# Secure Steganography for Audio Signals

**A.M.Negrat&A.Kumar**
**Higher Institute of Electronces, P.O.Box 38645 Beni-Walid, Libya**
**Email:Drnegrat@yahoo.com**

## Abstract

In this paper we have proposed a new method of audio steganography incorporating encryption and pseudorandom sequence as a key. The secret data has been encrypted using RSA and pseudorandom sequence. The encrypted data is then embedded in the audio signals. The use of the pseudorandom sequence increases the complexity of the encryption and the RSA algorithm gives a very tight cipher design.

**Keywords**- Steganography, Cryptography, RSA and pseudorandom

## 1. Introduction

The security of multimedia over network transmission and information concealment raises an increasing interest in a digital multimedia era. The issues are discussed in E-commerce and Web-commerce sporadically. Petitcolas et al. [5] reported a survey of information hiding methods. Cox et al. [1] reviewed the watermarking techniques. As the technology moves, a new schemes, based on combining the concept of cryptography and steganography will be introduced for hiding secret messages. Steganography [3] is a Greek ancient art of hiding information and is currently exploited to either put a digital image on the secret messages to hide the information or insert watermarks [1,6] into a digital image, audio, and/or video, to preserve an intellectual property or to claim the copyright. The research of using steganography is to invent an intelligent use of camouflage such that no one except the authorized person can read the secret message after decryption. Cryptography [4], on the other hand, is concerned with strategies based on a secret key for enciphering or concealing data such as text, image, audio, and video data. A commonly used cryptographic system, RSA system [7], based on Euler and Euclidean theorems from Number Theory may be used for encrypting the plaintext.

. A Non-Linear forward feedback shift Register (NLFFSR) is a mechanism for generating Pseudo random binary sequences [8, 9, 10, and 11]. Figure 1 shows a general model of an n-bit NLFFSR. It is a Non-linear forward feedback shift register with a feedback function f

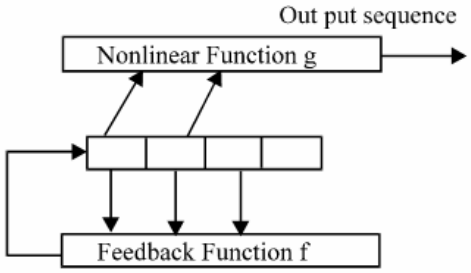


Figure (1): A General Model for 4-bit NLFFSR

NLFFSR are extremely good pseudorandom binary sequence generators [8, 9, 10, and 11]. When this register is loaded with any given initial value (except 0 which will generate a pseudorandom binary sequence of all 0s) it generates pseudorandom binary sequence, which has very good randomness and statistical properties. The only signal necessary for the generation of the binary sequence is a clock pulse. With each clock pulse a bit of the binary sequence is produced. A model of 4-bit NLFFSR is considered to demonstrate the functioning of NLFFSR with the feedback function $f = 1 + x + x_4$ and the non-linear function $g$ defined by $a_{n-1} \cdot a_{n-2} \oplus a_{n-2} \cdot a_{n-4}$ forming non-linear feed forward shift register generator. Its initial bit values are used (1111).

The output sequence : 011111000000001 $n$ $Z$ Generated by NLFFSR in is periodic of period 15, which is the same as the period of the sequence generated by NLFFSR of 4 bits.

Period of the sequence generated by NLFFSR is maximum if we use the primitive polynomial. To design any stream cipher system, one needs to consider the NLFFSR with primitive feedback polynomials as the basic building blocks. Period of the enciphering sequence can be increased if it is generated by following methods:

1. Addition of maximal length sequences.
2. Multiplication of maximal length sequences.
3. Using multi logic generalized linear feedback shift register.

The usefulness of these sequences depends in large part on there having nearly randomness

properties. Therefore such sequences are termed as pseudorandom binary sequences. The balance, run and correlation properties of these sequences make them more useful in the selection of secret keys [8, 9, 10, and 11]. The NLFFSR generated sequences are of great importance in many fields of engineering and sciences.

When performing data hiding on audio, one must exploit the weaknesses of the HAS, while at the same time being aware of the extreme sensitivity of the human auditory system. Various methods of the Audio Data Hiding are:

*Low-bit encoding: Binary* data can also be stored in the least-significant bit of audio files as it is stored in the least-significant bit of images. The primary disadvantage of this method is its poor immunity to manipulation.

Factors such as channel noise and re-sampling can easily destroy the hidden signal.

