

These methods for reaching the application requirement have to be fast while still keeping the compression ratio as same as the original. Several different methods have been suggested as the encryption for DCT-based methods. Methods known by the name zig-zag were created using Tang, another algorithm by Qiao and Nahrstedits which is based on the frequency distribution of two adjacent bytes in the MPEG bit stream. This method offers several advantages: resilience, profusion, dimensional selectively, and format flexibility.

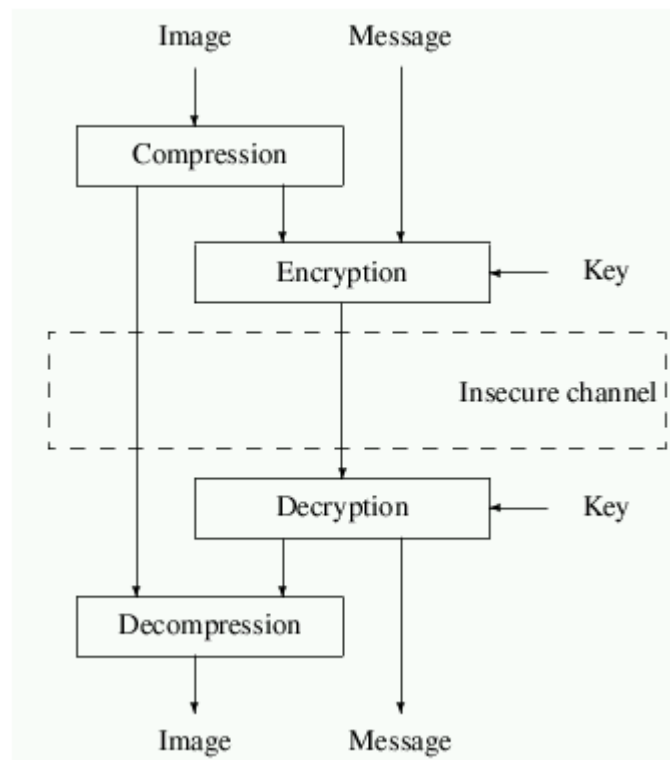


Figure 8. Selective encryption mechanism

(Source: <http://www.telecom.ulg.ac.be/publi/publications/mvd/sps-2004/>)

7.3 Chaotic Encryption

Chaotic encryption has high sensitivities for its initial values as well as its parameters, the mixing property, and its ergodicity. Ergodicity is a process in which every sequence sample is equally representative of the whole. This method is considered as one of the good candidates for cryptography. The main foundation for this type of encryption is the selection of the best chaotic map for certain encryption projects. [7] The chaotic map used for the encryption process should have the following properties:

Mixing property

The mixing property is connected with the property of dispersion in the algorithm. Just imagine the set of plain texts having an initial region in the phase space of the map, then it is the mixing property that signifies the scattering out of a single plain text over many cipher text.

Robust Chaos

A preferred algorithm should be able to spread the influence of a single key digit over many cipher digits. The key indicates the framework of an encryption algorithm. Thus, we should be concerned about the transformation, including both parameters and variable.

Parameter Set

The larger parameter space of the system implies that its single out version will have larger keys. During the permutation stage, a powerful dispersal effect is introduced by using a 3D-cat map-based dimensional bit-level shuffling algorithm.

7.4 Nonchaotic Encryption

Yue Wu has suggested image encryption using the Sudoku matrix. Encryption of the image according to this system consists of three stages. During the first stage, a reference Sudoku matrix is created and is used for the scrambling process. Then the intensities of the image pixels are changed using the reference Sudoku matrix values and finally the pixel value are shuffled using the same Sudoku matrix as mapping process. So with the help of this matrix we are able to encrypt any digital images (binary images, grey images, and RGB images) [8].

