Secure Image Transmission Through Unreliable Channels

P.VIJAYRAM REDDY, M.Sc (CS), M.Tech (CSE)
Dept of CSE
SICET
Hyderabad, India.

K.VENKATESH SHARMA, M.Tech (IT & CSE)
Prof. & HOD Dept of CSE
SICET
Hyderabad, India.

Dr.P. Mallesham, B.E, M.E,Ph.D;CSI
Principal
SICET
Hyderabad, India

P. RADHADEVI, M.C.A, M.Tech (CSE)
Assistant Professor Dept of CA
SNIST
Hyderabad, India

Abstract— **The research in the literature on the design of image security by using Arithmetic Coding and Advanced Encryption Standard. Arithmetic Coding offers extremely high coding efficiency and it provides little or no security as traditionally implemented. We present a modified scheme that offers both security and compression of images. The system utilizes an Arithmetic Coder and Advanced Encryption Standard in which the overall length within the range allocated to each symbol is preserved. The overall system provides simultaneous compression and encryption with negligible coding efficiency by accelerated hardware implementations.**

Key Words: Arithmetic Coding (AC), Encryption, Decryption and Advanced Encryption Standard (AES)

I. INTRODUCTION

The advances in communication technology and the growth of computer presser possessing power and storage, the difficulties in ensuring Defense data as well as individuals privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one to another. Various methods have been investigated and developed to protect data and personal privacy. Encryption is probably the most obvious one[4]. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks[5]. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, Furthermore. For reliable communications, channel coding is often employed. As such in this paper, a scheme based on encryption and channel coding has been proposed for secure data transmission over channels[1].

Arithmetic Coding is the most powerful technique for statically loss less encoding. A message is coded as a real number in an interval from 1 to 0 for data. Arithmetic Coding typically has a better compression ratio, as it produces a single symbol rather than several separate code words. Although AC offers high efficiency in coding, it provides less or no security as conventionally implemented.

II.DESCRIPTION

Arithmetic Coding has been developed extensively since its introduction several decades ago and is notable for offering extremely high coding efficiency. While many earlier-generation image and video coding standards such as JPEG, H.263, and MPEG-2 relied heavily on Huffman Coding for the entropy coding steps in compression, recent generation standards including JPEG2000 and H.264 utilize arithmetic coding. This has led to increased interest in arithmetic coding both in the context of image coding and also more generally for other applications. While Arithmetic Coding is extremely efficient, the issue of providing both security and compression simultaneously is growing more important and is given the increasing ubiquity of compressed image files in host applications of Defense, Internet and digital cameras and the common desire to provide security in association with these files. When both security and compression are sought, one approach is to simply use Arithmetic Coder (AC) in combining with Advanced Encryption Standard (AES).

A survey on image encryption techniques had eight remarks, which are listed below[13]:

- Permutation-only image and video encryption schemes are generally insecure against known and chosen-plaintext attacks.
- Secret permutation is not a prerequisite
- Cipher-text feedback is very useful for enhancing the security
- Cipher-text feedback can be enhanced further if combined with permutation
- Combining a simple stream cipher and a simple block cipher can help improve security
- The diffusion methods used in most chaos-based encryption schemes are too slow
- Selective encryption may provide enough security given the dependencies between the unencrypted and encrypted data
- A recommendation to use a slow, but stronger, cipher to encrypt selective data and fast, but weaker, cipher to encrypt the remaining data

Arithmetic Coding not provides security in the face of a chosen-plaintext attack, in which an attacker has the ability to specify a sequence of input symbols and observe the corresponding output, and to repeat this process, an arbitrary number of times. The present work aims to provide an AC system that is secure against a chosen plaintext attack by applying AES After Arithmetic Coder. A scheme that offers both compression and encryption is designed to achieve both security and compression. The system utilizes an Arithmetic Coder in which the overall length within the range [0,1) of real numbers for the data.

The overall system provides compression and encryption, with negligible coding efficiency penalty relative to a traditional Arithmetic Coder. The system consists of a first coding and encryption step applied to the bits produced by encryption. At the Resaving side decryption and decoding of the image.

