Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2012, Article ID 720791, 8 pages
doi:10.1155/2012/720791

Research Article

Secure and Reliable IPTV Multimedia Transmission Using Forward Error Correction

Chi-Huang Shih, Yeong-Yuh Xu, and Yao-Tien Wang

Department of Computer Science and Information Engineering, HungKuang University, Taichung 433, Taiwan

Correspondence should be addressed to Yeong-Yuh Xu, yyxu@sunrise.hk.edu.tw

Received 14 December 2011; Accepted 22 May 2012

Academic Editor: Hsiang-Fu Yu

With the wide deployment of Internet Protocol (IP) infrastructure and rapid development of digital technologies, Internet Protocol Television (IPTV) has emerged as one of the major multimedia access techniques. A general IPTV transmission system employs both encryption and forward error correction (FEC) to provide the authorized subscriber with a high-quality perceptual experience. This two-layer processing, however, complicates the system design in terms of computational cost and management cost. In this paper, we propose a novel FEC scheme to ensure the secure and reliable transmission for IPTV multimedia content and services. The proposed secure FEC utilizes the characteristics of FEC including the FEC-encoded redundancies and the limitation of error correction capacity to protect the multimedia packets against the malicious attacks and data transmission errors/losses. Experimental results demonstrate that the proposed scheme obtains similar performance compared with the joint encryption and FEC scheme.

1. Introduction

As digital technologies process, Internet Protocol Television (IPTV) has emerged in the past years to deliver high-quality multimedia services to end users over IP broadband networks. Generally, IPTV has multifaceted content such as video/audio/text/graphic/data and needs to provide the user-required quality of experience (QoE), interactivity, security, and reliability in the IP-based networks [1]. The typical IPTV applications include the cable TV-like service and video on demand (VoD). In the cable TV-like service, the service provider can provide the entertainment, news, and sports programs in a regular standard definition (SD) or further high definition (HD) format, while the VoD service supports more personal options to select their favorite multimedia content. Because the IP technology is basically the same for the IPTV and Internet applications, IPTV is likely to integrate the existing and independent services over the home network connection.

Since the content delivered through IPTV is mostly of high economic value and of copyright with user's subscription, secure and reliable transmission becomes an important issue in provisioning IPTV content and services. The basic principle of the service and content protection is to ensure that users are only able to obtain the services they are entitled to access and use the content in accordance with the right they have been granted [2, 3]. For content and service protection, the conditional access system (CAS) and digital right management (DRM) are two primary protection technologies on IPTV [4]. CAS is employed in the conventional TV industry to restrict certain television programs to certain users according to a billing mechanism. On the other hand, DRM is often utilized in the information technology (IT) industry to protect the digital data against illegal copy and redistribution. In both CAS and DRM, data encryption is one common security tool to provide the robust security control on the valued data. An essential requirement for data encryption in IPTV is the need to transmit a single encrypted stream to many users. Since different users can be authorized to receive different packages of services, this requirement is generally met by using multiple layers of encryption. In addition, frequent update of encryption keys is desired to avoid unauthorized data sharing due to illegal key extracting. Although the data encryption is a well-designed technique

in protecting sensitive data, its efficacy in IPTV environment can be affected based on the IP delivery characteristics such as packet loss [5, 6]. In order to protect the multimedia stream against transmission errors/losses, forward error correction (FEC) deliberately produces redundant data to enable the reconstruction of any multimedia packets which are lost during transmission. The IPTV standard developed by Digital Video Broadcasting (DVB) project specifies an application-layer FEC to perform packet loss repair for IPTV streaming media [7, 8].

One of the possible solutions to support a secure and reliable transmission is the integration of data encryption and FEC recovery [9–12]. The typical operation of this integration is to first encrypt the source data using a secret key which is available only at the end nodes, and then to generate the redundant FEC data for loss recovery purpose by encoding the encrypted data. Both the encrypted and redundant data are transmitted along the network path and the receiver processes the received data in a reverse order (i.e., FEC decoding and decryption). In [13], an image-coding scheme has been proposed to provide encryption and FEC based on Error Correction Codes (ECCs) over noisy channels. Related works in [14, 15] use turbo-codes-based error control scheme to combine with encryption for secure data transmission. Moreover, the cryptographic encryption scheme based on Advanced Encryption Standard (AES) [16] and the FEC protection scheme using turbo codes have been integrated to ensure a reliable and secure transmission [17]. Although the joint encryption and FEC scheme is effective enough, several performance problems arise in terms of computational cost and management cost. All costs contribute to the delay time, which is critical to the multimedia services, and complicate the IPTV system design. In general, the computational cost largely originates from the processing overhead including FEC encoding/decoding and encryption/decryption, while the management cost derives from the generation of multiple keys, frequent key updates, channel feedback messages carrying network conditions, and so on. In [18, 19], an iterative decoding approach for digital signatures has been developed to perform the error correction, in addition to the authentication capacity provided by the digital signature itself. However, this approach becomes more effective as an FEC scheme is present and most importantly the transmission data remains unsafe to the malicious attacks. It is therefore necessary to design a IPTV transmission system with light performance cost in delivering multimedia content securely and reliably.

