Designing a Subliminal Channel for Deceiving Enhancement

Dr. Abdulameer K.Hussain
Zarqa Private University

Summary
In view of the known function of the subliminal channel which is used to provide a high level authentication ,this paper presents a design of a new subliminal channel, based on a bit transformation with variable values , that ensures a better authentication level and maintain reliable degree of privacy . The method exhibits the advantages of using agreed policies and may be used as a method of deceiving opponents. Some of the secure parameters can be used that facilitate generating of authorized meaningful messages between two authenticated parties in spite of existing an enemy monitoring the message transmissions between the above parties. The idea of designing the subliminal channel presented in this paper is dependent on the prisoner's problem. Finally, this paper proposed secret equations that can be used to select the authenticated meaningful messages in an effective way differ from the previous subliminal channel.

Key words:
Cryptography, Authentication, Subliminal Channel , Digital Signature, Security

1. Introduction

Companies want to exploit computer networks to their full potential, connecting sites that may be situated on opposite sides of the earth. Individual users want to securely access remote sites without disclosing their identities or activities [1]. As long as there has been communication, there have been issues of privacy and authenticity. [2].Both individuals and companies have information that they don't want the whole world to know, so sending such information over an unprotected network is quite out of the question. Cryptographic techniques are covered in details in [3].

The classical form of authentication is to use a user id and a password transmitted in the clear. Once this was barely adequate, but nowadays authentication must be handled using more sophisticated techniques. Modern cryptography offers several techniques for very strong authentication, and they can be used to authenticate almost anything on a network; users, hosts, clients, servers, you name it.

In some contexts where authentication is used today, authorization would be a more proper technique. The distinction between the two is clear, but nevertheless they are often confused. When you authenticate yourself, you prove your identity, whereas you use authorization to prove that you are authorized to use some facility. This gets interesting when you realize that cryptography offers you the possibility to authorize yourself without disclosing your identity [1, 3].

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

The challenge of providing adequate protection is closely related to both secrecy and authentication methods. Similar to the need for varying degrees and types of secrecy, there are many different levels and types of authentication. Some environments require simply message authentication, with no need for secrecy, while others, both authentication and secrecy will be required [4]. In this paper we will describe the authentication aspect of protection in addition to secrecy.

There are different authentication methods which will be described briefly in Section 2. One of the important authentication methods is the subliminal channel which is a way of embedding information in public communication in an undetectable way. Some sort of shared secret (a key, knowledge of what to look for) is needed to reconstruct the subliminal information [5]. The subliminal channel is a covert communication channel that cannot be read by those for whom it is not intended. Some simple examples occur in everyday life when we, for instance, give a certain look to a certain person, or wink, or raise an eyebrow perhaps. Here, some form of communication is occurring between two (or more) parties, and those who listen to the conversation but do not observe the communicants will not see the subliminal channel. This is, of course, a very simple example but should serve to illustrate the concept [4].

2. Secrecy and Authentication

Suppose a sender wants to send a message to a receiver. Moreover, this sender wants to send the message securely. He/she wants to make sure an eavesdropper cannot read the message. A message is called plaintext(or clear text). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption. This is all shown in Figure 1.1.

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. Modern cryptologists are generally trained in theoretical mathematics—they have to be.