In the first step compressed with Arithmetic Coding so as to transmit the image using the shortest possible memory and encryption of the image encryption and decryption algorithms based on Advanced Encryption Standard.

III.ARITHEMATIC CODING

Unlike the variable-length codes, Arithmetic Coding generates single code word. i.e Arithmetic Coder does not generate code words one-to-one correspondence between source symbols and code words. Instead, an entire sequence of source symbols is assigned a single Arithmetic Code word.

The code word lies between interval of real numbers 0 and 1[1]. As the number of symbols in the input increases, the interval used to represent it becomes smaller and the number of bits required to represent the interval becomes larger[17]. Each symbol of the message reduces the size of the interval in accordance with the probability of occurrence.

Arithmetic Coding Encoder:

```
BEGIN
    Low_Val = 0.0; High_Val = 1.0; range = 1.0;

while (byte_symbol != nTerminator)
{
get (byte_symbol);

Low_Val = Low_Val + Symbol_Range * Symbol_Range_low(byte_symbol);
High_Val = Low_Val + Symbol_Range *
```

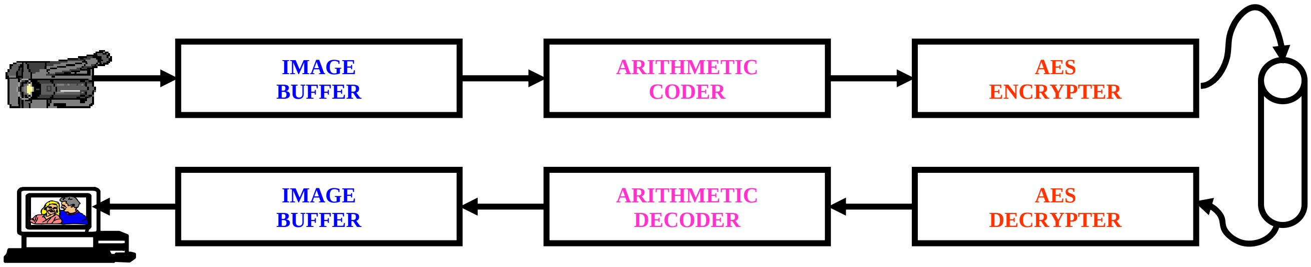

Figure 1. Block diagram of image transmission and reception scheme

```
Symbol_Range_high(byte_symbol);

    Symbol_Range = High_Val  – Low_Val ;

    }
    Output a code so that Low_Val  <= code < High_Val ;
    END
```

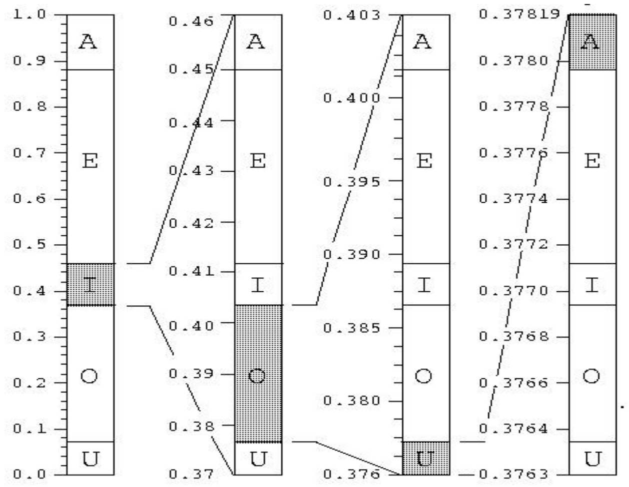

Figure 2. Restricting the interval using Arithmetic Coder

Arithmetic Coding Decoder:

```
BEGIN
         get encoded value = value(code);

         Do
         {

          find a byte_symbol s so
         that

         Symbol_Range_low(s)
         <= value <
         Symbol_Range_high(s);

         Output s;

         High_Val  =
         Symbol_Range_high(s);

    Symbil_Range  =  High_Val   -
Low_Val ;

    value = [value - Low_Val ] / Symbol_Range;
    }
    Until byte_symbol s is a nTerminator

    END
```

IV.AES ALGORITHM

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits[2]. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state[3]. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) .These rounds are governed by the following transformations[14]:

1) *Byte sub transformation:* Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and Affine Transformation.