In this paper, we propose a security-enhanced FEC scheme which achieves a secure and reliable transmission for valued IPTV content, by means of packet-level Reed-Solomon (RS) codes [20] with a set of security constraints on the FEC coding parameters. The proposed secure FEC focuses on providing the content or service protection to prevent malicious users from acquiring the unauthorized data, while aiming at improving data goodput by recovering the potential transmission errors/losses. Two key features of the secure FEC are (1) to transmit FEC-encoded data only and hence the original content data are prevented from exposing to the malicious users directly and (2) to deliberately control the amount of FEC-encoded data so that the error correction capacity provided by the FEC-encoded data fails to reconstruct source content data. As to the authorized user, the successful data reconstruction relies on an additional data storage between the content server and user. The experimental results show that the proposed secure FEC obtains the same performance as the joint AES encryption scheme with 128-bit key and the packet-level FEC scheme based on Reed-Solomon codes, in the data transmission.

The remainder of this paper is organized as follows. Section 2 reviews the standard packet-level FEC protection scheme using Reed-Solomon codes. Section 3 introduces the proposed secure FEC scheme. Section 4 describes the exposure rate of source data for measuring the security level in this paper and establishes an analytical model associated with the exposure rate. The performance evaluation results are presented and discussed in Section 5. Finally, Section 6 provides some brief concluding remarks and future works.

2. Standard FEC

Without loss of generality, we use systematic Reed-Solomon erasure codes RS (n, k_1) to protect multimedia data from channel losses. The RS encoder chooses k_1 multimedia data items as an FEC block and generates $(n - k_1)$ redundant data items for the block. Every data item has its own sequence number used to indicate the corresponding position within the block. With this position information, the RS decoder can locate the position of the lost items and then correct up to $(n - k_1)$ lost items. Furthermore, a packet-level RS code is applied as FEC since it has a high efficiency over error-prone channels [21]. Figure 1 illustrates the operations of packet-level FEC scheme. Packet-level FEC schemes group the source data packets into blocks of a predetermined size k_1 and then encode $n = k_1 + h_{\text{std}}$ packets for network transmission, where $h_{\text{std}} \geq 0$ is the number of redundant packets. The coding rate is thus defined as k_1/n. Provided that k_1 or more packets are successively received, the block can be completely reconstructed. In the standard packet-level FEC, given the target recovery probability R_{std}, the estimated packet loss rate P_B and fixed k_1, the lower bound on n can be computed in the sender using

$$R_{\text{std}}(n, k_1, P_B) = \sum_{i=k_1}^{n} \left[\binom{n}{i} (P_B)^{n-i} (1 - P_B)^{i} \right]. \quad (1)$$

On the other hand, the feedback packets are sent periodically from the receiver to the sender in order to obtain the timely channel information about P_B. Note that packet-level FEC extends the media stream simply by inserting redundant packets into the stream, and, therefore, the method requires only minor modification to the source packets.

3. Secure FEC

The secure FEC scheme aims at supporting reliable and secure transmission for multimedia IPTV flows. To achieve the secure transmission, the proposed FEC scheme is based on the packet-level RS codes and has two features: (1) only the

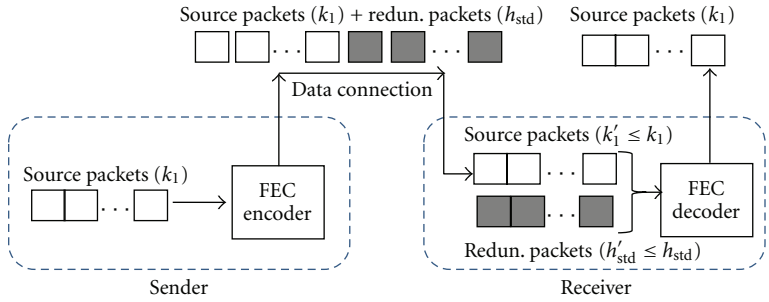


Figure 1: Overview of standard packet-level FEC scheme. This figure shows the FEC coding operations at both the sender and receiver. The maximum amount of loss packets that can be recovered is h_{std}.