A logistic map is used in order to control the size of a Sudoku matrix. Yue Wu has forwarded an ideal of a Latin square image cipher, which provides a 256 bit key length for the generation of a Latin square and thus generates a 256 x 256 square image resembling to look like a Sudoku matrix, i.e., no two digits in the same block can be aligned in the same row, column or box. Using LSIC, many desired properties of secure cipher can be achieved including:

- i. Large key space
- ii. High key sensitivities
- iii. Uniformly distributed cipher text
- iv. Excellent confusion and diffusion
- v. Semantically secure

Later on two new algorithms based on the Fibonacci code were presented: One for spatial domain and the other one for the frequency domain (also known as JPEG domain). The security key for the image scrambling algorithms are:

- Parameter (p and i)
- Size of original image

There is a huge number of possibilities for the security keys, making the scrambled image difficult to decrypt by unauthorized users thus making it more secure.

8 VARIOUS METHODS

Nowadays the internet is used for faster transmission of large volumes of important and valuable data. Since the internet has many points of attack, it is vulnerable to different kinds of attacks, so these data need to be protected from unauthorized access. Some of the methods for simple and secure solutions for image encryption and decryption are outlined in the following sections.

8.1 JPEG Encryption

A scalable encryption method compromising backward compatibility with the JPEG2000 images was developed by Osamu Watanabe. This encryption method informs the encrypted image to hold the multilevel encryption while still being able to decrease the computational complexity of the encryption. [9] The standard JPEG 2000 is used for the decoding of the encrypted image and some parameters of JPEG 2000 are saved after the encryption process. As a result of this, the time for encryption process is controlled by a selective encryption algorithm for faster processing.

Analysis of this method with JPEG image was carried out by W. Puech and J.M. Rodrigues. Their paper is mainly concerned with the disadvantages of both selective encryption (SE) and image compression. The SE is being generated by AES algorithm integrated with the Cipher Feedback (CFB) mode. For the image compression, the JPEG algorithm is used.

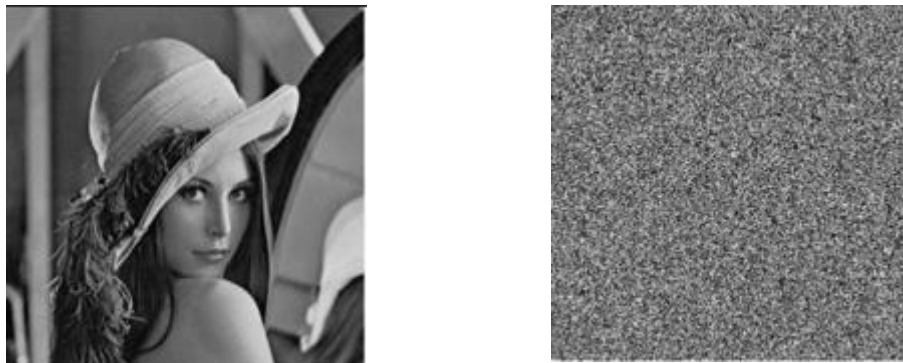


Figure 9. JPEG Encryption Example

(Source: <http://202.38.64.11/~whli/lab/imse.html>)

8.2 SCAN

S.S. Maniccam and N.G. Bourbakis have presented a new algorithm which performs two significant functions:

- i. Lossless compression of binary and grey-scale images
- ii. Encryption of binary and grey-scale images

The compression and encryption scheme are based on SCAN patterns which are generated by SCAN methodology. The SCAN is an official language based on 2D spatial-accessing methods capable of generating a wide range of scanning paths or space filling curves.



Figure 11. Scan Image Encryption Example

(Source: <http://ethesis.nitrkl.ac.in/6456/1/E-57.pdf>)

8.3 Hash Function

A new algorithm was proposed based on the SHA-512 hash function by S.M. Seyedzade and R.E.A.S Mirzakuchaki. It consists of two sections: firstly it processes the operation for shuffling one-half of an image and after that, the hash function is used to create a random number mask. After that the mask is XORed with the second part of the image which is finally going to be encrypted [9].

8.4 Visual Cryptography

Visual cryptography uses the characteristics of human ability to decrypt an encrypted image. It does not require any cryptography knowledge or difficult calculation. Still making sure that hackers cannot receive any idea about a secret image from a single cover image.

