ISSN 2250-3153

Recent Developments in Signal Encryption – A Critical Survey

S.Rajanarayanan and A. Pushparaghavan

Department of computer science and Engineering, Selvam College of Technology, Namakkal
srnarayanan_slm@yahoo.co.in

Abstract- In digitally modern world, the fundamental issue of multimedia data security (such as digital audio signals, images, and videos) is becoming a major concern due to the rapid development of digital communications and networking technologies. The methods and algorithms which are currently available for data protection uses cryptographic primitives for secure data transmission and reception by assuming that both sides must trust on each other. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. The major two conceptual blocks of cryptography is encryption and decryption. This is achieved by sending encrypted version of the data to the untrusted computers to process. Once when the computation process is completed on the encrypted data, the results will be sent back and the decryption is applied to extract the original data content. To ensure the decrypted result to be equal to the intended computed value, a structural method of encryption should be followed. Encryption is a technique which maintains confidentiality while sending and receiving data or storing the information. The principle of Kerckoffs' on the encryption states that the security must not rely on the obfuscation of code, but only on the secrecy of the decryption key. In this paper detailed description of symmetric and asymmetric encryption are given to provide a wider view of encryption techniques. The field of secure signal processing poses significant challenges for both signal processing and cryptography research; only few ready-to-go fully integrated solutions are available.

Index Terms- Encryption, Cryptography, Kerckoffs', Symmetric, Asymmetric

1. INTRODUCTION

Digital signal processing field has immensely wide range of applications including communication systems, multimedia data production, biological signal processing for health monitoring etc. Although these applications are widely developed, protection of information for secure communication is one of the major requirements. The methods and algorithms which are currently available for data protection uses cryptographic primitives for secure data transmission and reception by assuming that both sides must trust on each other. Using this technique, data cannot be accessed by third parties, but just not enough to provide complete security to the application.

Confidentiality of data should be ensured during communication and data storage while encryption is taken place. Recently, some additional features providing ability to delegate computations for encryption in untrusted computers or devices are added. This is achieved by sending encrypted version of the data to the untrusted computers to process. Once when the computation process is completed on the encrypted data, the results will be sent back and the decryption is applied to extract the original data content. To ensure the decrypted result to be equal to the intended computed value, a structural method of encryption should be followed.

Rivest et al. in 1978 proposed a homomorphic encryption [1] to solve this issue. Brickell and Yacobi in [2] pointed out some of the security weakness in the first proposals of Rivest et al. Followed the first attempt of Rivest et al, a numerous methods and algorithms have proposed to solve issues related to the data encryption on various contexts. These are: secret sharing schemes, threshold schemes [3], zero-knowledge proofs [4], oblivious transfer [5], commitment schemes [3], anonymity, privacy, electronic voting, electronic auctions, lottery protocols [6], protection of mobile agents[7], multiparty computation [3], mix-nets [8, 9], watermarking or fingerprinting protocols [10–11], and so forth.

2. FUNDAMENTALS OF ENCRYPTION

Encryption is a technique which maintains confidentiality while sending and receiving data or storing the information. The principle of Kerckoffs' on the encryption states that the security must not rely on the obfuscation of code, but only on the secrecy of the decryption key. In general, encryption techniques are classified into two broad categories: symmetric and asymmetric. The detailed explanation of these two types is given in the following section.

A. Symmetric Encryption

The term "Symmetric" states that both encryption and decryption of the data are carried out with the same secret key. Hence, the key must be known to both sender and the receiver in order to perform any secure communication. The major advantage of using symmetric encryption is for its fastness. However, it is not possible for two people who never met to use

such schemes directly. Block ciphers (AES [14, 15]) and stream ciphers (One-time pad [16], Snow 2.0 [17]), which are belongs to this category performs encryption faster.

B. Asymmetric Encryption

In terms of asymmetric encryption, the key used for encryption is different for it is used in decryption procedure. The encryption key is public as the decryption key remains private. Since there is no need of sender or receiver to agree on the sharing of secret key, these schemes are more functional than the symmetric techniques. More number of features are added to asymmetric schemes. However, asymmetric schemes have two major disadvantages; they are based on nontrivial mathematical computations, and much slower than the symmetric ones. RSA [18] and ElGamal [19] are the prominent algorithms belong to this category.

C. Issues of Encryption Performance

When compared block cipher against RSA algorithm, like AES it is typically 100 times faster while encryption and 2000 times faster while decryption, with about 60MB per second on a modest platform. Stream ciphers are even faster, some of them being able to encrypt/decrypt 100MB of data per second or more. Thus, the whole content of a DVD will take about a minute with a fast stream cipher encryption/decryption. In practice, it would require hours, or even days, to encrypt or decrypt for such huge amount of data when asymmetric encryption/decryption is used. Hence, the asymmetric cipher is used to encrypt only a short data, while the symmetric one is used for the longer one. The sender and the receiver do not need to share anything before performing the encryption/decryption as the symmetric key is transmitted with the help of the public key of the receiver. By combining the advantages of both efficiency of symmetric schemes and functionalities of the asymmetric schemes, performance of the encryption can be improved.