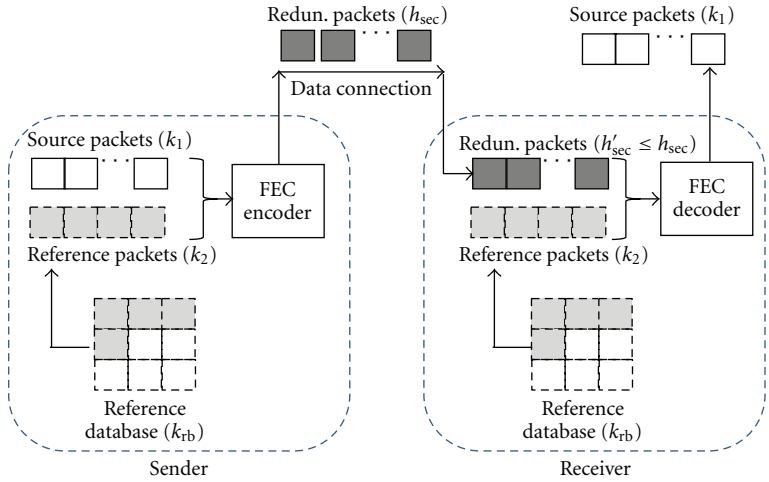


Figure 2: Overview of secure FEC scheme. Note that the reference packets k_2 are included in the FEC encoding/decoding, and the sender transmits redundant packets h_{sec}.

redundant data are delivered along the transmission path; in other words, the original source data are used in the encoding stage, and (2) both the data sending side and data receiving side need to maintain a consistent reference database where the reference data are selected to perform the FEC encoding with the source data at the data sending side, and the FEC decoding with the received redundant data at the data receiving side. Transmitting redundant data can avoid that the malicious host directly inspect the content of source data. It is noted that in the standard FEC, the transmission data include source and redundant data. Furthermore, the use of reference data in the FEC encoding/decoding stage causes the FEC decoding failure for the malicious host even if the malicious host attempts to decode the intercepted redundant data. Figure 2 illustrates the operations of secure FEC. The detained procedures can be summarized into five steps.

(1) Both the data sending side and receiving side have the similar k_2 reference packets.

(2) The data sending side generates the FEC redundant packets h_{sec} based on the source packets k_1 and the reference packets k_2.

(3) The data sending side transmits h_{sec} redundant packets through the network to the data receiving side.

(4) The data receiving side receives h_{sec}' packets and $h_{sec}' \leq h_{sec}$.

(5) The data receiving side uses the reference packets k_2 and the received packets h_{sec}' to reconstruct the source packets k_1.

According to the procedures described above, the condition that a block can be successfully recovered is given by

$$h_{sec} + k_2 \geq k_1 + k_2 \longrightarrow h_{sec} \geq k_1. \tag{2}$$

To prevent that the malicious host intercepts the transmitted packets h_{sec} between the data sending side and data receiving side, the value of h_{sec} must not exceed the amount of FEC-encoded source packets. That is

$$h_{sec} < k_1 + k_2. \tag{3}$$

Then the recovery probability in the secure FEC is shown as follows:

$$R_{sec}(h_{sec}, k_1, P_B) = \sum_{i=k_1}^{h_{sec}} \left[\binom{h_{sec}}{i} (P_B)^{h_{sec}-i} (1-P_B)^{i} \right], \quad \text{subject to } k_1 \leq h_{sec} < k_1 + k_2. \tag{4}$$

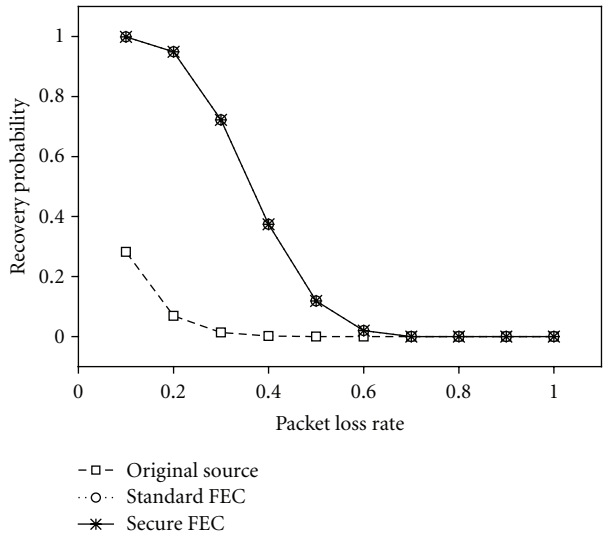


Figure 3: Coding rate for both the standard FEC and secure FEC is 2/3 with $k_1 = 12$.