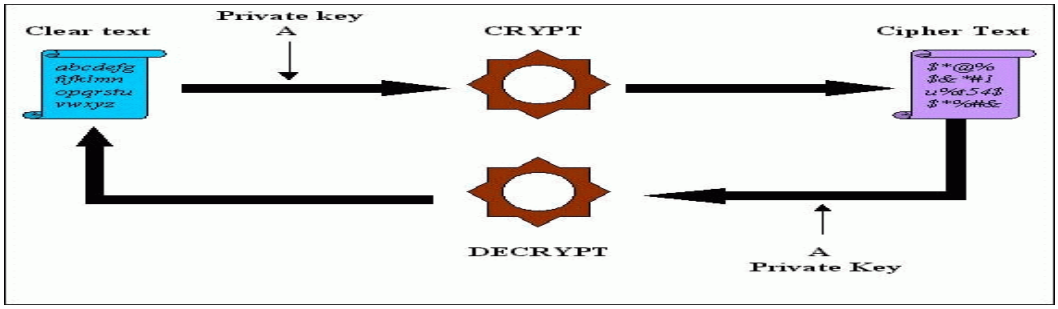

Figure 1.1 Encryption and Decryption

Plaintext is denoted by *M*, for message, or *P*, for plaintext. It can be a stream of bits, a text file, a bitmap, a stream of digitized voice, or a digital video image.. As far as a computer is concerned, *M* is simply binary data. The plaintext can be intended for either transmission or storage. In any case, *M* is the message to be encrypted.

Ciphertext is denoted by *C*. It is also binary data: sometimes the same size as *M*, sometimes larger. (By combining encryption with compression, *C* may be smaller than *M*. However, encryption does not accomplish this.) The encryption function *E*, operates on *M* to produce *C*. Or, in mathematical notation: $E(M) = C$ .In the reverse process, the decryption function *D* operates on *C* to produce *M*: $D(C) = M$ .Since the whole point of encrypting and then decrypting a message is to recover the original plaintext, the following identity must hold true: $D(E(M)) = M$

In addition to providing confidentiality, cryptography is often asked to do other jobs such as authentication where it should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else, integrity which means that it will be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one, and nonrepudiation where a sender should not be able to falsely deny later that he sent a message. [3, 4].

3. Authentication Methods

Authentication is the way you prove to the system that you are who you say you are. In any multi-user system, you must identify yourself, and the system must authenticate your identity, before you can use the system. There are three classic ways in which you can prove yourself:

1: Something you know, such as a password, PIN, or an out of wallet response.
2: Something you have, such as mobile phones, credit cards, or hardware security.
3: Something you are, such as a fingerprint, a retinal scan, or other biometric.

Passwords are still, far and away, the authentication tool of choice. Even when authentication devices like tokens and biometric devices are used, they're usually supplements to, not replacements for, conventional login IDs and passwords. Biometrics and key cards typically act only as a first line of defense against intruders, not as the only defense. These techniques are related to so-called physical security and Biometrics. [6].

According to the above discussion, there are two different cases that may be distinguished: user authentication and message authentication. User authentication can be made either directly when a user's specific characteristics (e.g. finger prints , voice frequency spectrum ,retina patterns, digital signatures flows, etc) are checked or indirectly when a unique secret piece of information is proved to be in the user's possession . As a matter of fact, the indirect user authentication is equivalent to message authentication. Message authentication relies upon imposing a prearranged structure of the message. As an example of elementary method of message authentication, let us look to the following figure and assume that the sender that the sender forwards information to the receiver whiles the channel is under the opponent's control.

Generally, also, the sender wants to know if the message he/she has forwarded has reached the intended destination. In order to fulfill this requirement, the receiver usually sends confirmation of any message he/she has received.

Now, we confine our attention to the simplest case of authentication where a single elementary message is sent and the receiver whishes to be able to determine its authenticity. In this case, the message authenticity relies upon fixing the set of so-called valid messages at both ends of the channel. [4] .

There are several authentication schemes, some of them use symmetric systems and others use asymmetric systems. These schemes are Shamir's fast authentication scheme [7],and this system had been broken by Odlyzko[8] , Ong- Schnorr-Shamir authentication scheme [9], EI Gamal's authentication scheme [10], and Rivest-Shamir-Adleman authentication scheme [11].

4. Digital Signatures – A Quick Overview

Handwritten signatures have been used for years to prove a certain document came from, or was approved by a specific person. You always sign credit card bills to prove that you are who you say you are. There are several reasons why a signature is compelling [3]: the signature is authentic and cannot be forged, the signature is not reusable and cannot be repudiated, and the signed document can not be altered.

