Journal of Advances in Computer Research
Quarterly ISSN: 2008-6148
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 5, No. 2, May 2014), Pages: 7-22
www.jacr.iausari.ac.ir

Data Steganography on VoIP through Combination of Residue Number System and DNA Sequences

Azin Azizifard*, Mohamad Qermezkon, Tahereh Postizadeh, Hamid Barati

Department of Computer Engineering, Dezfoul Branch , Islamic Azad University, Dezfoul Iran

Azizifard.Ofu@Gmail.Com;Qermezkon@Gmail.Com;Tahere.Poostizadeh@Gmail.Com;
Hbarati@Iaud.ac.ir

Received: 2013/11/28; Accepted: 2014/01/05

Abstract

Today, optimal performance and cost advantages of using Internet telephony are obvious. Despite current standardized techniques, voice transferring through protocol (VoIP) has lower security than traditional telephony. One of the most important security issues which should be noticed in using VoIP is end -to-end user[2] identity, i.e. when there is a connection between user A and B, user A should be assured of the identity of user B, and vice versa. The authentication of identity is one of so important information that could guarantee the security and integrity of information [1]. In this study, the security of VoIP and data steganography through the protocol has been investigated. Finally, a technique for data steganography[4] over this protocol will be proposed using the method of Residue Number System[3]. Also, using the combination of RNS, DNA sequences, and Huffman compressing algorithm, an algorithm is proposed for data steganography through VoIP. The algorithm improves security of the process of transmission of hidden text and can use the bandwidth effectively.

Keywords: *Voice Over Internet Protocol, Steganography, Session Initiation Protocol (SIP), Residue Number System, DNA String, Huffman Algorithm*

1. Introduction

VoIP which is known as IP Telephony facilitates using the Internet and computer networks for phone calls. Traditional telephones contrast with VoIP which employs digital technology and needs a network. Nowadays, there are several companies that offer this service on the Internet for those who are interested in it. In fact, using VoIP technology, individual´s voice is transmitted through IP information packages and computer networks such as the Internet. In order to transmit individual´s voice, VoIP could use special tools and hardware or it should be set on an environment based on personal computers. VoIP is a common term used for a group of transmission technologies to transmit voice connections over the networks based on IP such as the Internet and closed switching networks. Over VoIP, when you talk to your fiend on Skype certain transmitted information packages are ignored by your friend´s computer due to long delay and defect. It is possible to write a piece of software that intentionally sends delayed and defective packages containing certain information and a piece of software that processes these packages. Thus, a message can be transmitted secretly.

VoIP carries telephone signals as audio digital (usually using speech data compression technology, its rate is lowered, and it is transmitted as a set of data flow on IP). Using IP telephony based on VoIP, voice is encoded and transmitted as data packages over public or private IP networks. Also, on the destination the data packages are integrated and decoded. Security concerns are always the major barrier that prevents businesses from using VoIP technology. Although VoIP suggests lower cost and greater flexibility, it may cause significant risks and vulnerabilities. One of the major security issues faced by VoIP is end-to end user identity, specially the identity of responder and how to authenticate it.

A VoIP system is consisted of:

- VoIP telephony which usually is connected to computer network by a network port
- VoIP telephony server which creates and manages communications
- Telephony gate used for connecting to local telephone network (analog or digital)
- Analog telephone adaptor (ATA) which is used to connect usual analog telephones to VoIP networks.

In addition, sometimes it is also necessary to use accounting software, monitoring software, Fire Wall, and VPN.

VoIP technology has several applications in current telecommunication systems. Using this technology results in decreasing cost, improving facilities and reliability such as transmission of telephone lines, connecting telephone systems of offices, creating new center of subscribers support ,creating VoIP systems to replace traditional santral, using VoIP to expand telephone centers, using VoIP for telephones´ operators and cell phones´ operators. In general, VoIP has several advantages such as, many telephone facilities, its advantage in telephone conferencing, the possibility of using telephone software, sending fax on the network in the system, better use of network capacity, its advantage in flexible structure of network, the mobility of operators in this technology, lower cost long distance calling, higher security, its advantage in expanding network, connecting several offices and integrating telephone systems, and facility of monitoring through VoIP.

a. Steganography is the art of covert communication. The purpose of steganography is to conceal communication through placing message in a covert medium to cause the least discoverable change and avoid the probable discovering of the existence of secret message in medium. Humans are attracted to steganography for years. Steganography is important since often the revealing of a message (even an encrypted one) is not safe. The difference between steganography and cryptography is that cryptography does not conceal communication from attacker, but it conceals the concept of message [2]. In other words, cryptography seeks to conceal the very message, but steganography hides the very communication. Thus, cryptanalysis is successful when whole or part of message is discovered. But steganalysis is successful when the very existence of communication (secret message) is discovered or revealed [3]. Important information could be hidden in audio files. Changing least significant bits, information is added to audio files. The changes result in making noise on the file. But when hidden

information is not much, noise is not detectable to individuals at all and just so complicated software is able to discover it.