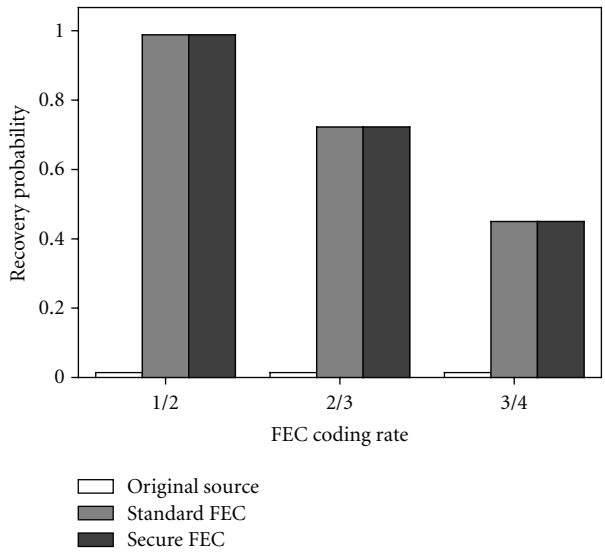


Figure 4: Comparison of recovery probability with varied FEC coding rates, when keeping $k_1 = 12$. The packet loss rate is fixed to 0.3.

According to (4), the amount of reference packets k_2 determines the efficiency of the secure FEC scheme since k_1 is typically a predefined value. Larger the value of k_2, higher the FEC recovery rate for a given packet loss rate P_B.

In keeping the consistent reference database between connection ends, the reference data can be initially set up as the secure FEC is installed to start its service and could be updated or expanded by selecting reference data from the reconstructed source data. It is noted that the source data are available only at the connection ends under the decoding constraint on the amount of redundant data (i.e., $k_1 \leq h_{\text{sec}} < (k_1 + k_2)$).

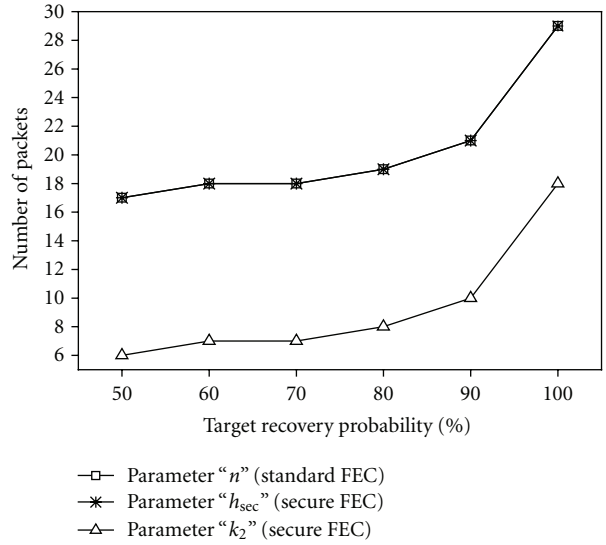


Figure 5: Observation on parameter changes with varied target recovery probabilities. The values of k_1 and P_B are 12 and 0.3, respectively.

4. Exposure Rate

In this section, we calculate the exposure rate to observe the degree of data inspection for the malicious host. For a data flow transmitting the source packets k_1 along the data path, the exposure rate (ER) can be easily obtained as the malicious host intercepts k_1' packets:

$$\text{ER}_{\text{src}}(k_1', k_1) = \frac{k_1'}{k_1}. \tag{5}$$

Let us assume that the malicious user can intercept the transmission packets in the presence of packet loss rate P_B. Then the value of k_1' can be computed as $k_1' = k_1 \times (1 - P_B)$ and (5) becomes $\text{ER}_{\text{src}}(k_1', k_1) = 1 - P_B$. The exposure rate represents the degree that the source data are exposed to any malicious host with the data interception capacity. As the value of ER approaches to 1, the malicious host can inspect more source content.

In the standard FEC, the delivery blocks inspected by the malicious host fall into one of two different categories: (1) the block is successfully reconstructed and (2) the block is not successfully decoded since the number of received packets is less than the number of source packets. In the first category, all k_1 source packets are completely reconstructed and the expected number of source packets, $E_{\text{FEC}(n,k_1),1}$, can be calculated as

$$E_{\text{FEC}(n,k_1),1} = k_1 \times R_{\text{std}}(n, k_1, P_B). \tag{6}$$

As to the second category, the number of lost packets is greater than $n - k_1$ within n transmitted packets and the

expected number of source packets, $E_{\mathrm{FEC}(n,k_1),2}$, is derived as follows:

$$E_{\mathrm{FEC}(n,k_1),2} = \frac{k_1}{n} \times \sum_{j=n-k_1+1}^{n} \left[\binom{n}{j} \times P_B^j \times (1-P_B)^{n-j} \times (n-j) \right]. \tag{7}$$

Therefore, the total expected number of source packets after decoding an FEC block is given by

$$E_{\mathrm{FEC}(n,k_1)} = k_1 \times R_{\mathrm{std}}(n,k_1,P_B) + \frac{k_1}{n} \times \sum_{j=n-k_1+1}^{n} \left[\binom{n}{j} \times P_B^j \times (1-P_B)^{n-j} \times (n-j) \right]. \tag{8}$$

Then, the exposure rate for an FEC block with k_1 source packets and n total transmission packets is given by

$$\mathrm{ER}_{\mathrm{std}}(n,k_1) = \frac{E_{\mathrm{FEC}(n,k_1)}}{k_1}. \tag{9}$$