D. Encryption Security Issues

In first, Shannon [20] formalized the security of encryption schemes in his seminal paper. He introduced the notion of perfect secrecy/unconditional security. According to this, knowledge of a cipher text does not give any information either about the corresponding plain text or about the key. Estimation of the security level is necessary in order to evaluate how secures the encryption schemes. Different authors addressed this security level estimation on their papers. This estimation may not be sufficient for several reasons. First, there may be other ways to break the system than solving the reference mathematical problem [21, 22]. Second, most of security proofs are performed in an idealized model called the random oracle model. In recent, more realistic model called the standard model is used to perform proofs ([23], [24]). Usually, to evaluate the attack capacity of the opponent, we distinguish among several contexts [25]: cipher text-only attacks where the opponent has access only to some cipher texts, known-plaintext attacks where the opponent has access to some pairs of corresponding plaintext-cipher texts, chosen-plaintext attacks which is same as previous, but the opponent can choose the plaintexts and get the corresponding cipher texts, and chosen-cipher text attacks ,the opponent has access to a decryption oracle, behaving as a black-box, that takes a cipher text and outputs the corresponding plaintext.

E. Appropriate Encryption Technique Selection

Selection of a right encryption scheme involves consideration of many constraints such as time, memory, security, and so forth. The time and memory criteria are very important in highly constrained architectures, often encountered in very small devices (PDAs, smart cards, RFID tags, etc.). They are also very important when a huge amount of data is processed at the same time. Schemes such as AES or RSA are generally used because of their reputation, but it is also to be noted that new schemes are proposed each year. Also, any new encryption proposal should satisfy the following diversity. First, it is necessary in order to be able to face new kinds of requirements. Second, should be able to rely an attack breaks.

3. LITERATURE REVIEW

Cuomo et al. in 2008[26] proposed a feature-based data embedding framework that synchronizes both embedder and receiver for error correction. The method employs modification of pitch for data embedding and uses Davey and Mackay's codes for insertion, deletion, and substitution (IDS) for synchronization and error recovery. Also, performance of the presented algorithm is improved using the expectation-maximization algorithm at the receiver end by estimating the channel parameters for the IDS decoding. The proposed method is very robust to the low-bit-rate speech coding channels.

An algorithm that embeds the data in the phase of non-voiced speech was presented by Hofbauer et al. in 2009 [27]. The method replaces the autoregressive excitation signal of speech signal in a frequency sub-band, which is robust against band pass filtering channels. Several sets of pulse shapes are derived to prevent inter-symbol interference for creating pass band embedding signal by simple filtering. Location of the embedded data is detected using a marker based scheme without the insertions or deletions occurrence. Chen et al. in 2007[28] proposed a Vector quantization (VQ) of linear prediction coefficients (LPCs) based method for speech encryption. Secret key is generated using the vector quantization indices of neighboring frames derived from the natural speech's characters. Chen et al. in 2007[29] presented a Codebook-excited linear prediction (CELP)-based speech encryption algorithm. This proposed algorithm utilizes compressed speech data for insertion, deletion and replacement for data embedding. Initially, speech data are slatted into multiple speech frames groups. The data encryption in the current frame is generated using the feature, line spectrum frequency (LSF) extracted in the current frame, the extracted pitch from of the succeeding frame, the embedded data in the preceding frame and the location index of the current frame. Finally, some of the least significant bits (LSBs) indicating the excitation pulse positions or excitation vectors are substituted for the watermark.

Speech encryption based on the time-trajectory model of the sinusoidal components of voiced speech signals is addressed Laurent Girin et al. in 2007[30]. This global approach is called long-term (LT) model, which uses amplitude and phase parameters of the discrete cosine functions for each entire voiced

section of speech. Stankovic et.al in 2010 [31] proposed a unified encryption approach that can be used for different types of data such as audio, image or video based on multidimensional time-frequency analysis is presented over here. Speech signals utilize time-frequency analysis while space/spatial-frequency analysis is used for image encryption. The combination of both methods used in speech and image encryption is extended for video encryption. Encryption coefficients are selected by computing local frequency content of the signal. Also, non-stationary filtering of the host signal is carried out in order to provide imperceptibility of the encryption. A study on the perceptual watermarking impacts on the stationary audio signals was presented by Larbi et.al in 2005[32]. The study is based on stationary indices, which represent a measure of variations in spectral characteristics of signals, using time-frequency representations. Separation of multiple source audio signals from a mixture using the watermarking concept was presented by Parvaix et.al in 2010[33]. In their approach, a specific two level encoder-decoder procedure is discussed over here. At the encoder end, before the mixing of source audio signals, each signal is encrypted with set of parameters that gives additional information. Then, these encrypted signals are mixed and transmitted. At the receiver end, using the prior knowledge of the encrypted source signals, each signal is separated from the mixture. This method of separation is called informed source separation (ISS). Results obtained in this method shows high performances.