A digital signature is a number (or numbers) dependent on some secret known to the signer, and on the signed message. Digital signatures are implemented using public-key cryptography: the signer has a private key used for creating signatures, and a public key used for signature verification.[12]

Attaching signatures to a message on a computer could be a very handy thing. If you sent someone a signed e-mail message with sensitive instructions on say, the handling of your will, they could take this message with a reasonable assumption of authenticity. [3]. Also, since the digital signature cannot possible be a physical part of the message it signs, we somehow need to "bind" the signature to the message [13].

5. Subliminal Channel Idea

The notion of subliminal channel (also called covert channel) was introduced by Simmons while considering his "Prisoner's Problem. In order to explain this notation, the description of prisoner's problem is found in [8,14]. As a brief description of the prisoner's problem we can say that a covert communication channels (also called subliminal channels) are often motivated as being solutions to the ``prisoners' problem.'' Consider two prisoners in separate cells who want to exchange messages, but must do so through the warden, who demands full view of the messages (that is, no encryption). A covert channel enables the prisoners to exchange secret information through messages that appear to be innocuous. A covert channel requires prior agreement on the part of the prisoners. For example if an odd length word corresponds to ``1'' and an even length word corresponds to ``0'', then the previous sentence contains the subliminal message ``101011010011'' [15]. So, a subliminal channel is a way of embedding information in public communication in an undetectable way. Some sort of shared secret (a key, knowledge of what to look for) is needed to reconstruct the
subliminal information [12].

Subliminal channels are a fascinating twist to digital signatures. Schneier [3] makes a good analogy of prisoner's problem The concept of subliminal channels in digital signature schemes was invented by Gustavus Simmons in 1983 [13] . The basic protocol (from [3]) goes like this:
1) Alice generates an innocuous message.
Dear Alice,
Elvis' singing can ameliorate Peter's emotions! Tom offered me orange
Rolaids! Randall opened Will's aging T-bird's engine in Georgia. Hot tamales!
Sincerely, Bob
2) Using a secret key she shares with Bob, Alice signs the message in such a way
that she hides her subliminal message in the signature.
3) Alice sends the message and its signature through Walter to Bob.
4) Walter checks the validity of the signature and makes sure there are no overt
escape plans in the message. Since he has no idea the subliminal message is
there, he passes the message along to Bob.
5) Bob confirms that the signature of the message is a valid signature of Alice.
6) Bob tosses the message in the trash and uses the secret key that he and Alice share to extract the subliminal message.

An important use of covert channels is in digital signatures .It is very interesting to note that the issue of subliminal channels in digital signature schemes first arose when the USA and USSR were deciding on a nuclear arms limitation treaty. Both nations agreed to place sensors in the other's nuclear facilities to check for compliance with the treaty. The following is from [16], which was in turn paraphrased from [7]. Since signatures with a subliminal message embedded in them look no different than regular signatures, Walter should never even know the channel exists. Even if he did know it was there, he doesn't know the secret key, and thus could not read the message. There are two types of these channels: broadband and narrowband. A broadband channel allows Alice to hide a subliminal message on the order of 160 bits, while a narrowband channel usually only hides a few bits per signature [17].

A subliminal channel is thus a covert communication channel to send a message to an authorized receiver. This message cannot be discovered by any unauthorized receiver. In [14], Simmons also invented the concept of subliminal channel in conventional digital signature schemes. The subliminal message is hidden in what looks like a normal digital signature and only authorized receiver can read it. The subliminal channel in a digital signature has several applications [18].

In 1985, Simmons [19] showed that in any digital signature scheme in which α bits are used to communicate a signature that provides β bits of security against forgery, where α > β, the remaining α - β bits are potentially available for subliminal communication. In [19], Simmons defined that if the subliminal channel uses all, or nearly all, of the α - β bits, it is said to be broadband (this means that this channel uses all available "space "in the signature), while if it uses only a fraction of the α - β bits, it is said to be narrowband. So, narrowband channels use a fraction of the available "space" but generally offer some other advantage over broadband channels.

However, the length of the digital signature generated in their proposed schemes is too long, while the size of the secret keys kept by the signer and the subliminal receiver are also large. Jan and Tseng proposed two new signature schemes with subliminal channels in [20].