Generally, VoIP technology uses protocols such as SIP (Session Initiation Protocol), and data control and transfer protocols such as Transmission Control Protocol (TCP), Real-Time Transport Protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP) [1].

b. SIP is used to establish, manage, and terminate sessions between 2 or more applications. SIP is a kind of service provider protocol. In this protocol, the applications of caller or user agents as clients and proxies are used medium to rout messages. Using SIP, especially for audio communications based on VoIP is increasing. Thus, SIP is considered as signaling protocol in IMS which is the bed of signaling for next generation networks. The reason of increasing use of SIP is its unique abilities such as the ability of separating signaling traffic from data traffic, the independence of the protocol from the content of messages, the kind of session being made, and text messages.

These advantages enable SIP to support a variety of multimedia communications such as audio calls, video calls, and text communication. However, the major aspect of SIP is its capability to move user, terminal, service, and session, i. e. a certain user can connect the network from everywhere and benefit from the services of SIP such as, receiving calls (like access his email from everywhere). Also, SIP has mechanisms which can be used to hand over communication while moving the terminals between 2 networks. According to significant growth of the use of SIP, comprehensive research has been done on the effectiveness of this protocol. SIP is an application layer protocol and based on text protocol which is standardized by IETF for session managements. The architecture of the protocol is consisted of 2 logical entities; user agent (UA) and server. User agents can be divided into 2 groups; user agent client (UAC), which sends SIP requests and user agent server (UAS), which returns SIP responses. Servers can be divided into several groups; registrar servers which register the user, redirect servers which locate the user by presenting possible locations of the user, and proxy servers which seek the user and are responsible for routing to send requests to a certain user and location. Proxy servers can be structured differently according to the condition and needs of network.

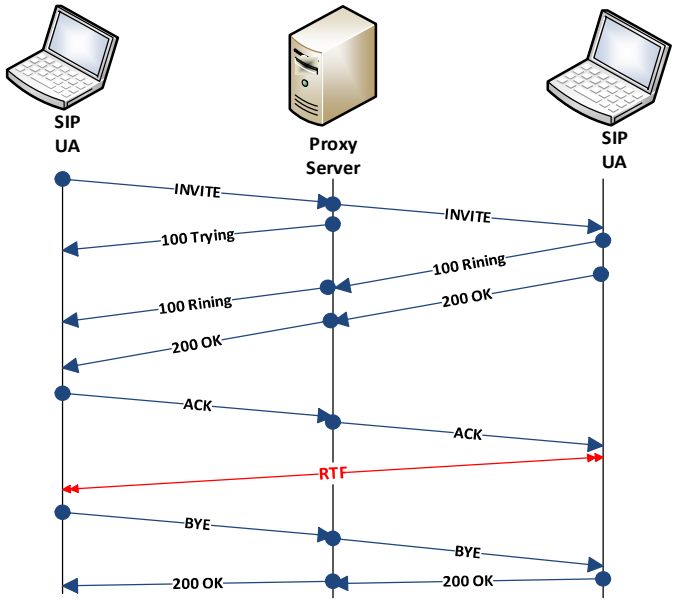

Figure 1.Exchanged messages in order to make calls over SIP

c. Huffman, In computer science and information theory, Huffman coding is an encoding algorithm of lossless data compression. The term refers to the use of a variable-length code table for encoding a source symbol (such as a character in a file). The variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. Huffman coding employs a specific method for choosing the representation method for each symbol. The method is called prefix-free codes (sometimes called prefix code),i. e. the bit string representing some particular symbol is never a prefix of the bit string representing any other symbol. The most common source symbols are expressed using shorter strings of bits than less common source symbols. The most efficient compression method of this type: no other mapping of individual source symbols to unique strings of bits can create a smaller average output size when the real symbol frequencies agree with those employed to create the code.

d. Residue Number System (RNS) is a non-weighted and unconventional system which is defined by a set of moduli and can support parallel, carry-free, high-speed, low power and secure arithmetic. Some of the important features of RNS are its capability of providing high speed, low power, and appropriate security. The advantages of multi-level RNS are the simple selection of moduli set or a large dynamic range. The most important issue in RNS is the selection of the moduli set. In RNS the parallel computations are done using division remainders according to certain number of moduli. The remainders are correspondingly smaller than the whole number in the standard representation. The remainder-based computation speeds up computation and decreases the power consumption [10].