Xiangyang et.al in 2007[34] proposed a novel approach for adaptive blind digital audio encryption. The method uses support vector regression algorithm for the extraction of the embedded information. The signal to be encrypted is first embedded in the audio signal along the template information. Adaptive quantization according to the local audio correlation and human auditory masking is used for embedding the information. At the decoding, corresponding template feature is selected and SVR is trained. Then, this trained model is used to predict actual outputs of the embedded information. The main features of this method include inaudible, robustness and high practicability. In addition to these, the algorithm can also extract the embedded information without original audio help.

Chen et.al in 2008[35] presented an audio encryption method which solves the tradeoff between robustness and imperceptibility of the echo hiding method. The method combines analysis-by-synthesis approach, interlaced kernels, and frequency hopping in order to achieve high robustness, perceptual quality and security. During the embedding process, the algorithm not only considers the characteristics of the host signal, but also the various attacks of embedded audio signals. Also, the influence of host signals and various attacks on the embedded data are minimized by introducing the interlaced kernels. In addition to these two techniques, frequency hopping is used to increase the security and robustness of the proposed algorithm. In frequency hopping, each audio segment for embedding is established by combining the fractions selected from all frequency bands based on a pseudo noise sequence as a secret key. The presented algorithm is superior in terms of robustness, security, and perceptual quality.

Satti et.al in 2009[36] presented a method for scrambling the signal for secret data hiding using quasi-group. This is a multilevel indexed transformation which is very effective in destroying the structure of the input signal and, therefore, it can be used as an excellent encryption technique. A novel method that hides data in digital audio was presented by Malik et.al in 2007[37]. Their algorithm exploits the low sensitivity of the human auditory system for the distortion of phase. Data hiding is carried out using set of all pass filters and its pole-zero locations are chosen as parameters to encode the information. In the separation procedure, power spectrum of the audio signal is estimated in the z-plane away from the unit circle. The estimated power spectrum is used to find the pole locations of the all pass filters in decoding procedure. The results of the mentioned algorithm shows effectiveness to withstand data attacks and provides improved perceptual and robustness to the data hiding. A wavelet based Patchwork Method (MPM) for audio signal embedding is presented by Kalantari et.al in 2009[38]. The embedding process in their method uses two subsets features of the host signal. One subset is modified multiplicatively according to the embedding information while another one is not changed. The approximation coefficients of the wavelet domain are used to embed data. To achieve error free detection, data embedding is carried out only in the frames where the energy ratio of the subsets lies between two predefined values. The quality of the method is achieved using iterative algorithm and the quality is evaluated using Perceptual Evaluation of Audio Quality (PEAQ) method at each iteration level. The algorithm presented in this paper is high robustness and provides inaudibility of the watermark insertion.

A binary information hiding system in the audio data was presented Baras et.al in 2006[39]. Their innovative embedding method consist various stages. A procedure for controlling inaudibility of the embedding, robustness of the system is maximized using informed embedding method and an efficient synchronization mechanism for low computation cost. The mentioned algorithm is evaluated on a real time audio signal and shows improved inaudibility, transmission reliability and computation cost. A modified Patchwork Algorithm for audio encoding was presented by In-Kwon Yeo et.al in 2003[40]. This statistical algorithm uses not only discrete cosine transform, but also discrete Fourier and wavelet domain. This enhanced Patchwork algorithm withstands various attacks defined by the Secure Digital Music Initiative (SDMI).

Sridharan et.al in 1991[41] presented a DFT based speech encryption system. Coefficients of DCT are modified to achieve the desired permutation in their method. The presented algorithm is used in band limited telephone channel for its low residual intelligibility and good recovered voice quality. Servetti et.al in 2002[42] proposed a speech encryption method based on the low complexity perception based partial schemes. In their proposed algorithm, the speech signal which is compressed by ITU-T G.729 standard is partitioned into two classes. These are: one, to be encrypted which is most perceptually relevant and another one is to be left unprotected. A two level partial encryption techniques are carried out, a low-protection and high-protection technique. The first one is used to prevent eavesdropping and the second one is used for performing full encryption of the

compressed bit stream. Goldburg et.al in 1993[43] proposed an analog speech encryption based on the discrete transform domain is discussed. In their method, four discrete orthogonal transforms have been evaluated for their suitability in encryption and found that DCT is the best transform to use in transform based encryption. Scrambling of the speech is achieved by modifying the DCT coefficients in this paper. Dawson et.al in 1991[44] described a discrete cosine transform based speech-encryption system suitable for communication over band-limited telephone channels. An energy modification technique is presented which dramatically reduces the residual intelligibility of the scrambled speech. In addition, a method used to reduce the undesirable effects of band limitation is described. Simulation results are included which demonstrate the improved performance of the scheme.

