VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

AN SECURE MELP COMMUNICATION USING ECC AND FEC

Srinivasan Nagaraj[1] and G. S. V. P. Raju[2]
[1]Department of Computer Science Engineering, GMRIT, GMR Nagar, Rajam, AP, India
[2]Department of CS and ST, Andhra University, Vishakapatnam, India
E-Mail: sri.mtech04@gmail.com

ABSTRACT

The purpose of cryptographic research is to devise protocols that provide a confidential and authenticated transmission channel for messages over an insecure channel. ECC used for encryption and decryption. They are typically fast and are suitable for processing small storage data. Many problems can be solved using ECC. In this paper we developed a security algorithm using the feature of ECC algorithm to provide the security for MELP-compressed speech transmission in noisy channels in conjunction with a forward error control scheme called Hamming distance code. Forward error correction (FEC) is a system of error control for data transmission. FEC avoids retransmission of data, at the cost of higher bandwidth requirements on average and we also devised a method to reduce noise during communication.

Keywords: MELP, encryption, ECC, decryption.

INTRODUCTION

Forward error correction algorithms

The TC algorithms can be squared and used and non-squared QAM constellations and include both Full-Turbo coding and Multilevel Turbo Coding

- Low-Density-Parity-Check Codes (LDPC) Forward Error Correcting (FEC) algorithms are available in several forms LIKE Full-Low-Density-Parity-Check Codes and QAM constellations
- BCH error correction algorithm is available in several forms includes different forms for the encoder and decoder.
- **Reed Solomon (RS) coding**

Reed Solomon (RS) FEC algorithms are available in several formats which includes pure software and different levels of hardware complexity utilizing UDI instructions. This algorim algorithm depends on some of the properties of Galois Field (GF) operations.

MELP

The recently-selected U.S. federal standard for 2400 bps speech compression employs mixed-excitation linear predictive coding.

MELP interprets short segments of speech as the output of a linear filter with an appropriate excitation signal. The job of the encoder is to design the filter and select the excitation signal and then represent both as efficiently as possible with a frame" of binary data; at the decoder, the encoded description is used to synthesize the filter and apply the excitation signal, thereby generating the speech segment.

Each MELP frame consists of 54 bits and represents 22.5 msec of speech

- Twenty Five bits are used to index the Filter's line spectral frequencies (LSF's) with a multi-stage vector quantizer (MSVQ) consisting of four stages - a first stage of seven bits and three more stages of six bits each.
- Two gain parameters are used in each frame one Five bits and the other three bits.
- Seven bits are used to index the pitch parameter.
- In the voiced frames, eight bits representing Fourier coefficients of the excitation signal are included; also included in voicing frames is four bits for bandpass shaping and one bit to indicate when a periodic pulse train is to be used for the excitation signal.
- In unvoiced frames, thirteen bits are used for error control.
- Finally, a one-bit sync bit is included with every MELP frame.

PROPOSED METHOD OF IMPLEMENTATION

Implementation of filtering

Block error correction codes: Error detection requires blocks are retransmitted. It is inadequate for the wireless communication for two purposes be quite high, which would result.

a) The bit error rate on a wireless link is quite high and would result in a large number of retransmissions.
b) In some cases, like satellite links the propagation delay is very long when compared to the transmission time of a frame.

It is popular to correct errors without requiring retransmission.
Using the bits that were transmitted.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

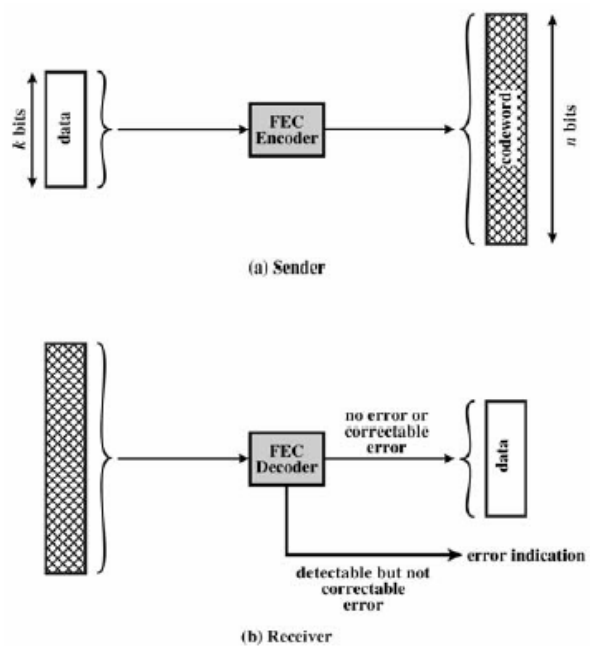


Figure-1. Forward error correction process.

This codeword might be similar to those forms the CRC approach above.

It might come from taking the original data, only adding extra bits. It may be created using a completely new set of bits.

The codewords is longer than the original data followed by the block is transmitted.