For our proposed secure FEC scheme, only FEC-encoded redundant packets are injected into the transmission channel, and the amount of injected packets has to be less than the sum of total source packets $(k_1 + k_2)$ for FEC encoding. It is noted that an FEC block can be completely reconstructed at the data receiver only when the amount of received packets is not less than the amount of total source packets. Letting the amount of intercepted packets be h'_{sec} in the secure FEC, we can obtain the following relation

$$h'_{\mathrm{sec}} \le h_{\mathrm{sec}} < k_1 + k_2. \tag{10}$$

Based on the relation above, in the secure FEC scheme, the malicious host receives ER = 0 since the malicious host cannot reconstruct the source packets k_1 with the intercepted packets h'_{sec}, and all intercepted packets are FEC-encoded redundancies. Considering that the malicious host might have k'_2 reference packets and $0 \le k'_2 \le k_2$, the recovery probability for the malicious host with k'_2 is computed as

$$R_{\mathrm{sec}}(h_{\mathrm{sec}},k_1,k'_2,P_B) = \begin{cases} 0, & \text{if } h_{\mathrm{sec}}+k'_2 < k_1+k_2, \\ \sum_{i=k_1+k_2-k'_2}^{h_{\mathrm{sec}}} \binom{h_{\mathrm{sec}}}{i} \times P_B^{h_{\mathrm{sec}}-i} \times (1-P_B)^i, & \text{if } h_{\mathrm{sec}}+k'_2 \ge k_1+k_2. \end{cases} \tag{11}$$

Then the exposure rate for the malicious host is given by

$$\mathrm{ER}_{\mathrm{sec}}(h_{\mathrm{sec}},k_1,k'_2,P_B) = \begin{cases} 0, & \text{if } h_{\mathrm{sec}}+k'_2 < k_1+k_2, \\ \left(k_1 \times R_{\mathrm{sec}}(h_{\mathrm{sec}},k'_2,P_B) + \frac{k_1}{h_{\mathrm{sec}}} \times \sum_{j=h_{\mathrm{sec}}+k'_2-(k_1+k_2)+1}^{h_{\mathrm{sec}}} \left[\binom{h_{\mathrm{sec}}}{i} \times P_B^i \times (1-P_B)^{h_{\mathrm{sec}}-i} \times (h_{\mathrm{sec}}-i) \right] \right) / k_1, & \text{if } h_{\mathrm{sec}}+k'_2 \ge k_1+k_2. \end{cases} \tag{12}$$

5. Performance Analysis and Discussions

In this section, the performance of the proposed secure FEC scheme has been evaluated in terms of FEC recovery capacity and data exposure degree. The standard FEC and secure FEC employed packet-level RS codes. In the standard FEC, the values of parameters (k_1, n) were set to $(12, 18)$, and in the secure FEC, the values of k_1 and h_{sec} were 12 and 18, respectively.

5.1. FEC Recovery Capacity. To observe the FEC capacity of the proposed scheme, we compare the secure FEC with the standard FEC and the original source flow. For the original source flow, the source packets are directly transmitted into the network, while the standard FEC transmits both the source packets and redundant packets. Figure 3 shows the results of the recovery probability as the packet loss rate varies. In Figure 3, all source packets are nearly lost as the packet loss rate is larger than 0.3. For the standard FEC and the secure FEC, both schemes have the decay curve as the packet loss rate increases and their curves are exactly the same for all values of packet loss rates. It is noted that the standard FEC has the loss recovery capacity of $(n-k_1)$ packets while the loss recovery capacity in the secure FEC is given by $(h_{\mathrm{sec}} + k_2) - (k_1 + k_2)$ and therefore $(n - k_1)$. As shown in Figure 3, based on the assumption that both schemes require