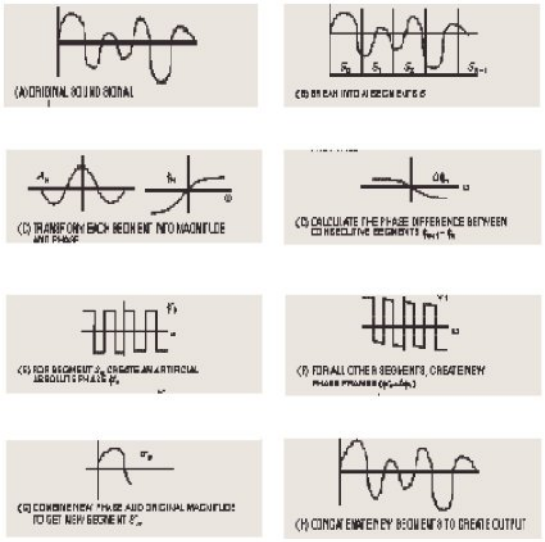

Figure (2) Encoding

*Phase coding:* The phase coding method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments. It is one of the most effective coding methods in terms of the signal-to-perceived noise ratio. When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small an inaudible coding can be achieved *(figure 2)*.

For the decoding process, the synchronization of the sequence is done before the decoding. The length of the segment, the DFT points, and the data interval must be known at the receiver. The value of the underlying phase of the first segment is detected as a 0 or 1, which represents the coded binary string *(figure -3)*.

*Spread spectrum:* While there are many variations on spread spectrum communication, we will concentrate on Direct Sequence Spread Spectrum encoding (DSSS). The DSSS method spreads the signal by multiplying it by a chip, a maximal length pseudorandom sequence modulated at a known rate. Since the host signals are in discrete-time format, we can use the sampling rate as the chip rate for coding. The result is that the most difficult problem in DSSS receiving, that of establishing the correct start and end of the chip quanta for phase locking purposes, is taken care of by the discrete nature of the signal. Consequently, a much higher chip rate, and therefore a higher associated data rate, is possible.

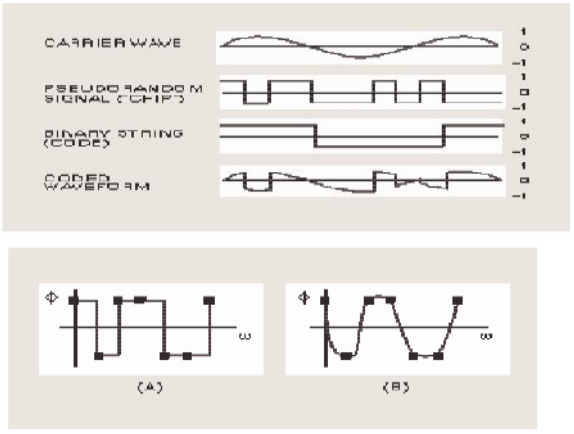


Figure (3) Decoding

Without this, a variety of signal locking algorithms may be used, but these are computationally expensive (*figure4 and figure 5)*

*Echo data hiding:* Echo data hiding embeds data into a host audio signal by introducing an echo. The data are hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. As the offset (or delay) between the original and the echo decreases, the two signals blend. At a certain point, the human ear cannot distinguish between the two signals. The echo is perceived as added resonance.

Data hiding in audio signals is especially challenging, because the human auditory system (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thousand to one. Sensitivity to additive random noise is also acute. The perturbations in a sound file can be detected as low as one part in ten million (80 dB below ambient level). However, there are some "holes" available. While the HAS has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out quiet sounds.

Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally, there are some environmental distortions so common as to be ignored by the listener in most cases.

The proposed method has been explained in section 2 and The Experimental results have been shown in section 3.

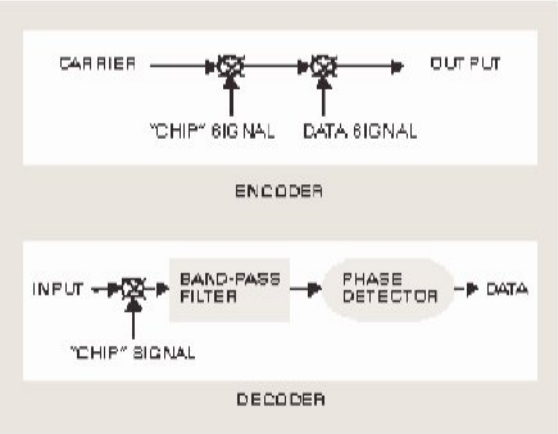


Figure 4:
Block Diagram of Spread Spectrum Technique

## 2. Proposed Method

Strength of any encryption algorithm depends on the random numbers generated and a commonly used cryptographic system, RSA system [7], based on Euler and Euclidean theorems from Number Theory, may encrypt a plaintext into a ciphertext with a public key (a, n), where $n = pq$ is a large number, $3 < a < m = (p-1)(q-1)$, and $gcd(a, m)=1$. Presumably, an RSA system realizes that only an authorized person knows how to factor n into the product of two primes, p and q, and so does the private key $b$ (that requires solving $ax \equiv 1 \ modm$) to decrypt the ciphertext, The usage of RSA system is based on issuing a very large number $n = pq$ such that for intruders using trial and error approaches can never find the secret key $b$ in their lifetime. Convert the raw data into its ASCII equivalent.

**1.** Since the strength of any encryption algorithm depends on the random numbers, generate a pseudorandom sequence of numbers through Pseudo Random Number Generator (PRNG).

**2.** Permute Data matrix $X$ to a permuted Data matrix $\Psi z$, where $\Psi z = \Phi z(X)$ and $\Phi z$ is permutation operation based on the pseudorandom sequence.