The system is optimum when all the moduli are relatively pair wise prime. Due to the features of RNS, it has many applications in arithmetic functions such as Digital Signal Processing [11], Digital Filtering [12], [13] image processing[14], [15] RSA ciphering system[16], [17] digital communications[18] Ad-hoc network, storing and retrieving information[19], Error detection and Correction[20], [21], [22], [23], [24]

and fault tolerant systems[25]. Generally, RNS is employed in those areas where addition, subtraction, and multiplication operations are being repeated. In addition, since in RNS the calculations on the remainders are done separately if one error occurs on one remainder it will not be transferred to other moduli. In other words, the architecture of this system is inherently fault tolerant and error detection and correction are possible [26], [27]. In this study, a method is proposed based on RNS which is able to conceal data in three dimensional images. These three dimensional images are called Sterreograms. In fact, these are flat and two dimensional images in which the third dimension is hidden [10]. Another advantage of the system is its security because to change from ternary valued logic to RNS and from RNS to ternary valued logic it is needed to know moduli. Thus, the system is a medium security symmetric key ciphering. RNS is specified by a moduli set such as {m1, m2, m3, …, mL} in which all moduli are positive integers. When all the moduli are relatively pair wise prime the system will have the largest possible dynamic range which equals [α ,α + M) in
Which α is an integer and M is:

$$M = \prod_{i=1}^{L} m_i \quad (1)$$

The integer X in $\alpha \leq X < \alpha + M$ has a single representation in Residue Number System which is shown by the set of remainders (x1, x2, x3,…,xL) . So:

$$x_i = X \bmod m_i \ , \ i = 1,2,...,L \quad (2)$$

According to the applications of RNS, for more security and accuracy a large dynamic range is needed. One important parameter to achieve a large dynamic range is the choice of moduli set and number of the chosen moduli. However, the choice of moduli and the number of them should offer large dynamic rage, appropriate calculation speed and hardware complexity.

One feature of RNS is its ability to split a large integer to smaller integers which cause doing operations in parallel and very high speed. One important issue in RNS is the choice of modular because it affects the complexity of system and conversion algorithm. To choose a set of moduli it is required to determine the number of moduli and the optimum modular as the main modular of system. On the other hand, the range of numbers should be considered, too (the system range of number is the product of all modular elements). When an appropriate modular is chosen, conversion of numbers to RNS will result in unique binary numbers.

e. DNA, In the real world DNA strings of cells identify personality, behavior, and personal aspects; based on this proved truth and by placing input terms in algorithm as human body, a DNA sequence was made. Due to the repetition of A,C,T,G characters, the created DNA sequence has a high capability of compression.
DNA strings are made up of putting four factors (A-adenine, C-cytosine, G-guanine, T-thymine) together like a series. To create DNA strings first their properties are determined, then the weight of each property is calculated in base 2 and a string of 0 and 1 is created. Next, the binary string is divided to 2 bit codes, the codes are equated with the table made for it, and DNA string is created.

2. Review of previous methods

One of the most important security issues which should be noticed in using VoIP is end-to-end user identity, especially the identity of the responder and how to authenticate it. Steganography is the art of data concealment and plays an important role in VoIP communication security. In fact, it can be used to transmit confidential data in secure, transmit secret messages, or secure the user identity itself.Some of the VoIP´s threats are Eavesdropping, Denial of Service, Session Hijacking, VoIP Spam, Rogue Sets, and Toll fraud.

Related works that are investigated as the groung of this study are:

The study of Christian Kratzer et al. that used VoIP in steganography to send hidden message [4] is so helpful and functional for providing the security of certain messages during VoIP calls. But it can be used in a wider level for security of VoIP communications.

The study of Mazurczyk and Kotulski [6] proposed a security protocol that was used (based on VoIP) for data steganography and digital steganography. The protocol can authenticate and integrate data. Data steganography has been used to create a covert channel through which control bits are sent, and digital steganography is used to transmit real data.