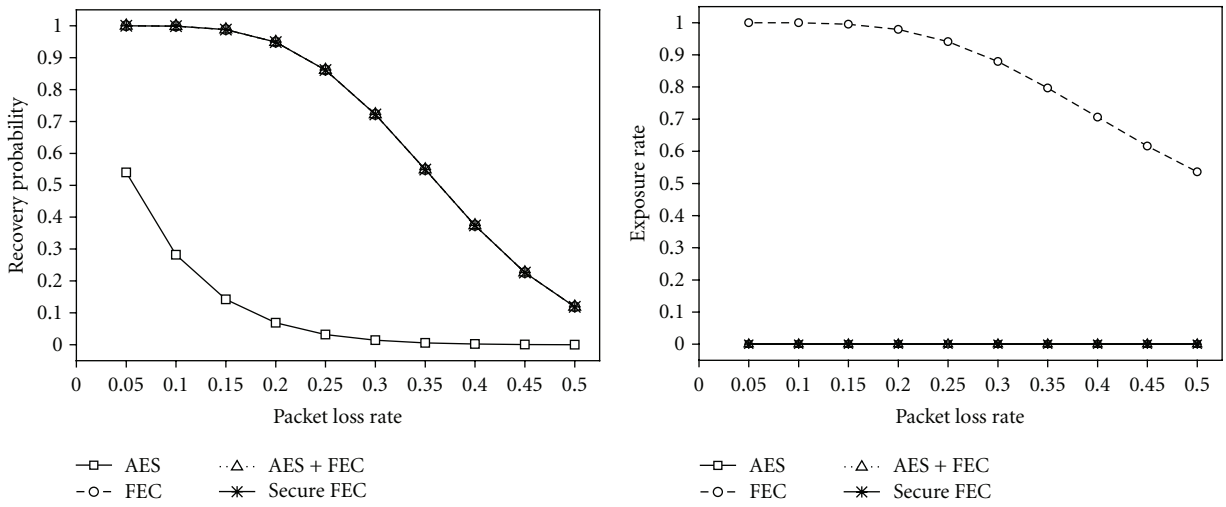


Figure 6: System performance comparison with varied packet loss rates. (a) Recovery probability; (b) exposure rate. Noted that label "FEC" represents the standard FEC.

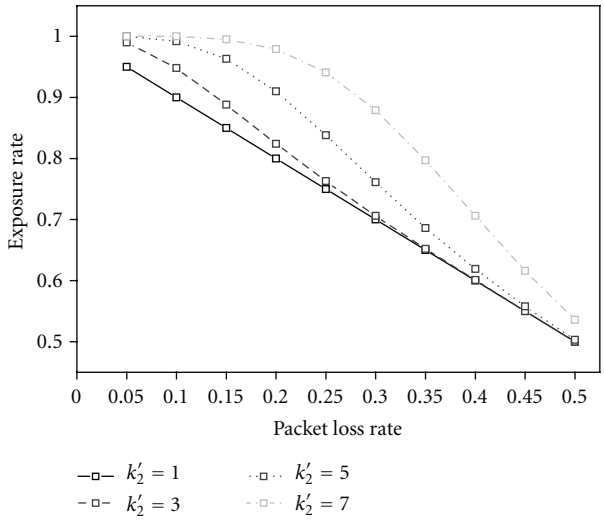


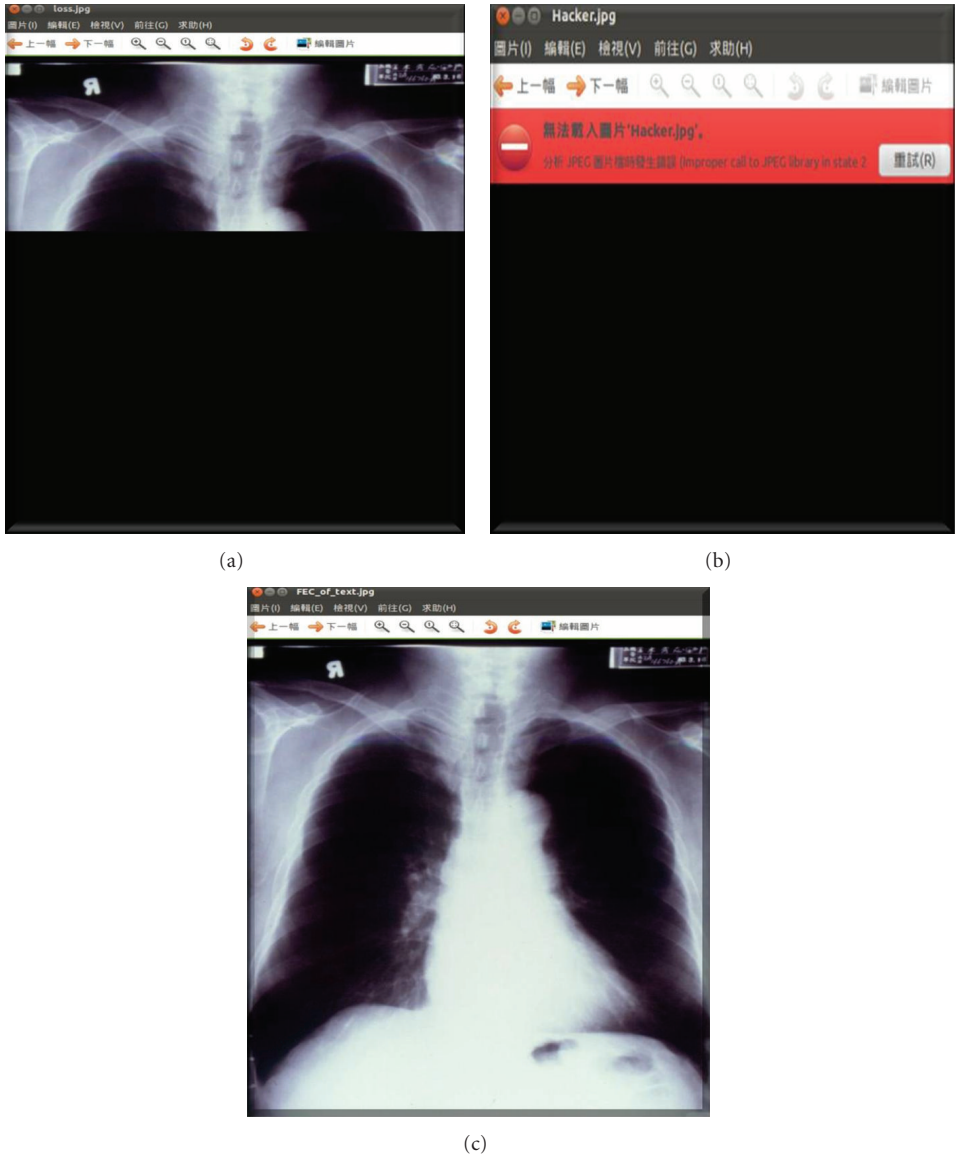
Figure 7: Exposure rate performances when different k_2' are applied to the secure FEC. This figure shows the performance impact as the reference packets are leaked to the malicious user.