Goldburg et.al in 1993[45] investigated a technique for the frequency domain speech encryption. This method investigates codebook vector which is similar to the vector quantization of speech that can be used in speech scramblers attacks. The proposed algorithm shows improved security in the frequency domain speech encryption. Li et.al in 2003[46] proposed a novel condition for synchronization and stabilization of Chua's cryptosystems which is used for multimedia encryption. As per their concept, a magnifying glass is used to enlarge and observe any mismatch in the parameter and hence increase the security level and sensitivity of the Chua's cryptosystem.Chung-Ping Wu et.al in 2005[47] proposed an algorithm which uses two approaches for combining encryption and compression of multimedia data. They are selective encryption and modified entropy coders. First, the limitation of the selective encryption is examined using cryptanalysis, and, using multiple statistical models, entropy coders are turned into encryption ciphers. A high level security is achieved in this technique without affecting the performance and computational speed of the encoders.

A wavelet based approach for speech encryption was proposed by Shahreza et.al in 2008[48]. The algorithm utilizes Least Significant Bits of detail coefficients of the wavelet transform to achieve encryption in an adaptive manner. Since, the information is not hidden in the silent parts of the speech signal; there is no need of silent detection algorithms when using this approach. When compared to a typical wavelet domain LSB, this method achieves zero error in hiding/unhiding process. Also, the SNR measure of the encrypted signal using this method implies that the imperceptible level of the audio is high than original audio. A method using augmented identity matrix for the speech encryption was presented by Tingting Xu et.al in 2009 [49]. By analyzing the redundancy parameters of the coded speech signal, enhanced encryption is achieved with low computational complexity in real time applications using this method.Shirali-Shahreza et.al in 2010[51] proposed a novel algorithm for speech signal encryption. In their method, information hiding is achieved by changing the silent intervals of the speech signal. The main features of this method are robustness MPEG-1 layer III (MP3) compression, low computation without scarifying the quality of the speech.

Aoki in 2010[51] proposed a loss less steganography technique for G.711 codec which is mainly used in telephony systems such as VoIP. The LSB of the redundancy parameters of G.711 is exploited in order to achieve encryption.

Chai Peiqi et.al in 2005[52] proposed a novel blind speech authentication algorithm which comprises linear predictive coding (LPC) and least significant bit (LSB) steganography. In this method of speech authentication, the encryption is carried out by replacing the LSB with extracted invariable LPC prediction error feature of the speech signal. Djebbar et.al in 2010[53] addressed a method to limits the impact of large data embedding on to the wideband speech signal. The maximum number of bits that can be confined without inducing any noticeable distortion on the speech is first determined and the encryption is applied only on selected frequency components. The algorithm is very robust against noise addition, achieves high security without affecting the quality of the noise signal.

Yong Feng Huang et.al in 2011[54] presented a data embedding algorithm using G.723.1 codec mainly used in Voice over Internet Protocol (VoIP). The algorithm analyzes the inactive frames of low bit rate audio streams for the embedding process. The proposed algorithm in this paper achieves high perfect imperceptibility with a high data embedding capacity. Another speech encryption on VOIP was presented by Hui Tian et.al in 2009[55]. Their algorithm uses well known least significant bits substitution approach for information embedding with a trade between well security and high hiding capacity. By distributing the LSBs non-uniformly, the algorithm provides resistance to the statistical detection of the data with the use of M-sequence technique. The encrypted information is accurately retrieved using a RSA key agreement and the synchronized sequence transmission techniques. The proposed system is effective and provides good security and transparency.

Zhi-jun Wu et.al in 2003[56] presented an analysis by synthesis approach for speech information embedding. This approach provides the ability to embed dynamic secret speech information onto the host speech signal with good achievement in efficiency and quality. Rui Miao et.al in 2011[57] presented an effective speech encryption using least significant bits substitution in VOIP. Unlike a conventional LSB encryption which uses flat regions of speech signal for embedding, the presented method suggests a adaptive steganography scheme that selects lower embedding bit rate in the flat segments, while the sharp segments can camouflage more secret message. A study that analysis and encrypts message on the unused bits of G.723.1 codec audio frames was presented by Huang et.al in 2011[58]. In this novel analysis, the authors suggest second detection and regression analysis in order to achieve encryption over VOIP. A system for speech information hiding telephone was presented by Wu Zhi-jun et.al in 101[59]. The overall system is designed using one fixed point DSP TMS320C54x and three floating DSPs TMS320C31, and a single-chip micro-controller for embedding the information. Hui Tian et.al in 2008[60] proposed another speech encryption method for VOIP using LSBs. The system presented by them can not only protect the information, but can also withstand both extraction attack and deceptive attack effectively.