2) *Shift rows transformation:* Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes[11].

3) *Mix columns transformation:* Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

4) *Add round key transformation:* Is a simple XOR between the working state and the round key. This transformation is its own inverse.

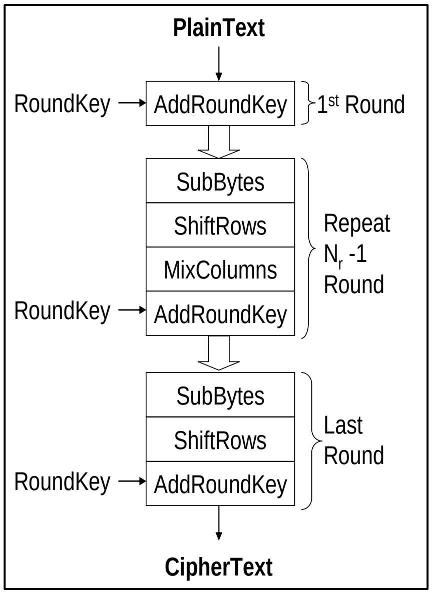

Figure3a: diagram of AES encryption algorithm

Expansion Key:

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text[5]. The AES algorithms is designed to use one of three key sizes (N_k). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm[9]. This key expansion routine can be performed all at once or 'on the fly' calculating words as they are needed.

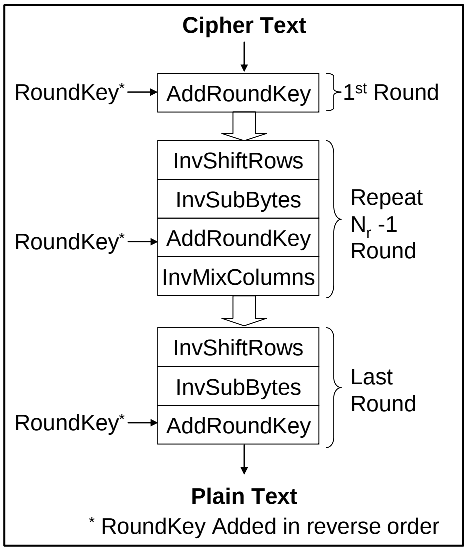

Figure3b: diagram of AES decryption algorithm

Strengths:

- AES is extremely fast compared to other block ciphers. (Though there are tradeoff between size and speed)[13]
- The round transformation is parallel by design. This is important in dedicated hardware as it allows even faster execution.
- AES was designed to be amenable to pipelining.
- The cipher does not use arithmetic operations so has no bias towards big or little endian architectures.
- AES is fully self-supporting. Does not use S-Boxes of other ciphers, bits from Rand tables, digits of π or any other such jokes. (Their quote, not mine)[16]
- AES is not based on obscure or not well-understood processes.
- The tight cipher and simple design does not leave enough room to hide a trap door.