the same bandwidth consumption (i.e., $h_{\text{sec}} = n$), the secure FEC can obtain the similar performance as the standard FEC. The similar observations can also be found in Figure 4. Figure 4 shows the results of the recovery probability for three FEC coding rates of 1/2, 2/3, and 3/4.

To study the operating behavior of the secure FEC, Figure 5 shows the values of parameters (n, h_{sec}, k_2) in packets as the target recovery probability is given. For the secure FEC, the required redundant packets h_{sec} are increased in order to achieve a higher recovery probability. Meanwhile, to ensure the secure transmission, the amount of reference packets k_2 needs to be increased accordingly. It is worth to note that the necessary condition of h_{sec} used in the secure FEC to avoid the successful FEC decoding by the malicious host is $h_{\text{sec}} < (k_1 + k_2)$, and the lower bound of k_2 is hence $k_2 > (h_{\text{sec}} - k_1)$. The curve of k_2 presented in Figure 5 is plotted by using its minimum value for a given target recovery probability (i.e., $k_2 = (h_{\text{sec}} - k_1) + 1$).

5.2. Data Exposure Degree. We then compare the proposed secure FEC with the encryption scheme, and the joint encryption and FEC scheme. In this study, AES with 128-bit key and packet-level FEC using RS codes are considered. Throughout the evaluation, we assume that a malicious host is located at the receiver side and is capable of performing FEC decoding. Four cases are studied: AES, standard FEC, joint AES and standard FEC, and secure FEC. Figure 6 shows the performance results in terms of recovery probability and exposure rate, from the perspective of a malicious host. From Figure 6, it can be seen that (1) AES has a exposure rate of 0 to guarantee the secure transmission in Figure 6(b) and in Figure 6(a), it has the much lower recovery probability than other three cases; (2) in Figure 6(b), standard FEC obtains the higher values of exposure rates than other cases with secure protection capacities, and as the packet loss rate increases, the exposure rate of FEC is decreased since the recovery probability of FEC is decreased accordingly to receive less source data for the malicious host; and (3) the secure FEC achieves the same performance as the joint AES and FEC scheme in Figures 6(a) and 6(b) to ensure the secure and reliable transmission.

Figure 7 shows the performance impacts when the malicious host is assumed to be capable of acquiring the reference packets. As shown in Figure 7, leaking more reference packets has a higher probability to expose source data to the malicious host. Furthermore, a higher exposure rate is also observed in the presence of lower packet loss rate because the FEC process at the malicious host is easier to reconstruct the source data.



(a) (b)

(c)

Figure 8: Snapshots of experiment results at three different receiving sides. (a) AES receiver without FEC capacity; (b) malicious receiver with FEC capacity; (c) secure FEC receiver.

5.3. Implementation and Experimental Results. To examine the effectiveness of our proposed secure FEC, the secure FEC scheme was implemented on the Linux platform and employed to transmit a sequence of images. In the experimental setup, five machines were connected with a Fast Ethernet LAN. They included an AES sender, an AES receiver, a secure FEC sender, a secure FEC receiver, and a malicious receiver attempting to peak the transmission data. The packet size is 1246 Bytes and all receivers apply the same packet loss traces of $P_B = 0.1$ to the received packet stream.

Figures 8(a)–8(c) presents the snapshots for the AES receiver, malicious receiver, and secure FEC receiver, respectively. From Figure 8, we can observe that (1) the AES receiver can only obtain a part of source packets after decrypting the received data, in the presence of packet loss; (2) the malicious receiver is unable to inspect the content of the transmitted data for either the AES connection or the secure FEC connection; and (3) the secure FEC receiver can receive the complete source data after the successful FEC reconstruction.