Skopin et.al in 2010[61] proposed an analog audio steganography, which allows embedding human speech signal to the sound file. The authors presented two approaches for the

speech hiding. In their first approach, unheard places of human speech in a music spectrum is analyzed and used for speech encryption using the technology called spectrum shift. In the second method of their proposal, a technique called spectrum spreading is used for the purpose of encryption on a new signal which is obtained by inverse Fourier transform of combined human voice harmonics and music. A study that addresses solution for speech quality degradation due to the packet loss in VOIP using steganography was presented by Aoki in 2007[62]. The authors suggest a technique called packet loss concealment for the reduction speech quality degradation. Sinha et.al in 2006 [63] attempted a speech signal encryption onto the image using the concept neuro-genetic speech processing. In this method, null ciphers are extracted from the voice signal of Bengali speaker using neuro genetic approach and then veiled with an image.

4. COMPARATIVE SECURITY TECHNIQUES

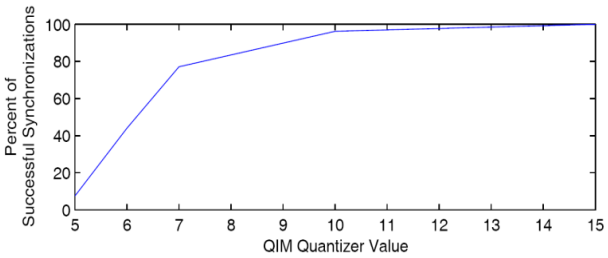

Fig.1 Monte-carlo simulation results illustrating dependence of synchronization performance on QIM step size.

To further examine the performance of the Monte-Carlo simulations were performed and the percent of times the successful synchronization and data recovery was accomplished was determined. This percentage was computed for different value of the QIM embedding steps Δ for the case of no compression. The corresponding result are shown in Fig.1. Note that the performance degrades with decrease in QIM steps size as expected. For $\Delta = 15$ no cases of failed synchronization / recovery were observed and for $\Delta=10$ over 95% of times synchronization was regained. To evaluate the pitch-modificaton based speech watermark with synchronization.[26]

CDW (CONTENT DEPENDENT MULTIPURPOSE WATERMARKING).Ten varieties of gray-scale cover images of size 512 X 512 were used. One of them was watermarked, estimated, and copied to the other 9 unwatermarked images to form 9 counterfeit stego images. By repeating this procedure,90 counterfeit stego images were obtained. All BERs obtained by applying IWCA to our method fell within [0.4847 0.5198] (all were sufficiently larger than T), which indicates the absence of watermarks. Obviously, the experimental results are consistent with the analytic result (Eq. (4)) [27].

The implementation target device is the TMS320C5502 digital signal processor, which is a commercially popular device in low-power areas. Under the assumption that the PE algorithms are implemented on this device using the C language, the execution cycle counts of the PE algorithms with the different PESs are compared in Table 3. To quantify the computational complexity in an actual condition, the cycle counts were measured during a three-minute period, which is equivalent to the average call duration. Implementation results show that, compared to the FE algorithm, the PE algorithm with the class 3 PES only requires nearly 40% cycle counts.[42]

Table 1. Comparison of computational load of the PESs

PES	Encryption rate(%)	Cycle counts per call(3min)	Cycle count ratio (%)
Class 1	5	3,528,000	26.20
Class 2	10	4,284,000	31.82
Class 3	20	5,292,000	39.30
Class 4, LPS	30	6,480,000	48.13
Class 5	40	7,704,000	57.22
HPS	45	8,388,000	62.30
FE	100	13,464,000	100.00

Table 2. Number of cycles for the key expansion

#cycles (key,block length)	AES CD(Ansi C)		BrianGladman (VC++)	
	Rijndael	Rijndael-1	Rijndael	Rijndael-1
(128,128)	2100	2900	305	1389
(192,128)	2600	3600	277	1595
(256,128)	2800	3800	374	1960

The cipher and its inverse take the same time. The difference in performance that is discussed in the section on mplementation, is only caused by the difference in the key set-up. Table 3 gives the figures for the raw encryption, when implemented in C, without counting the overhead caused by the AES API.[14]

Table 3.Cipher (and inverse) performance

(key,block length)	AES CD(Ansi C)		BrianGladman (VC++)	
	Speed (mbits/sec)	#cycles/block	Speed (mbits/sec)	#cycles/block
(128,128)	27.0	950	70.5	363
(192,128)	22.8	1125	59.3	432
(256,128)	1.8	1295	51.2	500

We gratefully accepted the generous offer from Cryptix to produce the Java implementation. Cryptix provides however no performance figures. Our estimates are based on the execution time of the KAT and MCT code on a 200 MHz Pentium, running Linux. The JDK1.1.1 Java compiler was used. The performance figures of the Java implementation are given in Table 4.