Some of subliminal channel are designed to present different solutions of the prisoner's problem. One of these schemes is the elementary subliminal channel which allows the transmission of one-bit messages. In order to do this, the concept of redundancy of transmitting information must be introduced [4]. The Simmons subliminal channel is due to Simmons and it is based on the factorization problem [13]. Other schemes are Ong-Schnorr-Shamir subliminal channel and designed by Simmons [21] and Seberry-Jones subliminal channel has designed using Shamir's fast authentication [22] . Finally, some examples of recent subliminal channels are covered in details in [23] and [24].

6. Proposed Subliminal Channel

In this paper, we propose a design of a new subliminal channel based on Prisoner's problem. In order to design this subliminal channel , the two parties (representing the prisoners sharing this channel) agree in advance upon the number of bits (n) used to generate the message of binary messages (C) .The elements of this set is equal to 2^n . For example, if n=3, then we can generate 2^3=8 binary elements each contains three bits and starting from values 0 to 7 in decimal representation. The two parties are then assign bit positions (b) to each element in the set C starting form position zero (b_0) to position (b_7) in this example . So, in our example for n=3, the elements position are labeled as $b_0,b_1,b_2,\ldots b_7$. In general, the positions of elements for any value of n is $b_0,b_1,\ldots,b_{2^n-1}$. After that, the set C is divided into two equal sets of binary messages C_0 and C_1, where C_0 contains the binary messages located at even positions of the set C i.e., bit positions $b_0,b_2,\ldots..b_{2^n-2}$, while the other set C_1 contains the even bit positions $b_1,b_3,\ldots b_{2^n-1}$.The next step is encoding the elements of these two sets using biquinary code (5043210). In order to explain such conversion, let us take the following simple example:

Suppose we want to encode the decimal number 3 whose binary representation is 0011 .Using the decimal representation (8421) ,we can simply convert 0011 to decimal number 3 by the following traditional computation :
0*8+0*4+1*2+1*1=3. The same decimal number 3 is represented in biquinary (5043210) as 0101000. So, using the same principle of the above computation, we can convert 0101000 to 3 as follows:
*0*5+1*0+0*4+1*3+0*2+0*1+0*0=0+0+0+3+0+0+0=3*.
Using biquinary code provides an additional secrecy to the channel between the two parties. The codes of some decimal numbers in biquinary code are illustrated in table 1.

Furthermore , the two parties select two prime numbers p ,q and an initial positive inter (r) such that GCD (p,r)=1 and GCD (q,r)=1 .Then , the parties select one element which is considered a meaningful message from each set C_0 and C_1. The meaningful messages can be chosen according to the following equations:

$$x_1 = [(\sum_{i=b_0}^{i=b_{2n-2}} i \oplus r) + (p * q)/(r-1) \bmod 2^n] \quad (1)$$

$$x_2 = [(\sum_{i=b_1}^{i=b_{2n-1}} i \oplus r) + (p * q)/(r+1) \bmod 2^n] \quad (2)$$

Where x_1 and x_2 represents the selected meaningful messages which are authenticated between the two parties. These two equations can be used to generate the authenticated meaningful messages such that the two messages may be in different sets of C_0 and C_1 or may be belong to either of C_0 or C_1 . As we see these two equations contains multiple secret parameter, so they provide more secure channel. In addition, these two equations give an alternative method of selecting the meaningful messages.

Now, consider that the enemy may steal some secret parameters, then the probability of discovering the authenticated meaningful messages can be calculated as follows:

When the messages are in different sets (C_0 and C_1) , then the probability is$1/(2^n/2)* 1/(2^n/2) = 1/(1/(2^n/2)^2)$ (without using the secret equations) , whereas the probability of finding these messages if the two meaningful messages belong to either one set, then the probability becomes $(1/1/(2^n/2) + 1/1/(2^n/2)=2/1/(2^n/2))$,so the total probability is T(P) :

$$T(P)= 1/(1/(2^n/2)^2) +2/1/(2^n/2)= \frac{1+2(1/2^n/2)}{(1/2^n/2)^2} \quad (3)$$

As we choose larger value of n , then the probability in equation (3) decreases.