6. Conclusions

In this paper, a novel FEC scheme, which is equipped with both the error correction and security-enhanced capacity, is proposed so as to provide the secure and reliable transmission for valued IPTV content. We have derived the mathematical model to calculate data recovery rate and exposure rate for performance analysis purpose and conducted experiments to demonstrate the validity of the proposed secure FEC. To conclude, the secure FEC can protect the content data against the transmission losses and the unauthorized

access. Our future works are (1) to further study the secure FEC applications on the security issues such as authentication and data alteration and (2) to incorporate with encryption and watermarking to achieve robust security promise to end users while the overall performance cost can be minimized.

Acknowledgment

This work was supported by the National Science Council, Taiwan, under Grant no. NSC100-2221-E-241-014.

References

[1] J. Maisonneuve, M. Deschanel, J. Heiles et al., "An Overview of IPTV Standards Development," *IEEE Transactions on Broadcasting*, vol. 55, no. 2, pp. 315–328, 2009.

[2] M. Jeffrey, S. Park, K. Lee, G. Adams, and S. Savage, "Content security for IPTV," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 138–146, 2008.

[3] S. O. Hwang, "Content and service protection for IPTV," *IEEE Transactions on Broadcasting*, vol. 55, no. 2, pp. 425–436, 2009.

[4] H. Zhang, C. Chen, L. Zhao, S. Yang, and L. Zhou, "Content Protection for IPTV-current state of the art and challenges," in *Proceedings of the IMACS Multiconference on Computational Engineering in Systems Applications (CESA '06)*, pp. 1680–1685, Beijing, China, October 2006.

[5] M. Ellis and C. Perkins, "Packet loss characteristics of IPTV-like traffic on residential links," in *Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC '10)*, Las Vegas, Nev, USA, January 2010.

[6] M. Cha, G. Choudhury, J. Yates, A. Shaikh, and S. Moon, "Case study: resilient backbone design for IPTV services," in *Proceedings of the International World Wide Web Conference, IPTV Workshop*, 2006.

[7] Society of Motion Picture and Television Engineers, "Forward error correction for real-time video/audio transport over IP networks," SMPTE specification 2022-1, 2007.

[8] Digital Video Broadcasting (DVB), "IP datacast over DVB-H: content delivery protocols," ETSI TS 102 472.

[9] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshmi, "Opportunistic encryption: a trade-off between security and throughput in wireless networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 313–324, 2007.

[10] M. Ruiping, L. Xing, and H. E. Michel, "A new mechanism for achieving secure and reliable data transmission in wireless sensor networks," in *Proceedings of the IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability*, pp. 274–279, Woburn, Mass, USA, May 2007.

[11] A. Neri, D. Blasi, L. Gizzi, and P. Campisi, "Joint Security and Channel Coding for Ofdm Communications," in *Proceedings of the European Signal Processing Conference (EUSIPCO'08)*, Lausanne, Switzerland, 2008.

[12] X. Zhu, Q. Sun, Z. Zhang, and C. W. Chen, "A joint ECC based media error and authentication protection scheme," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '08)*, pp. 13–16, Hannover, Germany, June 2008.

[13] C. Nanjunda, M. A. Haleem, and R. Chandramouli, "Robust encryption for secure image transmission over wireless channels," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, pp. 1287–1291, Seoul, Korea, May 2005.

[14] A. Neri, D. Blasi, P. Campisi, and E. Maiorana, "Joint authentication and forward error correction of still images," in *Proceedings of the European Signal Processing Conference (EUSIPCO'10)*, pp. 2111–2115, Aalborg, Denmark, August 2010.

[15] L. Yao and L. Cao, "Turbo codes-based image transmission for channels with multiple types of distortion," *IEEE Transactions on Image Processing*, vol. 17, no. 11, pp. 2112–2121, 2008.

[16] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer, 2002.

[17] H. Cam, V. Ozduran, and O. N. Ucan, "A combined encryption and error correction scheme: AES-turbo," *Journal of Electrical and Electronics Engineering*, vol. 9, no. 1, pp. 891–896, 2009.

[18] N. Zivic, "On using the message digest for error correction in wireless communication networks," in *Proceedings of the International Workshop on Wireless Distributed Networks*, Istanbul, Turkey, September 2010.

[19] N. Zivic and C. Ruland, "Parallel joint channel coding and cryptography," *International Journal of Computer Science and Engineering*, vol. 4, pp. 140–144, 2008.

[20] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," *ACM SIGCOMM Computer Communication Review*, vol. 27, no. 2, pp. 24–36, 1997.

[21] F. Borgonovo and A. Capone, "Efficiency of error-control schemes for real-time wireless applications on the Gilbert channel," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 1, pp. 246–258, 2005.