This system was introduced by using a Hilbert curve and two queues, by Sen-Jen Lin, Ja-Chen Lin and Wen-Pinn Fang. The Hilbert curve was used for reducing the problem from the 2-D image to 1-D binary string while the white queue is being used to accumulate enough white pixel ('m' white pixels) so that all these 'm' white pixels could only use one matrix rather than 'm' matrix. The black queue is used for a similar purpose in a corresponding way. Stacking the shadows results into an image of high quality. However, C.C. Chang, C.S. Tsai and T.S. Chen have suggested that the visual cryptography scheme should be able to support a huge image format like the colour and grey scale. They also added that the random-looking shares appear to be mistrustful making it exposed to attack in the middle, to prevent such attacks, only essential shares should be made. Binary encoding was used by Y.C. Hou, F. Lin, and C.Y. Chang for representing the subpixels selected for each block and then applied the AND/OR operation in random to calculate the binary code for the stacking subpixels of all the block in the cover image. The code can range from anywhere

between 0-255, but it can be even expanded depending on the factor. Therefore, a secret image can be 256 colour or true colour [9].

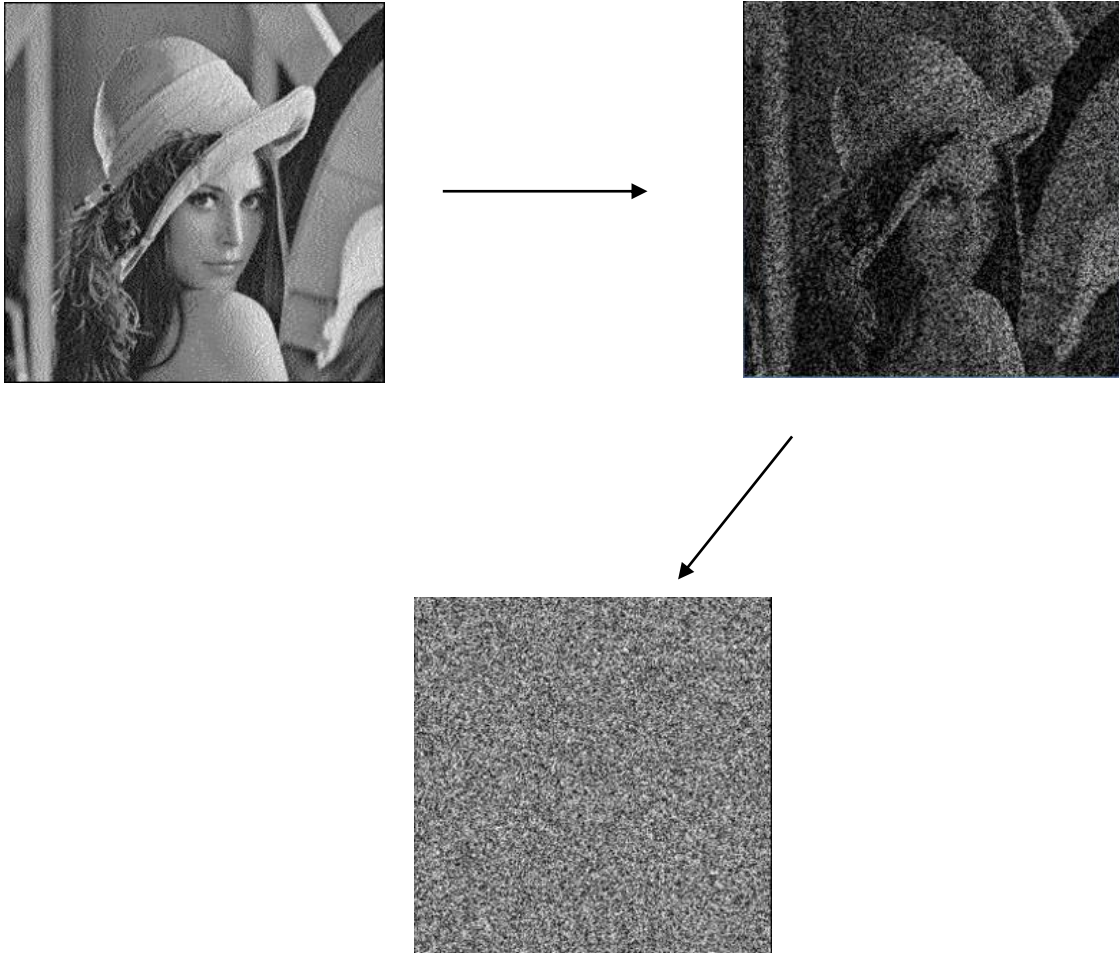


Figure 11. Visual Cryptography Example

(Source:<http://citeseerx.ist.psu.edu/viewdoc10.1.1.457.50771&type=pdf>)