At the receiver, comparing the received codeword with the set of valid codewords can result in one of five possible outcomes

i. There are no bit errors

The received codeword are the similar to the transmitted codeword. The matching source data so as to codeword is output from the decoder.

ii. An error is detected and can be corrected

For the bit error patterns - That the received codeword is close to a valid codeword. Assumed that nearby codeword was sent. It also assumed that the source data for that codeword should be used.

iii. An error is detected but cannot be corrected

The received codeword is close to two or more valid codewords.We cannot assume which codeword was the original. It is determined only that error has detected and the frame should be retransmitted.

iv. An error is not detected

The error pattern occurs that transforms the transmitted codeword into another valid codeword. Then the receiver assumes no error has been occurred.

The output of the decoder is the source data for a wrong codeword.

v. The error is detected and is erroneously corrected

Block code principles

Hamming Distance

Given are two example sequences.

$v_1 = 011011$, $v_2 = 110001$

The Hamming Distance is can be defined as the number of bits which disagree.

$d(v_1 , v_2) = 3$

Decoding rule: Use the closest codeword (in terms of hamming distance).

The five bits in the codeword, there fore 2^5=32 possible received codewords.

Four are valid; the 28 others are come from bit errors.

In several cases, a potential received codeword is a Hamming distance of 1 from a valid codeword.

The code consisting of codewords represented by w_i, the minimum Hamming distance is defined as.

$$d_{\min} = \min_{i \neq j} \left[d(\mathbf{w}_i , \mathbf{w}_j) \right]$$

- For the example: $\mathbf{v}_1 = 011011$, $\mathbf{v}_2 = 110001$, $d_{min} = 3$.

The below formula used for utmost number of guaranteed correctable errors is

$$t_{corr} = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

- From the example, $t_{corr} = (3-1)/2 = 1$ bit error can be corrected.

PROPOSED METHOD OF IMPLEMENTATION

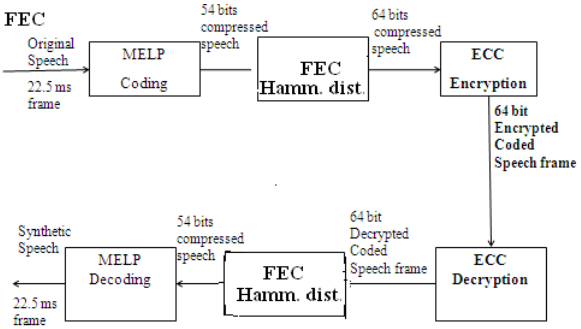


Figure-2. Block diagram for the system model.

Elliptic Curve Cryptography

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987) and Victor Miller (Miller 1986) independently proposed the public key cryptosystems using elliptic curve. The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem.

In the current paper for the purpose of encryption and decryption using elliptic curves we consider the equation of the form

$Y^2 = x^3+ax+b$

Elliptic Curve Domain Parameters are D = (q, FR, a, b, G, n)

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

- ***q***: prime power, that is q = p or q = 2^m, where p is a prime
- ***FR***: field illustration of the method used for representing field elements ∈ F_q
- ***a, b***: field elements, they specify the equation of the elliptic curve E over F_q,
- $y^2 = x^3 + ax + b$
- ***G***: A base point represented by G= (x_g, y_g) on E (F_q)
- ***n***: Generated Prime number.

Elliptic curve Named so because they are described by cubic equations o f the form $y^2 + axy + by = x^3 + cx^2 + dx + e$

In which all the coefficients are real numbers satisfying some of the simple conditions

- where single element denoted *O* and called the *point at infinity* or the *zero point* and Elliptic curves over finite field

- Define ECC over a finite field
- The elliptic group mod *p*, where *p* is a prime number
- Choose 2 nonnegative integers *a* and *b* are < *p* that satisfies $[4a^3 + 27b^2] \pmod p \neq 0$
- $E_p(a,b)$ denotes that the elliptic group mod *p* whose element (*x*,*y*) are pairs of non-negative integers less than *p* satisfying $y^2 \equiv x^3 + ax + b \pmod p$ with *O*.

Step-1: Data compression

The original speech is buffered into 22.5 ms frames and conceded through MELP coding filter. The 22.5 ms frame coded into 54 bits compressed speech frame.

Step-2: Forward error correction

In MELP algorithm, Forward Error Correction (FEC) is implemented in the unvoiced mode, the FEC of Hamming distance code is applied and its output is encrypted using ECC.

Step-3: Encryption using ECC: Encryption process is performed on the voice data.

Step-4: Decryption using ECC: Decryption process is performed on the Encrypted voice data.

RESULTS

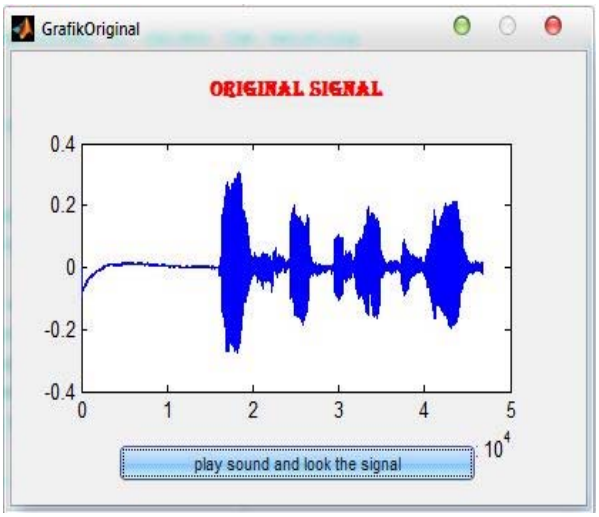


Figure-3. Signal processing.