V. RESULTS

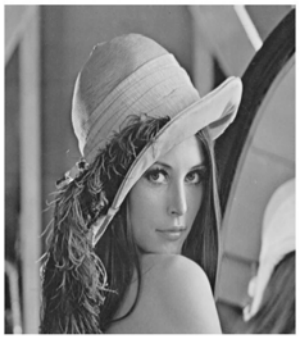

Fig 4a: Input Image

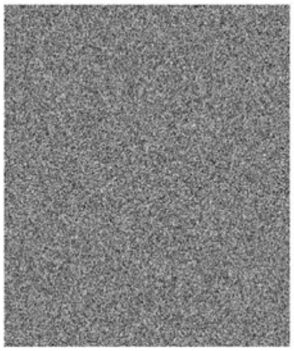

Fig 4b: Encrypted Image

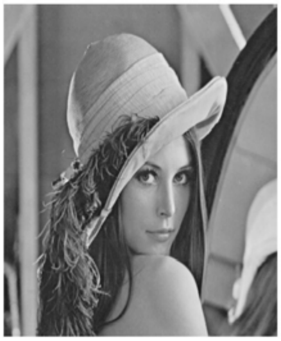

Fig 4c: Decrypted Image

VI. CONCLUSIONS

The system offers compression and security, illegal data or image access in wireless and fixed unreliable communication networks. The Advanced Encryption Standard. Offers the flexibility of allowing different key size 128 bit, 192 bit and 256-bit key. Security based on the various random key selections, different S-box and different and strong Transformations Thus; the algorithm provides many different flexible implementations. Arithmetic coding is extremely efficient, Arithmetic coding typically has a better compression ratio, as it produces a single symbol rather than several separate code words.

VII. REFERENCES

1. "Secure Arithmetic Coding" In Ieee Transactions On Signal Processing, Vol. 55, No. 5, Pp. 2263–2272, May 2007.
2. Advanced Encryption Standard (Aes), Fed. Inf. Process. Standards Pub. 197, 26, Nist.
3. Cryptographyand Network Security Principles And Practices, Fourth Edition By William Stallings.
4. Arithmetic Coding For Data Coiupression Ian H. Willen, Radford M. Neal, And John G. Cleary "Communications Of The Acm" June 1987 Volume 30 Number 6.
5. Data Compression The Complete Reference Fourth Edition By David Salomon.
6. Introduction To Data Compression Third Edition By Khalid Sayood.
7. N. Bourbakis, A. Dollas, Scan-Based Compression-Encryption Hiding For Video On Demand. *Ieee Multimedia Mag*. 10, 79–87, 2003.
8. Bell, Timothy C., Cleary, John G "Text Compression", Prentice Hall, Englewood Nj.
9.AES *Proposal : Rijndael* Joan Daemen, Vincent Rijmen, 2nd verof document to NIST.
10. Wikipedia, Page Title: Block cipher modes of operation http://en.wikipedia.org/ wiki/Cipher_block_chaining
11. *Selecting the Advanced Encryption Standard* Burr, W.E.; Security & Privacy Magazine, IEEE Volume 1, Issue 2, Mar-Apr 2003 Page(s):43 - 52
12. *Title: Introduction to Cryptography* Author: Johannes A Buchman Publisher:
13. Cache-Timing attacks on AES Daniel J Bernstein Preliminary version of report to National Science Foundation, grant CCR-9983950.
14. Fast implementation of AES cryptographic algorithms in smart cards Chi-Feng Lu; Yan-Shun Kao; Hsia-Ling Chiang; Chung-Huang Yang; Security Technology, 2003.
15. Shuang Wu, Dengguo Feng, and Wenling Wu. Cryptanalysis of the LANE Hash Function. In Michael J. Jacobson, Vincent Rijmen, and Rei Safavi-Naini, editors, SAC, Lecture Notes in Computer Science. Springer, 2009. To appear.
16. Vincent Rijmen. Cryptanalysis and design of iterated block ciphers. Ph.D. thesis, KULeuven 1997.
17. Krystian Matusiewicz, Mar__a Naya-Plasencia, Ivica Nikolic, Yu Sasaki, and Martin Schl a_er. Rebound Attack on the Full LANE Compression Function. In Mitsuru Matsui, editor, ASIACRYPT, Lecture Notes in Computer Science. Springer, 2009. to appear.
18. D. Jones, "Applications of splay trees to data compression," *Commun. ACM*, 996–1007, 1988.
19. H. Cheng and X. Li, "Partial encryption of compressed images and videos", *IEEE Trans. Signal Processing*, 48: 2439-2451,2000.
20. Li. Shujun, Li. Chengqing, C. Guanrong, *Fellow.,IEEE.*, Dan Zhang., and Nikolaos,G., Bourbakis *Fellow., IEEE*. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf

This page is left intentionally blank