9 SECURITY ANALYSIS

Security is a major issue in cryptology. A good image encryption scheme should resist various attacks such as known plain text attack, cipher-text-only attack, statistical analysis attack, and brute-force attacks. Some of the security analyses are as follows:

9.1 Exhaustive Key Search

A secure encryption algorithm should be one having a large key space. The larger the key space, the fewer the chances for an attack on the encrypted design. Suppose an algorithm has a K -bit key, then the extensive key search requires 2^K trials for breaking the key.

9.2 Key Sensitivity Analysis

A perfect image encryption process should be dealt sensitively with a secret key, meaning that the change of a single bit in the secret key produces a completely different cipher-image [10]. Such type of sensitivity can be addressed with respect to two aspects:

i. Encryption

Two different cipher text images, C_1 and C_2 , created with respect to the same plaintext image using two encryption keys K_1 and K_2 , with the difference of only one bit between the two keys.

ii. Decryption

Two different decrypted images, D_1 and D_2 , created with respect to the same cipher text image using two encryption keys, K_1 and K_2 , with the difference of only one bit between the two keys.

9.3 Histogram Analysis

This is one of the most genuine methods that illustrates the quality of the encrypted image since a quality image encryption method contributes to encrypt a plain text image to random, thus making it a requirement for seeing a uniformly-distributed histogram for a cipher text image.

9.4 Information Entropy Tests

Even though Histogram analysis is the most genuine analysis, showing how uniformly a cipher text image pixels can be distributed, it still has one problem, indicating how well or badly the histogram distributes. Information entropy can be defined as the significant measurement of randomness of a signal source.

$$H(X) = - \sum_{i=1}^n \Pr(x_i) \log_2 \Pr(x_i)$$

$$\Pr(X = x_i) = \frac{1}{F}$$

Equation 1. Information Entropy Equation

In simple words, the information entropy can be used to compute the randomness of the image shown in the above equation.

Where;

X= test image

X_i=possible value in X

Pr (x_i) = probability of random pixels in X having the value X_i

H(x) = achieved when X is uniformly distributed F = number of allowed intensity scale associating image format

9.5 UACI and NPCR tests

NPCR and UACI were first shown in 2004 by, Yaobin Mao and Guanrong Chen. Since then NPCR and UACI become two widely used security analyses in the image encryption community.

$$N(C^1, C^2) = \sum_{i=1}^M \sum_{j=1}^N \frac{D(i, j)}{T} \times 100\%$$

$$U(C^1, C^2) = \sum_{i=1}^M \sum_{j=1}^N \frac{|C^1(i, j) - C^2(i, j)|}{L \cdot T} \times 100\%$$

$$D(i, j) = \begin{cases} 0, & \text{if } C^1(i, j) = C^2(i, j) \\ 1, & \text{if } C^1(i, j) \neq C^2(i, j) \end{cases}$$

Equation 2. UACI and NPCR equation

The two equations above can be used to describe the cipher text image C_1 and C_2 whose plaintext image are slightly different. The function $D(i, j)$ denotes whether the two pixels located at the grid of the image (i, j) of C_1 and C_2 are equal. T denotes the total number of pixels in the cipher text image and L being the largest allowed pixel intensity. It can be noticed that NPCR focuses on the absolute number of pixels which changes its value during the differential attacks. While UACI is focusing on the averaged difference between the cipher text images.