The study of Kotulski and Mazurczyk [7] evaluated steganography techniques of access for SIP which can be used for creating channels at the phase of VoIP call signaling. The proposed algorithm can estimate the amount of data which can be transmitted for a kind of IP phone call (2.36 Kilobytes per second).

The study of Xiao Honghua and Xiao Bo and Hung Yongfeng [8] proposed the rather new steganography algorithm. The algorithm is presented as matching method least significant bit and a method for avoiding loss of confidential data based on audio information.

The study of AOKI Naofumi [9] proposed a method of compression steganography for G.711 with less risk of losing and without any damage.

Feng Cao and Cullen Jennings [5] proposed a new protocol based on data steganography to conceal the identity of responder in response message. This protocol is a backwards compatibility (reverse). Some solutions are proposed for authentication of identity at final terminals over VoIP.

The study of Ahmed Maher et al., Steganography for Voice Over IP (VOIP) [1], starts with this description that nowadays many hackers are looking for new methods and techniques to gain access to confidential information and penetrate further into networks. The authors investigated the security of VoIP and the role of data steganography in VoIP communication and then proposed mechanism to secure data over VoIP through One Time Password (OTP). The proposed technique influences the function of SIP signaling messages through addition of extra control bit and using public-key encoding to encoding covert string. Thus, it is possible to authenticate the responder using One Time Password (OTP) and concealing the password in SIP control bit. Also hash chain can be used as an OTP algorithm.

The idea of “hash chain” was first presented by Lamport in 1981 and has been used for safeguarding against password eavesdropping.

A hash chain of length N is created by using a one-way hash function h recursively to an initial seed value s.

$$hN(s) = h(h(\ldots h(s)\ldots))(N \text{ times}) \quad (3)$$

hN(s) is securely distributed. Then the elements of the hash chain are used one by one until the value of s is reached. It is claimed that it is possible to conceal the hash chain value which acts as an identity of the responder in the SIP message headers, such as Call-ID. Using the identity of the responder in hidden manner in the response message guarantees the authentication of responder. However, the remaining part and the important one are to guarantee the integrity of the message. It is done by guarantee a digest string from the message body and the identity of responder and conceal it distributed among the SIP headers.

$$Digest\text{-}string = message\text{-}body * responder\text{-}identity \quad (4)$$

The new proposed response identity flow containing the One Time Password for user identity and the digest-string for message integrity are shown in Figure 2.