Table 4.Cipher (and inverse) performance in java

Key/block length	Speed	#cycles for rijndael
(128,128)	1100 kbit/s	23.0kcycles
(192,128)	930 kbit/s	27.6kcycles
(256,128)	790 kbit/s	32.3kcycles

5. CONCLUSION

In this paper, we have presented the art encryption and decryption schemes discussing their performances and security issues. Different researchers have contributed their work to this field, and some of the algorithms are been explained here. Nowadays, such techniques are studied in wide application contexts, but the research is still challenging in the encryptographic community to design more powerful/secure schemes.

REFERENCES

[1] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," in Foundations of Secure Computation, 1978, pp. 169–177.

[2] E. Brickell and Y. Yacobi, "On privacy homomorphisms," in Advances in Cryptology (EUROCRYPT '87), Lecture Notes in Computer Science, Springer, 1987, vol. 304, pp. 117–126,

[3] D. Rappe, "Homomorphic cryptosystems and their applications", Ph.D. thesis, University of Dortmund, Germany, 2004,.

[4] R. Cramer and I. Damgard, "Zero-knowledge for finite field arthmetic, or: can zeroknowledge be for free?" in Advances in Cryptology (CRYPTO '98), Lecture Notes in Computer Science, Springer, vol. 1462 , pp. 424–441.

[5] H. Lipmaa, "Verifiable homomorphic oblivious transfer and private equality test," in Advances in Cryptology (ASIACRYPT'03), Lecture Notes in Computer Science, Springer, vol. 2894, pp. 416- 433.

[6] P.-A. Fouque, G. Poupard, and J. Stern, "Sharing decryption in the context of voting or lotteries," in Proceedings of the 4th International Conference on Financial Cryptography, 2000,vol. 1962, pp. 90–104 .

[7] T. Sander and C. Tschudin, "Protecting mobile agents against malicious hosts," in Mobile Agents and Security, Springer, 1998, vol. 1419, pp. 44–60.

[8] P. Golle,M. Jakobsson, A. Juels, and P. Syverson, "Universal reencryption for mixnets," in Proceedings of the RSA Conference Cryptographers,2004, vol. 2964, pp. 163–178.

[9] I. Damgard and M. Jurik, "A length-flexible threshold cryptosystem with applications," in Proceedings of the 8th Australian Conference on Information Security and Privacy, 2003, vol. 2727.

[10] A. Adelsbach, S. Katzenbeisser, and A. Sadeghi, "Cryptology meets watermarking: detecting watermarks with minimal or zero-knowledge disclosures," in Proceedings of the European Signal Processing Conference, 2002.

[11] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on aditive homomorphic property," IEEE Transactions on Image Processing, 2005, vol. 14, no. 12, pp. 2129–2139.

[12] A. Kerckhoffs, "La cryptographie militaire (part i)," Journal des Sciences Militaires, 1883, vol. 9, no. 1, pp. 5–38.

[13] A. Kerckhoffs, "La cryptographie militaire (part ii)," Journal des Sciences Militaires, 1883, vol. 9, no. 2, pp. 161–191.

[14] J. Daemen and V. Rijmen, "The block cipher RIJNDAEL," (CARDIS'98) , Springer ,2000, vol. 1820, pp. 247–256.

[15] J. Daemen and V. Rijmen, "The design of Rijndael," in AES—the Advanced Encryption Standard, Informtion Security and Cryptography, Springer, 2002.

[16] G. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," Journal of the American Institute of Electrical Engineers,1926, vol. 45, pp. 109-115.

[17] P. Ekdahl and T. Johansson, "A new version of the stream cipher SNOW," in Selected Areas in Cryptography (SAC '02), Springer, 2002, vol. 2595, pp. 47–61.

[18] R. Rivest, A. Shamir, and L. Adleman, "Amethod for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 1978, vol. 21, no. 2, pp. 120–126.

[19] T. ElGamal, "A prublic key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (CRYPTO '84), Springer, 1985, vol. 196, pp. 10–18.

[20] C. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, 1949, vol. 28, pp. 656–715.

[21] M. Ajtai and C. Dwork, "A public key cryptosystem with worst-case/average-case equivalence," in Proceedings of the 29th ACM Symposium on Theory of Computing, 1997, pp. 284–293.

[22] P. Nguyen and J. Stern, "Cryptanalysis of the Ajtai- Dwork cryptosystem," in Advances in Cryptology (CRYPTO '98), Springer, 1999, vol. 1462 , pp. 223–242.

[23] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle model, revisited," in Proceedings of the 30th ACM Symposium on Theory of Computing, 1998, pp. 209–218.