9.6 Correlation Coefficient Analysis

This is the factor determining how many similarities two variable have with each other. This is commonly used for the measurement of encryption quality for all the types of cryptography. The co-efficient of correlation (r_{xy}) can be computed as follows:

$$r_{xy} = \frac{\text{Cov}(x, y)}{\sigma_x \sigma_y}$$

$$\sigma_x = \sqrt{\text{VAR}(x)}$$

$$\sigma_y = \sqrt{\text{VAR}(y)}$$

$$\text{VAR}(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$

$$\text{VAR}(y) = \frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2$$

$$\text{Cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))$$

Equation 3. Correlation and Coefficient Equation

Where; x and y = the values of two pixels in the same location in the original and ciphered images
 $\text{Cov}(x, y)$ = covariance at these pixels
 $\text{VAR}(x)$ and $\text{VAR}(y)$ = variance values of pixel values x and y in both original and cipher image;
 σ_x and σ_y = standard deviations of both x and y pixel value;

E = expectation operator; N = image Dimension

10 CONCLUSION

There are various cryptography techniques and sub-techniques. Some techniques perform partial encryption while others perform full encryption. Some of the methods carry out image compressions but others do not. Depending on the type of application, speed, bandwidth, confidentiality, security and authenticity extent, one may select a particular type of encryption method. Each and every method has its own merits and demerits. One must think in selecting a proper cipher because now cryptanalysis techniques research is under focus. Once a cipher is developed, one must carry out various security analyses mentioned in the paper.

There is tremendous potential in this field for future research and deployment. With a possibility of developing such encryption schemes for motion compensation and implementation on embedded device architectures.

REFERENCES

1. Borka Jerman-Blazic, Tomaz Klobucar, 2002. *Advanced Communications and Multimedia Security*. New York: Springer Science+Business Media New York.
2. Ching-Yung Lin, 2006. *Topics in Signal Processing -- Multimedia Security Systems*. [Online] Available at: http://www.ee.columbia.edu/~cylin/course/mss/MSS_notes.html [Accessed 1 10 2015].
3. Emanuil Rednic; Andrei Toma, n.d. Software Analysis. *SECURITY MANAGEMENT IN A MULTIMEDIA SYSTEM*, 4(2), pp. 237-247.
4. A. Pande, J. Zambreno, 2013. Advances in Multimedia Encryption. In: *Embedded Multimedia Security Systems*. London: Springer-Verlag, pp. 11-22. [Online] Available at: http://www.springer.com/cda/content/document/cda_downloadaddocument/9781447144588-c2.pdf?SGWID=0-0-45-1345406-p174549534 [Accessed 11 10 2015].
5. Saha Arunabh n.d. *Overview of Multimedia Security*, s.l.: s.n. [Online] Available at: http://www.academia.edu/8199308/Overview_of_Multimedia_Security [Accessed 15 11 2015].
6. Thuraisingham Bhavani., 2007. *Security and privacy for multimedia database management systems*, pp. 14-29. [Online] Available at: https://www.utdallas.edu/~bxt043000/Publications/Journal-Papers/DAS/J33_Security_and_privacy_for_multimedia_database_management_systems.pdf [Accessed 1.11.2015]
7. Amit Pande; Prasant Mohapatra; Joseph Zambreno, n.d. Securing Multimedia Content using Joint Compression and Encryption, s.l.: s.n. [Online] Available at: <http://spirit.cs.ucdavis.edu/pubs/journal/amit-multi.pdf> [Accessed 15 10 2015].
8. Wenjun Zeng, Heather Yu and Ching-Yung Lin , 2006. *Multimedia Security Technologies for Digital Rights Management*. s.l.:Academic Press.
9. Sonal Guleria, Sonia Vatta, 2013. *TO ENHANCE MULTIMEDIA SECURITY IN CLOUD COMPUTING ENVIRONMENT USING CROSSBREED ALGORITHM*, 2(6), pp. 562-568. [Online] Available at: <http://www.ijaiem.org/Volume2Issue6/IJAIEM-2013-06-26-083.pdf> [Accessed 11 10 2015].
10. Shaimaa A. El-said, Khalid F. A. Hussein, and Mohamed M. Fouad, 2011. International Journal of Signal Processing, Image Processing and Pattern Recognition. *Securing Multimedia Transmission Using Optimized Multiple Huffman Tables Technique*, 4(1), pp. 49-64. [Online] Available at: http://www.sersc.org/journals/IJSIP/vol4_no1/4.pdf [Accessed 11 10 2015]

