SECURE AND SCALABLE VIDEO TRANSMISSION

Abstract: We propose an efficient scheme to construct fountain codes that can provide unequal error protection (UEP) property. To reduce the coding complexity and improve the performance of previous duplicate UEP scheme in the literature, we implement different rate low density parity check (LDPC) codes instead of the duplication process and replace the high complexity classical robust solution distribution (RSD) by low constant average degree distributions with high intermediate symbol recovery rates (ISRR). Asymptotic analysis of both duplicate scheme and our scheme is obtained by deriving unequal density evolution formulas over the binary erasure channel (BEC). Compared to previous UEP schemes, our scheme has lower complexity. Experimental results show that our scheme can obtain better decoding performance, especially for smaller input information length. Comparison of peak signal-noise ratio (PSNR) performance for the scalable video coding shows that, for moderate input information length, our scheme can provide a better basic video quality at lower overhead, but needs larger overhead to achieve a high video quality.

Index Terms: Scalable, Security, Video Transmission.

I. INTRODUCTION

In this project, we will have authenticated users who will transfer video and the data transmitted via video will be secured and will be in encrypted form. We verify that the performance of our scheme is undesirable while concatenating low rate LDPC codes with LT codes based on the Raptor DD, which is mainly due to the well-known avalanche effect in LT decoding. To enable only trusted and authenticated users to upload and send any confidential video files over a secure network to another user with enhanced encryption decryption and compression techniques. Recently, application layer forward error correction has been widely used to enhance multimedia communication. Fountain codes are proposed as a flexible and efficient solution for data transmission over packet erasure networks. Unlike traditional fixed-rate coding schemes, fountain codes are rate less in the sense that such codes can generate a potentially limitless number of encoded output bits from k input information bits.

www.gjaet.com

In wireless packet erasure networks, efficient multimedia transmission is a challenging task. This is due to time-varying channel characteristics and heterogeneity of end-user devices (e.g., laptop, tablet and mobile phone). The most important layer and the less important layers are referred to as the base layer (BL) and enhancement layers (ELs), respectively. We derive the density evolution (DE) formulas for duplicate UEP scheme over the binary erasure channel (BEC), and verify that duplicate UEP scheme cannot improve performance by increasing the expanding factor while utilizing constant average degree distributions.

We propose a novel and efficient UEP fountain coding scheme by combining different rate LDPC codes and low constant average degree distributions with high ISRR. Asymptotic analysis and experimental results show that our proposed scheme has lower coding complexity and can achieve better performance improvement.

II. LITERATURE SURVEY

Chen Guanghua et al. proposed an AVS real time high definition video encoder for its high memory bandwidth and large calculation complexity caused by the new coding features of variable block size and 4-tap filter. The proposed design is implemented on FPGA with operating frequency of 150 MHz and can support 1080p (1920*1080)/30fps AVS real time encoder [1].

Xue Bai et al. introduced a new color model, Dynamic Color Flow, which incorporates motion estimation into color modeling in a probabilistic framework, and adaptively changes model parameters to match the local properties of the motion. The proposed model accurately and reliable describes changes in the science's appearance caused by motion across frames [2].

Esa Rahlu et al. implemented a new salient object segmentation method based on combining as a measure with a conditional random field. The proposed saliency measure is format ted using a statistical framework and local feature contrast in illumination, color, and motion information [3].

Mohammed et al. presented an improved DC prediction mode based on the distance between the predicted and reference pixels. The proposed system adaptively
selects the number of prediction mode for each 4*4 or 8*8 blocks, which reduces the number of overhead bit's and computation all cost of the encoder [4].

Eugeny Belyaev et al, proposed a new spatial scalable and low complexity video compression algorithm based on multiplication free three dimensional discrete pseudo cosine transform. This paper shows an efficient results compared with H.264/SVC as well as it can be used for robust video transmission over wireless channels [5].

Linh Tran Ho et al., introduced a robust motion estimation scheme using a direction integrated genetic algorithm to speed up the encoding process of H.264/AVC video compression as well as to keep low bits to code frames. The obtained results show that the proposed motion estimation obtains the expressive results for both the number of bits to code a frame and the time cost to code a frame [6].

Evgeny Kaminsky et al, proposed an effective DCT-domain video encoder architecture that International Journal on Soft Computing (IJSC) Vol.2, No.4, November 201169 decreases the computational complexity of conventional hybrid video encoders by reducing the number of transform operations between the pixel and DCT domain.

The proposed system is based on the conventional hybrid coder and on a set of fast integer composition DCT transform. The proposed architecture may be used for the future Internet and 4G applications [7].

Cong Dao Han et al, implemented a novel search algorithm which utilizes an adaptive hexagon and small diamond search to enhance search speed. Simulation results showed that the proposed approach can speed up the search process with little effect on distortion performance compared with other adaptive approaches [8].

This work presents Reliable Download analyses with and without interleaving in MBMS (Multimedia Broadcast Multicast Services) under various network conditions specific to MBMS. Since MBMS download mechanism uses unidirectional multicast from one sender to a group of receivers, an application layer FEC (Forward Error Correction) is used to recover from packet losses. Our work considers Reed Solomon and Raptor FEC coding. We have done experimental work to discover Reed Solomon FEC performance under MBMS link conditions while we used analytical model for Raptor FEC under the same environment [9].