[24] P. Paillier, "Impossibility proofs for RSA signatures in the standard model," in Proceedings of the RSA Conference, 2007, vol. 4377, pp. 31–48.

[25] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, 1976, vol. 22, no. 6, pp. 644–654.

[26] Coumou, D.J.; Sharma, G," Insertion, Deletion Codes With Feature-Based Embedding: A New Paradigm for Watermark Synchronization with Applications to Speech Watermarking", 2008, vol. 3, No.2, pp: 153 – 165.

[27] Hofbauer, K.; Kubin, G.; Kleijn, W.B.,"Speech Watermarking for Analog Flat-Fading Bandpass Channels", IEEE Transactions on Audio, Speech, and Language Processing, 2009,vol.17, no.8, pp: 1624 – 1637.

[28] Chen, N.; Zhu, J., "Robust speech watermarking algorithm", Electronics Letters,2007, vol. 3,no. 24, pp: 1393- 1395.

[29] Chen, O.T.-C.; Chia-Hsiung Liu," Content-Dependent Watermarking Scheme in Compressed Speech With Identifying Manner and Location of Attacks", IEEE Transactions on Audio, Speech, and Language Processing, 2007,vol. 15, no.5, pp: 1605 – 1616.

[30] Laurent Girin; Mohammad Firouzmand; Sylvain Marchand," Perceptual Long-Term Variable-Rate Sinusoidal Modeling of Speech", IEEE Transactions on Audio, Speech, and Language Processing, 2007, vol.15, no.3, pp: 851 – 861.

[31] Stankovic, S.; Orovic, I.; Zaric, N, " An Application of Multidimensional Time-Frequency Analysis as a Base for the Unified Watermarking Approach", IEEE Transactions on Image Processing, 2010, vol.19, no.3, pp: 736 – 745.

[32] Larbi, S.D.; Jaidane-Saidane, M, "Audio watermarking: a way to stationnarize audio signals", IEEE Transactions on Signal Processing, 2005, vol. 53, no.2, pp: 816 – 823.

[33] Parvaix, M.; Girin, L.; Brossier, J.-M, "A Watermarking-Based Method for Informed Source Separation of Audio Signals With a Single Sensor", IEEE Transactions on Audio, Speech, and Language Processing, 2010, vol.18, no.6, pp: 1464 – 1475.

[34] Xiangyang Wang; Wei Qi; Panpan Niu, "A New Adaptive Digital Audio Watermarking Based on Support Vector Regression", IEEE Transactions on Audio, Speech, and Language Processing,2007, vol.15, no.8, pp: 2270 – 2277.

[35] Chen, O.T.-C.; Wen-Chih Wu, "Highly Robust, Secure, and Perceptual-Quality Echo Hiding Scheme", IEEE Transactions on Audio, Speech, and Language Processing, 2008 vol.16, no.3, pp: 629 – 638.

[36] Satti, M.; Kak, S, "Multilevel Indexed Quasigroup Encryption for Data and Speech", IEEE Transactions on Broadcasting, 2009, vol.55, no.2, pp: 270 – 281.

[37] Malik, H.M.A.; Ansari, R.; Khokhar, A.A, "Robust Data Hiding in Audio Using Allpass Filters", IEEE Transactions on Audio, Speech, and Language Processing, 2007, vol.15, no.4, pp: 1296 – 1304.

[38] Kalantari, N.K.; Akhaee, M.A.; Ahadi, S.M.; Amindavar, H, "Robust Multiplicative Patchwork Method for Audio Watermarking", IEEE Transactions on Audio, Speech, and Language Processing, 2009, vol. 17, no. 6, pp; 1133 – 1141.

[39] Baras, C.; Moreau, N.; Dymarski, P, "Controlling the inaudibility and maximizing the robustness in an audio annotation watermarking system ", IEEE Transactions on Audio, Speech, and Language Processing, 2006, vol.14, no.5, pp: 1772 – 1782.

[40] In-Kwon Yeo; Hyoung Joong Kim, "Modified patchwork algorithm: a novel audio watermarking scheme", IEEE Transactions on Speech and Audio Processing, 2003, vol.11, no.4, pp: 381 – 386.

[41] Sridharan, S.; Dawson, E.; Goldburg, B, "Fast Fourier transform based speech encryption system", IEEE Communications, Speech and Vision, 1991, vol.138, no.3, pp: 215 – 223.

[42] Servetti, A.; De Martin, J.C., "Perception-based partial encryption of compressed speech", IEEE Transactions on Speech and Audio Processing, 2002, vol.10, no.8, pp: 637 – 643.