To add more secrecy to the algorithm, these generated messages shifted left at the sender end by a variable value $(\frac{r}{n})$ .At the receipt end , the receiver returns back this message by performing shift right by the same value $(\frac{r}{n})$.

Another important point in this algorithm is that the value of (r) may be changed in each next transmission according to new date and time of the next transmission which provides a secure factor for the subliminal channel. If we suppose that D stands for date and T stands for time ,then the new value of (r) for the next transmission can calculated as follows :

$$r = \frac{r+\alpha}{\mathrm{r}} \quad (4)$$

$$\alpha=E(D||T) \quad (5)$$

, where E represents any encryption algorithm(in this method, we use RSA algorithm) and || represents concatenation .The concatenated date and time are converted to digital ones.

So according to the above explanation, our algorithm steps as follows:

Algorithm

INPUT: An n-bit, two prime number p ,q (secret), a positive integer r such that GCD(r,p)=1 and GCd(r,p)=1.

OUTPUT : Two sets of binary groups C1,C0 such that we can choose one element from each set .(X1,X2).

1: Generate 2^n bits

2: Divide 2^n bits into two groups C_0 which represent odd bits positions and C1which represent even bits positions,

$C_0 = b_0, b_2,b_4,\ldots\ldots b_2{}^n{}_{-2}$, where b denotes to a distinct bit position

$C_1= b_1,b_3,b_5, \ldots\ldots b_2{}^n{}_{-1}$

3: Convert set of all possible bits into biquinary code and these news generated codes are sent via the channel .

3.1: Calculate the meaningful message according to the following secret equation:

$$x_1 = [(\sum_{i=b_0}^{i=b_{2n-2}} i \oplus r) + (p*q)/(r-1) \bmod 2^n]$$

3.2: Calculate the meaningful message according to the following secret equation:

$$x_2 = [(\sum_{i=_{b1}}^{i=b_{2n-1}} i \oplus r) + (p*q)/(r+1) \bmod 2^n]$$

3.3 : Sift left x_1 and x_2 certain times according to the following formula:

X_{11}= (x_1 shift left (r/n)), where r/n represents the number of shifts.

X_{12}=(x_2 shift left(r/n))

4: Return x_{11}, x_{12}

5: select new value to r for the next transmission according to the formula $r = \frac{r+\alpha}{\mathrm{r}}$, where α=E (D||T).

6: Go to step 1.

7. Analysis

The propsed paper presents important steps which lead to 1:Refering to equation (3) we find that this method provides a probability less than other subliminal channels and this probability approaches to zero when n becomes very large .So, we reach to an approximately perfect secure subliminal channel.

2:Using equations(2) and (3) in selecting the meaningful messages at different sets not in one set(as do the other subliminal channels)gives a mean of deceiving the enemy in an affective way. These

3: These equations (2) and (3) have many secure parameters such as selecting prime numbers p, q in advance. Other parameters are selected by the agreement between the parties and we know that the most important mean to reach the perfect security as Shannon said [4].

8. Results

The two authentic meaningful messages generated when n=3,p=11,q=17,and initial value of r=3 is as follows:

The numbers of all possible values are: 000 001 010 011 100 101 110 111

The even bits C_0 = 000 010 100 110

The odd bits C_1 = 001 011 101 111

By applying equations (1) and (2) we get two meaningful messages which are x_1=010 from set C_0 and x_2= 101from

set C_1 which are in different sets . But if use another value of r for next transmission depending on data and time of the next transmission, we get another different meaningful messages which are x_1= 010 and x_2=110 and these two values are in one set C_0. Figure 1 illustrates different values of meaningful messages by using different values of r with n=3 with different values of (r) .