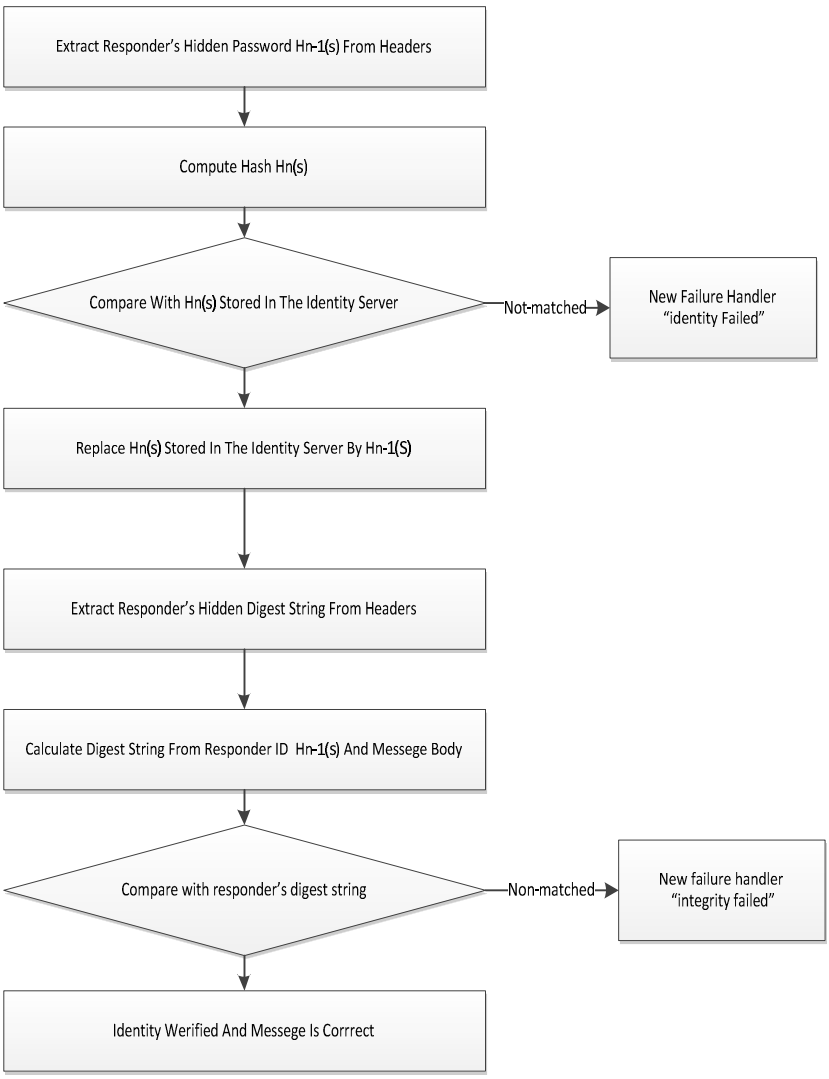

Figure 2. New proposed flow of response identity

In SIP, covert channels and steganography can act as threat to transmit malicious data, but it can be used also to secure the SIP itself. Adding additional headers to SIP message can result in latency of response messages. Steganography can be employed to conceal the responder identity in SIP message fields.

Thus, it will not influence the latency of message. Moreover, using One Time Password to identify the responder guarantees that the responder identity will not be stolen because the password is used only one at a time.

3. Proposed method

In the proposed method, using Huffman Algorithm, RNS, and DNA sequences, a suitable level of steganography over VoIP is achieved to improve security of message and make the most of the available bandwidth. One the most applicable protocols used in VoIP is SIP. This protocol is able to transmit signaling packages (audio) and data individually. In this study, this feature of SIP is used for exchanging and concealing data. In this proposed method, first the input string is changed into a bit string, using Huffman Algorithm. But after discovering characters´ frequencies, frequency weighting value is turned to modular (rn -1, rn ,rn +1) and the value of R and N as the main key of decoding are provided just for sender and receiver. Without having this key, decoding of text code is impossible. Now after converting frequencies of characters (the number of times that the characters repeat in text) into RNS, the resulting numbers produced by frequency divided by modular are converted into binary numbers. Thus, a series of 0 and 1 bit are produced. This study considers fixed number of required bits to represent frequency. Therefore, at the side of receiver, received bits of the main string can be reconstructed. After producing the binary string using DNA sequences, a string will be produced. If Huffman Algorithm be re-implemented on this string of numbers a very high level of compression is achieved (because DNA string is made up of the repetition of four characters A,C,G,T, if Huffman Algorithm be used for produced DNA string, a good level of compression will be achieved in comparison to simple text).

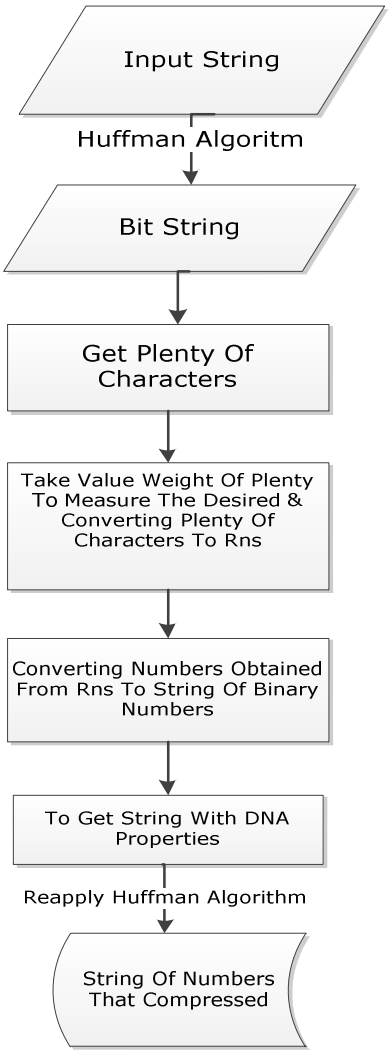

Figure 3. Encoding diagram

In the following, the general method of proposed algorithm has been presented step by step:

Step 1: First, input string is converted to a bit string using Huffman Algorithm. In this study, weights of the components of DNA sequences are presented in table 1.