3. Further strengthen the encryption procedure by using RSA algorithm.

4. Issue an RSA *public key (a,n)*, where $n=pq$, $p$ and $q$ are large prime numbers, $m=(p-1)(q-1)$. $gcd(a,m)=1$ and $ab \equiv 1 \ mod$ m must be satisfied [4,7].

5. Encrypt each word obtained in (3) by the strategy of an RSA system to get the enciphered message Z.

6. Mix the encrypted data with the audio signals

7. To decrypt and recover the message, an authorized person must know decryption key, the factors $p$ and $q$ of $n$, which is extremely difficult although not unsolvable.

8. Apply RSA algorithm again. Issue an RSA private *key, b,* to recover the data back in permuted form.

9. Original data matrix can be obtained again from $\Psi z$ with the inverse operation of $\Phi z$ on it i.e $\Phi z\text{-}1(\Psi z) = \Phi z\text{-}1(\Phi z(X)) = X$ as $\Phi z\text{-}1 \ \Phi z$ forms an identity operator.

## 3. Experimental Results

We took a raw text file containing the secret message to be embedded in an Audio File. As the algorithm says the data has to be permuted according to the pseudorandom sequence generated and encrypted through the RSA algorithm, the two prime numbers *113* and *563* have been chosen and the RSA algorithm generates public key, 3 which acts as an encryption key and a private key, *41963* which acts as a decryption key. The experimental results have been shown in *figure 5*.

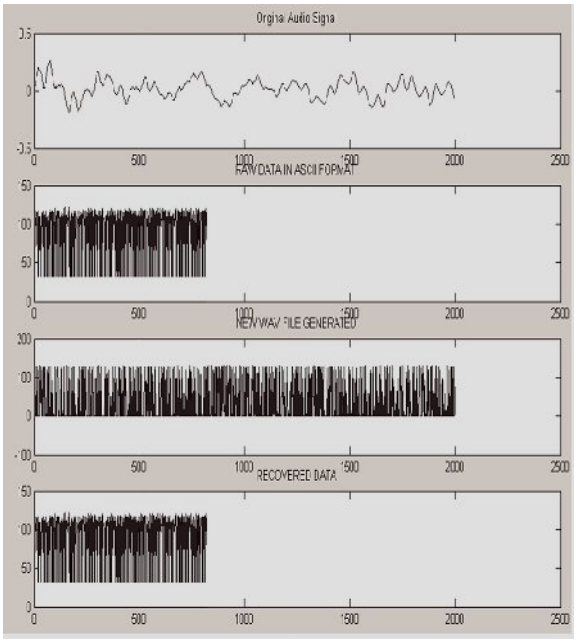


Figure (5) Experimental Results

## 4. References

[1] Cox, I.J., Kilian, J., Leighton, T., Shamoon, T.: Secure, spread spectrum watermarking for multimedia, IEEE Trans. Image Processing, Vol. 6, No. 12, (1997) 1673-1687

[2] Dubes, R.C., Jain, A.K.: Random field models in image analysis, Journal of Applied Statistics, Vol. 16, (1989) 131-164.
[3] Johnson N.F., Jajodia, S.: Exploring steganography: Seeing the unseen, IEEE Computer Magazine, Vol. 32, (1998) 26-34.
[4] Van Der Lubbe, J.C.A.: Basic methods of cryptography, Cambridge University Press, (1999)
[5] Petitcolas, F.A.P., Anderson, R.J., Kuhn, K.G.: Information hiding - A survey, Proceedings of the IEEE, Vol. 87, (1999) 1062-1078
[6] Pitas, I.: A method for watermark casting on digital images, IEEE Trans. Image Processing, Vol. 8, (1998) 775-780
[7] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, Communications of ACM, Vol. 21, (1978) 120-126Wolfgang, R.B., Podilchuk, C.I., Delp, E.J.: Proceedings of the IEEE, Vol. 87, (1999) 1108-1126.
[8] Rajpal, N., A. Kumar, S. Dudhani and P.R. Jindal, 2004. Copyright protection using non linear forward feedback shift register and error correction technique. 7th Ann. Intl. Conf. Map India, New Delhi, India.
[9] Rajpal, N., A. Kumar and P.R. Jindal, 2004. Demonstrating the use of error coding technique in the field of steganography, along with linear feedback shift register technique. 2nd Workshop on Computer Vision, Graphics and Image Processing, Gwalior, India, pp: 22-27.
[10] Rajpal, N., A. Kumar, P.R. Jindal and A. Saroagi, 2004. An investigation into the use of linear feedback shift register for data encrypting and data hiding in the field of steganography. Conf. e-security, Cyber Crime and Law. Chandigarh, India.
[11] Ahmad, A., M.J. Al-Musharafi, S. Al-Busaidi, A. Al-Naamany and J.A. Jervase, 2001. An NLFSR based sequence generation for stream ciphers. Proc. Intl. Conf. Sequences and their Applications (SETA '01), pp: 11-12.