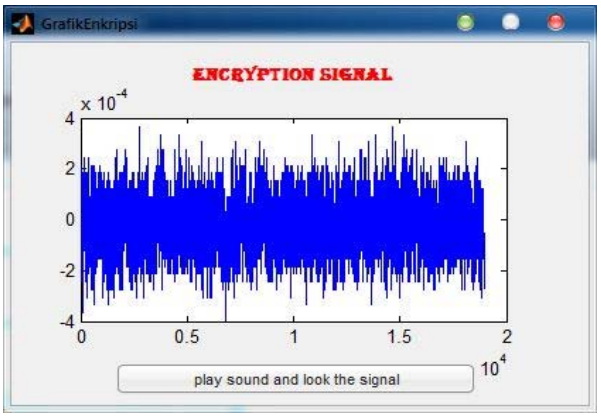
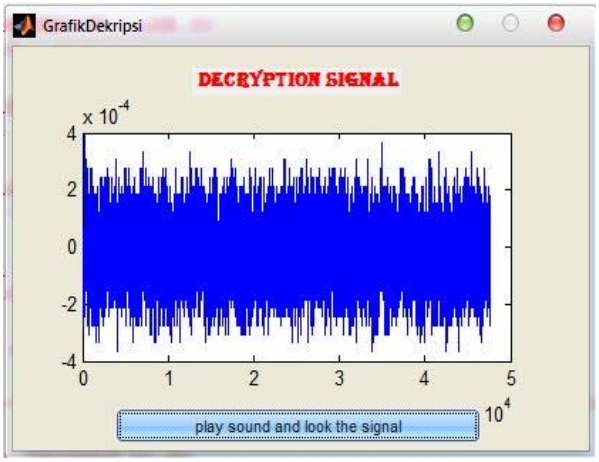


Figure-4. Encryption signal screen.



.

Figure-5. Decryption signal screen.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

CONCLUSIONS

MELP speech coder has been selected as the U.S. federal standard for 2400 bps speech compression. The quality of MELP-compressed speech when transmitted over noisy communication channels in conjunction with a different error control schemes. In this paper we developed a security algorithm using the feature of ECC to provide the security for MELP-compressed speech transmission in noisy channels in conjunction with a forward error control scheme Hamming distance code. We also devised a method to reduce noise during communication. Our proposed method is comparatively good performance at key generation and the onfidential data is highly safe and reliable. To adjust for this loss, we developed a noise reduction filter in MATLAB. This work presently implemented with ECC prime filed Approach but further extended ECC with GF field and also enhanced by making this method compatible to encrypt multimedia data which has to be transmitted securely over unsecured channels.

REFERENCES

[1] Stallings, W.: Cryptography and Network Security: Principles and Practices, 3rd edn. Pearson Education 2004.

[2] A New Substitution Block Cipher Using Genetic Algorithm, Srinivasan Nagaraj1, D.S.V.P. Raju2, and Kishore Bhamidipati- SPRINGER, 2013.

[3] Ye Zhu, Yuanchao Lu and AniVikram "On Privacy of Encrypted Speech Communication", Dependable and Science Computing IEE Transaction, Vol. 9, No. 4, July/August 2012.

[4] Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo random number generator. SIAM J. Compute 15(2), 364-383 1986.

[5] Cryptanalytic Attacks on Pseudorandom Number Generators John Kelsey *Bruce Schneier* David Wagner Chris Hal y.

[6] PENG Tan, CUI Huijuan, TANG Kun. 2010. Speech coding and transmission algorithm based on multi folded barrel shifting majority judgment; Journal of Tsinghua University (Science and Technology).

[7] JI Zhe, LI Ye, CUI Huijuan, TANG Kun. 2009. Leaping frame detection and processing with a 2.4 kb/s SELP vocoder; Journal of Tsinghua University (Science and Technology).

[8] Arundhati S. Mehendale and M. R. Dixit. 2011. Speaker Identification, Signal and Image Processing: An International Journal (SIPIJ). Vol. 2, No. 2, June 2011.

[9] Jelena NIKOLIC, Zoran PERIC. 2008. Lloyd-Max's Algorithm Implementation in Speech Coding Algorithm Based on Forward Adaptive Technique, INFORMATICA, 2008, Vol. 19, No. 2, 255-270.

[10] Wai C. Chu. 2003. Speech Coding Algorithms, Wiley Interscience.

[11] Ghosal Prasun, Biswas Malabika, Biswas Manish, "A Compact FPGA Implementation of Triple-DES Encryption System with IP Core Generation and On-Chip, Verification," in Proceedings of International Conference on Industrial Engineering and Operations Management, 2010.

[12] Tin Lai Win and Nant Christina KyaW "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR) ", World cademy of Science, Engineering and Technology, 2008.