III. SYSTEM ARCHITECTURE

![System Architecture](image)

Figure 1: System Architecture

IV. PROPOSED SYSTEM

We provide a prediction model for the duplicate scheme to estimate the performance. In order to reduce the complexity of this scheme, we test the weaker Raptor DD instead of RSD and find that the performance seriously degrades. To solve the performance degradation problem, we propose a novel UEP scheme by replacing the Duplication process with low rate LDPC codes. Duplication concept belongs to repetition codes, which perform worse than LDPC Codes. Therefore, the duplicate scheme of improves BER performance at the cost of higher coding complexity by using the stronger RSD. Because of the utilization of LDPC codes in our scheme, we can get better performance and eliminate error floor even though we exploit weakened LT codes.

Moreover, our approach can achieve flexible non-integer repeat factor1 by choosing appropriate value for the code rate of LDPC codes. Instead, duplicate scheme just achieves integer duplication. Our scheme is similar to traditional Raptor codes, but the difference is that we use low rate LDPC codes to achieve UEP while the traditional Raptor codes utilize high rate LDPC pre-codes to obtain better performance.
Furthermore, we verify that the performance of our scheme is undesirable while concatenating low rate LDPC codes with LT codes based on the Raptor DD, which is mainly due to the well-known avalanche effect in LT decoding. So we further utilize weaker DDs with high intermediate symbol recovery rates (ISRR) instead of the Raptor DD and conclude that our proposed scheme can not only obtain better performance but also have lower coding complexity.

V. ALGORITHMS
1) AES CBC Encryption and Decryption Algorithm:
This algorithm provides the following cryptographic functionalities
- Encryption using AES
- Decryption using AES
Generate a AES key (specify the Key size during this phase); Create the Cipher

To Encrypt: Initialize the Cipher for Encryption
To Decrypt: Initialize the Cipher for Decryption

- **Step 1**: Generate an AES key using Key Generator. Initialize the key size to 128 bits (16 bytes)
- **Step 2**: Generate an Initialization Vector (IV)
  a) Use Secure Random to generate random bit. The size of the IV matches the block size of the cipher (128 bits for AES)
  b) Construct the appropriate Iv Parameter Spec object for the data to pass to Cipher's init() method.
- **Step 3**: Create a Cipher by specifying the following parameters
  a) Algorithm name - here it is AES
  b) Mode - here it is CBC mode
  c) Padding - e.g. PKCS7 or PKCS5
- **Step 4**: Initialize the Cipher for Encryption
- **Step 5**: Encrypt the Data
  a) Declare / Initialize the Data. Here the data is of type String
  b) Convert the Input Text to Bytes
  c) Encrypt the bytes using do Final method
- **Step 6**: Decrypt the Data
  a) Initialize a new instance of Cipher for Decryption (normally don't reuse the same object). Be sure to obtain the same IV bytes for CBC mode.
  b) Decrypt the cipher bytes using do Final method.

2) Pseudo random number Generation (PRNG):
A random number is a number that cannot be predicted by an observer before it is generated – if the number is generated within the range [0, N-1], then its value cannot be predicted with any better probability than 1/N – the above is true even if the observer is given all previously generated numbers f a cryptographic pseudo-random number generator (PRNG) is a mechanism that processes somewhat unpredictable inputs and generates pseudo-random outputs.

**Steps of PRNG:**
- $S$ a finite set of states,
- $\mu$ a probability distribution on $S$, called the initial distribution,
- A transition function $f : S \rightarrow S$,
- A finite set of output symbols $U$,
- An output function $g : S \rightarrow U$. Then the generation of random numbers is as follows:

- Generate the initial state (called the seed) $s_0$ according to $\mu$ and compute $u_0 = g(s_0)$,
- Iterate for $i = 1, \ldots, si = f(si−1)$ and $ui = g(si)$. Generally, the seed $s_0$ is determined using the clock machine, and so the random variates $u_0, u_1, \ldots$ seems i.i.d.
- uniform random variates. The period of a RNG, a key characteristic, is the smallest integer $p \in \mathbb{N}$, such that $\forall n \in \mathbb{N}, sp+n = sn$.

VI. CONCLUSION
We propose a novel construction for fountain codes to provide UEP property. Our approach is an improved design of the duplicate UEP scheme. We replace the duplication process with LDPC codes and simultaneously Utilize the weaker DDs with high ISRR instead of high complexity classical RSD.

We verify that it is impossible to improve the performance by increasing $EF$ in both the duplicate UEP scheme and our scheme while utilizing weaker DDs. Compared to other schemes, our scheme has lower complexity for the same performance. Simulation results demonstrate that our scheme can obtain better BER and FER performance especially for smaller input information length (e.g., $k = 1000$). Comparison of PSNR performance shows that, for moderate input length, our scheme can provide a better basic video quality at lower overhead, but needs larger overhead to achieve a high video quality.
VII. FUTURE SCOPE

- **Live video Conferencing:** There can be transmission of live video conferences.
- **Size of video:** There will be no limitations on larger size videos.
- Make transmission compatible with lower bandwidth/slow internet connections.

REFERENCES

[12] Dejan Vukobratovic, Vladimir Stankovic, —Scalable Video Multicast Using Expanding Window Fountain Codes, —IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 11, NO. 6, OCTOBER 2009. Secure and Scalable Video Transmission Group No. 6 SAOE, Department of Computer Engg. 32 Year 2016-17