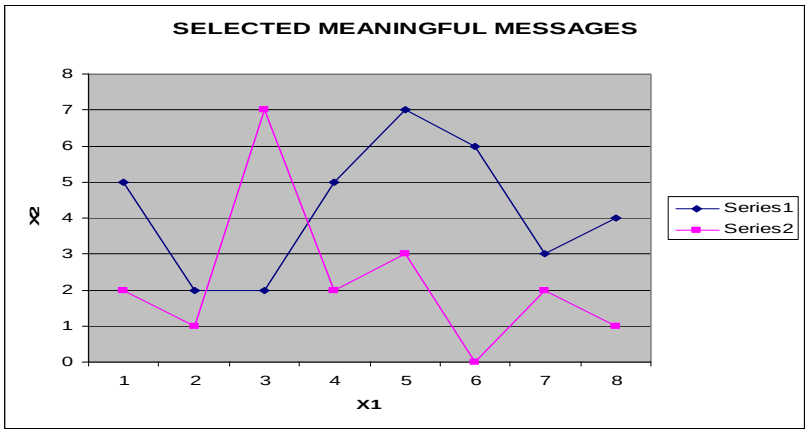

Figure 1: Different values for meaningful messages when n=3.

The selected meaningful messages are then coded by using biquinary code(5043210) as illustrated in table1.

Decimal Representation	*The original codes(421)*	*(biquinary)5043210*
0	*000*	*0100001*
1	*001*	*0100010*
2	*010*	*0100100*
3	*011*	*0101000*
4	*100*	*0110000*
5	*101*	*1000001*
6	*110*	*1000010*
7	*111*	*1000100*

Table1: Biquinary code

In the same manner we can get different values for meaningful messages by using different values of n , p,q and r. Figures 2,3,and 4 illustrates some of these values:

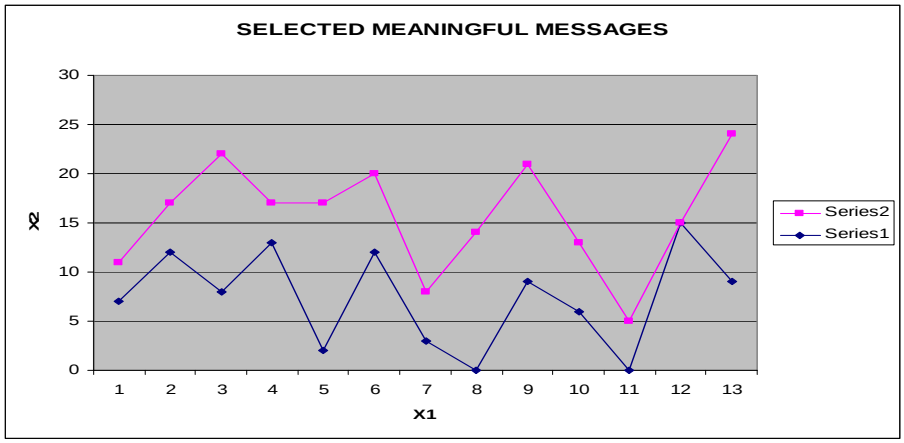

Figure2: Different values for meaningful messages when n=4.