[43] Goldburg, B.; Sridharan, S.; Dawson, E., "Design and cryptanalysis of transform-based analog speech scramblers,", IEEE Journal on Selected

Areas in Communications, 1993,vol.11, no.5, pp: 735 – 744.
[44] Dawson, E. "Design of a discrete cosine transform based speech scrambler", Electronics Letters , 1991, vol. 27, no.7, pp: 613 – 614.
[45] Goldburg, B.; Sridharan, S.; Dawson, E.;, "Cryptanalysis of frequency domain analogue speech scramblers", in Proceedings IEE Communications, Speech and Vision, 1993, vol.140, no.4, pp: 235 – 239.
[46] Li, K.; Soh, Y.C.; Li, Z.G., "Chaotic cryptosystem with high sensitivity to parameter mismatch", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2003, vol. 50, no.4, pp: 579 – 583.
[47] Chung-Ping Wu; Kuo, C.-C.J., "Design of integrated multimedia compression and encryption systems", IEEE Transactions on Multimedia, 2005, vol.7, no.5, pp: 828 – 839.
[48] Shahreza, S.S.; Shalmani, M.T.M., "High capacity error free wavelet Domain Speech Steganography", IEEE International Conference on Acoustics, Speech and Signal Processing, 2008, pp: 1729 – 1732.
[49] Tingting Xu; Zhen Yang;, "Simple and effective speech steganography in G.723.1 low-rate codes", International Conference on Wireless Communications & Signal Processing, 2009, pp: 1 – 4.
[50] Shirali-Shahreza, M.H.; Shirali-Shahreza, S., "Real-time and MPEG-1 layer III compression resistant steganography in speech", IET Information Security, 2010, vol.4, no.1, pp: 1 – 7.
[51] Aoki, N, "A Semi-lossless Steganography Technique for G.711 Telephony Speech", International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010, pp: 534 – 537.
[52] Chai Peiqi; Liu Jingyong; Pei Dingyu; Yang Zhiqiang, "LPC Prediction Error Combined with LSB Steganography for Blind Speech Authentication", IEEE 7th Workshop on Multimedia Signal Processing, 2005, pp: 1 – 4.
[53] Djebbar, F.; Hamam, H.; Abed-Meraim, K.; Guerchi, D., "Controlled Distortion for High Capacity Data-in-Speech Spectrum Steganography", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing , 2010, pp: 212 – 215.
[54] Yong Feng Huang; Shanyu Tang; Jian Yuan; "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec" IEEE Transactions on Information Forensics and Security, 2011, vol.6, no.2, pp: 296 – 306.
[55] Hui Tian; Ke Zhou; Hong Jiang; Jin Liu; Yongfeng Huang; Dan Feng; "An M-Sequence Based Steganography Model for Voice over IP", IEEE International Conference on Communications, 2009, pp: 1 – 5.
[56] Zhi-jun Wu; Wei Yang; Yi-xian Yang; "ABS-based speech information hiding approach", Electronics Letters, 2003, vol.39, no.22, pp: 1617 – 1619.
[57] Rui Miao; Yongfeng Huang; "An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP", IEEE International Conference on Communications, 2011, pp: 1 – 5.
[58] Huang, Y.; Tang, S.; Bao, C.; Yip, Y.J.; "Steganalysis of compressed speech to detect covert voice over Internet protocol channels", IET Information Security, 2011, vol.5, no.1, pp: 26 – 32.
[59] Wu Zhi-jun; Niu Xin-Xin; Yang Yi-xian; "Design of speech information hiding telephone", in Proceedings IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, 2002, vol.1, pp: 113 – 116.
[60] Hui Tian; Ke Zhou; Yongfeng Huang; Dan Feng; Jin Liu; "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", The 9th International Conference on Young Computer Scientists, 2008, pp: 647 – 652.
[61] Skopin, D.E.; El-Emary, I.M.M.; Rasras, R.J.; Diab, R.S.; "Advanced algorithms in audio steganography for hiding human speech signal", 2nd International Conference on Advanced Computer Control, 2010, vol.3, pp: 29 – 32.
[62] Aoki, N.; "Potential of Value-Added Speech Communications by Using Steganography", Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, vol.2, pp: 251 – 254.
[63] Sinha, T.S.; Sanyal, G.; "Neuro-Genetic based Speech Processing for Promoting Global Cyber Security using Steganography technique", Annual IEEE India Conference, pp: 1 – 6.

First Author– S.Rajanarayanan, CA, MPhil, ME, (Ph.D), Assistant Professor, Selvam College of Technology, Department of Computer Science and Engineering, Namakkal, Tamil Nadu, India.E-mail: srnarayanan_slm@yahoo.co.in

Second Author – Dr. A. Pushparaghavan BE, MBA, M.Tech, Ph.D is the Principal and Professor of Electronics and Communication Engineering in Selvam College of Technology, Namakkal from April 2011. He worked in different capacity from Lecturer to Professor and Dean in various leading institutions like Bannari Amman Institute of Technology, PB College of Engineering and PSR Engineering College. He is having around 20 Years of experience in teaching including academic research.