Table 1. Weights of the components of DNA sequences

Weight	Component
0 0	A
0 1	C
1 0	G
1 1	T

For example the proposed algorithm converts following string as a string of 0 and 1 which can be transmitted on SIP. The string is:

String: This is an example of a Huffman tree.

Step 2: Creating Huffman tree for frequencies

Now using Huffman Algorithm, a tree of existing and composing characters´ frequencies is created. The tree is shown in Figure 4.

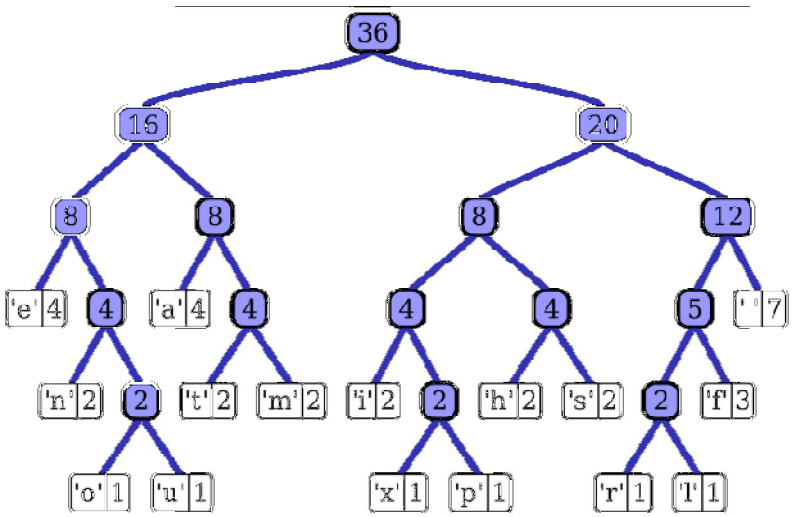

Figure 4. Huffman tree created by string characters´ frequencies

(The number of times that the characters repeat in text)

Step 3: Creation of frequency table based on existing tree

Table 2. A sample of the table of frequencies based on the input string tree

Word	Repetition
Space	7
A	4
E	4
F	3
H	2
I	2
M	2
N	2
S	2
T	2
L	1
O	1
P	1
R	1
U	1
X	1

Step 4: Conversion of the value of characters´ frequencies to RNS

To add the first level of security (encoding using RNS), table 2´s frequencies are converted to moduli (3 4 5). This modular is considered as the main code key. The kind of using modular is not limited (this modular is considered as code key and any other triple modular can be used). In fact, the proposed algorithm is able to use any kind of modular to offer a suitable level of bit compression while transmitting on the channel.

Table 3. Converting frequency from decimal to RNS by 3-moduli sets

Word	Repeat	Created String After Taking To Module
Space	7	11110
A	4	10100
E	4	10100
F	3	01111
H	2	101010
I	2	101010
M	2	101010
N	2	101010
S	2	101010
T	2	101010
L	1	111
O	1	111
P	1	111
R	1	111
U	1	111
X	1	111

Step 5: Creation of a string of 0 and 1 bits

The bits resulted from converting the value of characters´ frequencies (mentioned in the table 3) are put together in a series. The result is the following string:
Binary Array:
1111010100101000111110101010101010101010101010101010101011111111111111111111

Step 6: Conversion of binary string to DNA sequence
DNA Sequence: TTCCAGGATTGGGGGGGGGGGGGGGGGTTTTTTTTT

Step 7: Using Huffman Algorithm to compress

Again Huffman Algorithm is implemented on DNA sequence, but a brief binary string is created due to the nature of DNA sequences (DNA strings are made up of four

elements A, C, G, and T). The string can be transmitted on SIP using data packages. Thus, both steganography and compression are done.

To compress created DNA string, the elements are divided into groups of four:

DNA sequence: TTCC AGGA TTGG GGGG GGGGGGGG TTTT TTTT T

Table 4. Frequencies of created groups to place in Huffman Algorithm

Mark	Sign	Repeat	Code
A	TTCC	1	1
B	AGGA	1	1
C	TTGG	1	1
D	GGGG	4	100
E	TTTT	2	10
F	T	1	1

Step 8: Reimplementation of Huffman Algorithm

According to obtained frequency, Huffman Algorithm is re-implemented. Re-implementing Huffman Algorithm based on table 4 of frequencies, it is possible to use following binary values instead of any rows:

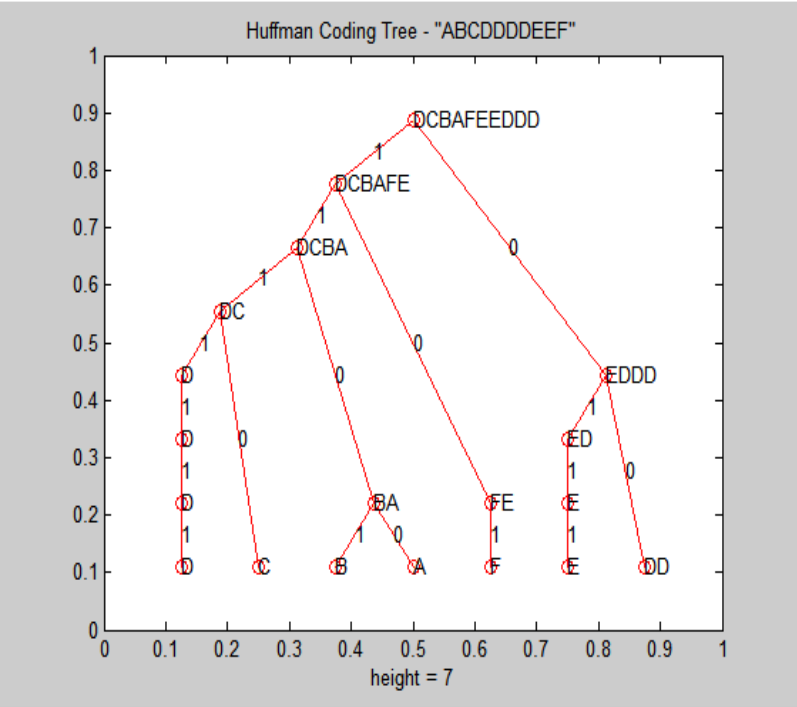

Figure 5: Huffman tree of DNA string

Table 5. Encoding

Symbol	Code
A	1100
B	1101
C	1110
D	1111
E	0111
F	101

Step 9: Transmission of created string on the channel

Using proposed algorithm, just 110011011110111111111111111101110111101 bit string is transmitted on the channel. The string indicates the text: this is an example of a Huffman tree. As it is demonstrated an encoded string of 24 bits is transmitted on the channel instead of a string of 75 bits which equals 53.3% of the compression of the string.

To reverse, the process is down in reverse, but to convert data from RNS to original numbers CRT or CRT-NEW is used.

4. Conclusion

In this method, RNS is used for symmetric encoding. Due to irreversible nature of Residue Number System, without knowing the module it provides a reasonable level of symmetric encoding. Then produced bit string algorithm is turned to a DNA sequence. This sequence has only 4 characters, so it can prove a reasonable level of compression. Also using the method, the defect of increasing the number of bits at the encoding time which is due to using RNS is covered. In the proposed algorithm, RNS is used to encode with symmetric key. Due to the irreversible nature of RNS, without knowing the module and having several combinations and values of a module, the system can provide acceptable security to guarantee the irreversibility of the hidden text and change the compressed string to the string consisted of DNA sequences which are made of reoccurrence of 4 characters A,C,T, and G. Implementing Huffman Algorithm on the string provides an appropriate level of compression which cause lower consumption of information bandwidth. Also it is covered using the proposed overhead method created by RNS while encoding. Due to using SIP protocol, transmission of hidden data as a text and without interfering with audio packages is possible. Thus, the quality of voice is not influenced by the packages of hidden text.

References

[1] Ahmed Maher, Mohamed Hashim, Abdel Fatah Hegazy, Bahaa Hasan, "Steganography For Voice Over Ip (Voip)," Proceedings Of The 7th Wseas International Conference On Information Security And Privacy, 2008.

[2] K.Wong, X.Qi,K. Tanaka,"A DCT-based Mod4 steganographic method," Signal Processing, Vol. 87, No. 6, 2007, pp. 1251-1263.

[3] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, "Steganalysis of Pixel-Value Differencing Stegano-graphic Method," Proceedings of IEEE Pacific Rim, 2007, pp. 292-295.

[4] Christian Kratzer, Jana Dittmann, ThomasVogel, "ReykHillert: Design and Evaluation of Steganography for Voice-over-IP," ISCAS 2006.