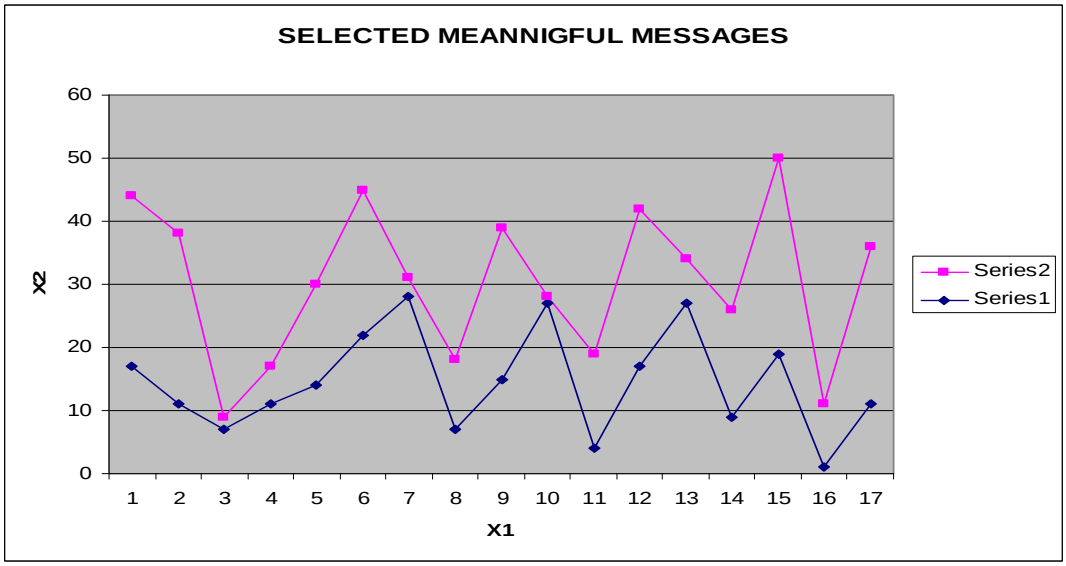

Figure3: Different values for meaningful messages when n=5.

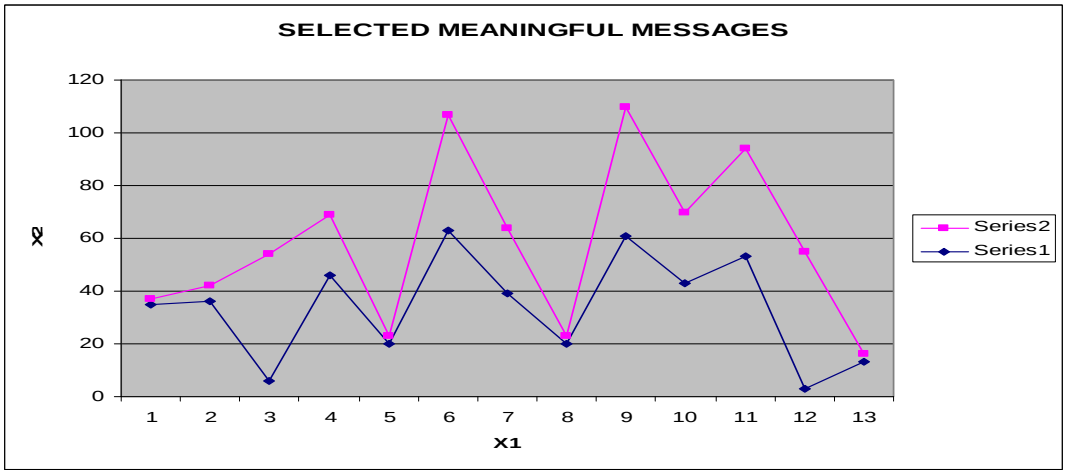

Figure3: Different values for meaningful messages when n=6.

9. Conclusion

The subliminal channel proposed in this work relies on applying bit transformation with variable values that are used to generate vast and different transmitted messages. Using different values enables parties to enhance their secrecy against enemies .The parties must agree in advance about how to change this value such as using secret equations that generates a new value of n. For instance, they can agree on changing these values after m of days. Most of the subliminal channels choose one fixed meaningful message for each set of even and odd binary values ,but the subliminal channel in this paper uses a method of selecting these meaningful messages according to secret equations such as equation 1 and equation 2 proposed in section 6 . These equations provide the authorized parties with different meaningful messages rather than selecting them as fixed values. According to this method, the authorized users can give an additional secrecy that can deceive the enemy because the equations contains secure parameters such as p, q, n and r, and in additions to these secure values the two parties had agreed in advance about how they will use these secret parameters. Another additional secrecy factor can be provided by this method so that the two parties can transmit messages in an alternative form which is relatively different from the original subliminal methods and performed in the initialization of the transmission. This done by converting the set of all possible messages (which are known to the enemy) to another and different messages by choosing biquniary code , so the subliminal channel proposed in this paper provides two important secrecy enhancements first ,by using variable initial secret agreement and second ,secret equations which ensure hiding of the original messages and selecting meaningful messages from either different sets or may both in on distinct se . Consequently, this will lead to deceive the enemy in such a way that he/she will face difficulties to break the subliminal channel because the enemy in all traditional subliminal channels concentrates his effort on selecting messages from different sets. As a future work, one can use different forms of hiding the original messages such padding the messages with extra piece of information at any position within the original messages. Finally, the proposed method had been applied practically and gives important results.

References

[1] http://www.niksula.cs,hut.fi/~ged/NetSec/

[2] S. Goldwasser and M. Bellare, "Digital Signatures," *Lecture Notes on Cryptography"*, 1997, pp. 96-118.

[3] B .Schneier, "*Applied Cryptography Second Edition: protocols, algorithms, and source code in C"*, John Wiley & Sons, 1996.

[4] J. Seberry , J .Pieprzk," Cryptography: "An introduction to Computer Security" , Printice Hall, 1989.

[5] G. J. Simmons, " Subliminal Communication is Easy Using the DSA", Lecture Notes in Computer Science,765:218–232, 1994.

[6] D. Russell & G.T. Gangemi, Sr.," Computer Security Basics,1st Edition", July 19910-937175-71-4, Order Number: 714,464 pages, $29.95

[7] A .Shamir, "A fast signature scheme ", MIT Laboratory for Computer science , Tech.Memo . 107,July 1978.

[8] A.M .Odlyzko , , "Cryptanalytic attacks on multiplicative knapsack cryptosystem and on Shamir's fast signature scheme" , IEEE Trans. on Inform. Theory , Vol. IT30,No,4, July 1984,pp.594-601.

[9] H .Ong- Schnorr , , A. Shamir ,. , "An efficient signature scheme based on quadratic equations" , Proceedings of the 16th Symposium on the Theory of Computing , Washinton DC, April 1984.

[10] T .El Gamal ,., "A public key cryptosystem and signature scheme based on discrete logarithms" , IEEE Trans. on Inform. Theory , Vol. IT31,No,4, July 1985,pp.469-72.

[11] R. Rivest , , A. Shamir , L. Adleman , , "A method of obtaining digital signatures and public –key cryptosystems" , CACM , Vol . 21 , No . 2 Feb. 1978, pp120-8.

[12] S.Hardy , "Making Use of the Subliminal Channel in DSA", The Fifth HOPE July 10, 2004, http://www.aculei.net/_shardy

[13] D.R .Stinson.," Cryptology: Theory and Practice", CRC Press, Inc., 1995.

[14] G.J. Simmons , . , "The prisoners' problem and the subliminal channel" , Advances in Cryptology : Proceedings of CRYPTO 83 ,(ed. D. Chaum), Plenum , New York , 1984,pp.51-67.

[15] http://www.rsa.com/rsalabs/node.asp?id=2351

[16] R. Anderson, S. Vaudenay, V.Preneel., K .Nyberg., "The Newton Channel,"Information Hiding 1996, 1996, pp. 134-148.

[17] N. Carruthers, "Digital Signature Schemes", Department of Math and Computer Science Middlebury College,December 9, 1997

[18] G.J. Simmons., "The history of subliminal channels", IEEE Jour. on sel. Areas Comm., Vol.16,No.4, pp.452-462, 1998.

[19] G.J. Simmons., "A secure subliminal channel", in Advances in Cryptology, Crypto' 85, LNCS 218, pp.33-41, Springer-Verlag, 1985.

[20] J.K. Jan and Y.M. Tseng, "New digital signature with subliminal channels based on the discrete logarithm problem", ICPP Workshop 1999, pp.198-203.

[21] G.J .Simmons., "The subliminal channels and the digital signatures", Sandia National Laboratory , preprint 1984,

[22] J. Seberry , , "A subliminal channel in codes for authentication without secrecy ", Ars Combinatorial , Vol . 19A, 1985,pp. 337-42.

[23] A. Beimel and Y. Stahl. "Robust information-theoretic private information retrieval", 3rd Conf. on Security in Communication Networks, volume 2576 of Lecture Notes in Computer Science, pages 326{341. Springer-Verlag, 2002.

[24] I. Goldberg. "Improving the Robustness of Private Information Retrieval". In Proceedings of the 2007 IEEE Symposium on Security and Privacy, May 2007. http://www.cypherpunks.ca/~iang/pubs/robustpir.pdf.