[5] Feng Cao, Cullen Jennings,"Providing ResponseIdentity and Authentication in IP Telephony,"Proceedings of the First International Conferenceon Availability, Reliability and Security(ARES'06), 2006

[6] Mazurczyk, W., Kotulski, Z."New Security and Control Protocol for VoIP Based on Steganography and Digital Watermarking," Annales UMCS, Informatica, AI 5, pp. 417-426, ISNN 1732-1360

[7] Mazurczyk, W., Kotulski, "Covert Channels in SIP for VoIP Signalling," Proc. of 4th International Conference on Global E-security 2008.

[8] Huang Yongfeng, Xiao Bo, Xiao Honghua, "Implementation of Covert Communication based on Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2008.

[9] Naofumi AOKI, "A Technique of Lossless Steganography for G.711 Telephony Speech," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

[10] Szabo, S.N., and Tanaka, R.I., "Residue Arithmetic and its Applications to Computer Technology," McGraw-Hill, New York (1967).

[11] M. Soderstrand, A. et al. Eds, "Residue number system arithmetic: modern applications in digital signal processing," New York, IEEE Press, (1986).

[12] M. A. Soderstrand and R. A. Escott, "VLSI Implementation in Multiple-Valued Logic of an FIR Digital Filter Using Residue Number System Arithmetic," IEEE Transactions on Circuits and Systems, Vol. 33, No. 1, 1986,pp. 5-25,

[13] R. Conway and J. Nelson, "Improved RNS FIR Filter Architectures," IEEE Transactions on Circuits and Systems II:Express Briefs, Vol. 51, No. 1, 2004,pp. 26-28.

[14] W. Wang, M.N.S. Swamy and M.O. Ahmad, "RNS Application for Digital Image Processing ," Proceedings of the 4th IEEE International Workshop on System-on-Chip for Real-Time Applications (IWSOC'04), 2004, pp. 77-80.

[15] F. Taylor, "A Single Modulus ALU for Signal Processing," IEEE Transactions on Acoustics, Speech, Signal Processing, , Vol. 33, No 5,1985, pp. 1302-1315.

[16] M. Ciet, M. Nevel, E. Peetersl, and J. J. Quisquater, "Parallel FPGA implementation of RSA with residue number systems," Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, Vol. 2,2003, pp. 806-810.

[17] J. C. Bajard and L. Imbert, "Brief contributions: A Full Implementation RSA in RNS," IEEE Transactions on Computer, Vol. 53, No. 6,2004, pp. 769-774.

[18] J. Ramirez et al., "Fast RNS FPL-Based Communications Receiver Design and Implementation," Proceedings 12th Int'l Conference. Field Programmable Logic,2002, pp. 472-481.

[19] J.-C. Bajard and L. Imbert."A Full RNS Implementation of RSA". In: IEEE TransactionsComputers53.6 ,2004, pp. 769–774.

[20] H. Krishna, K-Y. Lin, and J-D. A Coding ,"Theory Approach to Error Control in Redundant Residue Number Systems I: Theory and Single Error Correction,",in the Sun IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, vol.39, no.1, 1992, pp. 8-17.

[21] G. Jaberipur, B. Parhami, and M. Ghodsi, "A Class of Stored-Transfer Representations for Redundant Number Systems," Proc. 35th Asilomar Conf. Signals, Systems, and Computers, Pacific Grove, CA, 4-7 ,2001, pp. 1304-1308..

[22] J. D. Sun and H. Krishna, "A coding theory approach to error controlin redundant residue number systems— Part II: Multiple error detection and correction," IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process,vol. 39, no. 1,1992, pp. 18–34.

[23] R. W. Watson and C. W. Hastings, “Self-checked computation using residue arithmetic,” Proceedings of the IEEE, 1966, vol. 54, pp. 1920-1931.
[24] Yang, L.-L., &Hanzo, L,” Redundant residue number system based error correction codes,” In Vehicular technologyconference, 2001. vtc 2001 fall. ieeevts 54th (Vol. 3, pp. 1472–1476).
[25] E. Kinoshita, K. Lee, ”A residue arithmetic extension for reliable scientific computation”, IEEE Transactions on Computers, Vol. 46, No. 2, 1997, pp. 129-138.
[26] Yang, L-L and Hanzo, L,” http://eprints.soton.ac.uk/257133/ In, VTC'2001 (Fall), Atlantic City, USA, 07 - 10 , 2001.
[27] H. M. Yassine, "Hierachical Residue number system suitable for VLSI Arithmetic Architectures" IEEE, 1992.