

An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography

## Navneet Singh Sikarwar

*Abstract*— In this paper a protocol is elucidated, it is based on multilevel steganography and dynamic cryptography in the secure information transmission, because the growing possibilities of modern communications require the special means of confidential and intellectual property protection against unauthorized access and use. Especially these problems are actually for computer networks, which make possible to exchange the large amount of digital information (text, audio, video, and image). The use of multilevel steganography provides more strength compare to simple steganography technique and similarly dynamic cryptography also gives more strength compare to simple cryptography.

*Index Terms*— Dynamic Key Cryptography, Multilevel Steganography, Steganography, Cryptography and Secure Communication

### I. INTRODUCTION

THE term "Secure Information Transmission" is not new today. In fact several examples from the times of ancient Greece are available in Kahn [1]. In recent years, everything is trending toward digitalization and with the rapid development of the Internet technologies, digital media can be transmitted conveniently over the network. Therefore, messages need to be transmitted secretly through the digital media by using the many security techniques available in market, generally it are based on either steganography or cryptography.

Steganography derived from Greek word literally means covered writing. It includes vast array of secret communication method that conceals message very existence. Computer based steganography allows changes to be made to what are known as digital carriers such as images or sounds. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-file with the help of secret key, a so-called stego-file is obtained [2]. This paper uses the Multi-Level Steganography, is a new concept for hidden communication in computer networks. It uses at least two steganographic methods are utilized either these methods are same or different type; in such a way that one method serves as a carrier for the second one [3], [4], [5].

Cryptography is the study of secret (Crypto) writing (graphy). Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual underlying cryptography). Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are generically classified along three independent dimensions [6], [11].

There are two basic techniques in cryptography [7], [12], [13]: symmetric and asymmetric cryptography. In symmetric cryptography, encrypted and decrypted keys are the same. In contrast, cryptography using different encrypted keys from decrypted keys is called asymmetric cryptography. Each of them has pros and cons. Because of its characteristics, asymmetric cryptography is more secure than symmetric in key distribution and exchange. However, symmetric cryptography is significantly faster than asymmetric cryptography. However if we want same level of security, then size of asymmetric key must be ten times or more that of symmetric key size [8], [14], [15].

The Dynamic cryptography is required where a message is divided into many parts and each part of the message is encrypted by a new key. This requirement will be accrued the problem in cryptography: "How we manage and shared the set of keys between the communicated parties". One of the solution of this problem is dynamic cryptography, in dynamic cryptography very few initial information are shared only one time by very secure channel [9], [10],

This paper give an idea about integrated synchronized protocol for secure information transmission derived from multilevel steganography and dynamic cryptography. The success of any dynamic cryptography will depends on secure channel by which initial information are shared, this paper also give an architecture for secure channel.

Navneet Singh Sikarwar; Assistant Professor & Head of Department, Department of Computer Science & Engineering, B.S.A. College of Engineering & Technology, Mathura (U.P.), India. Email: i\_m\_navneet@yahoo.co.in

The rest of paper is structured as follows. In the following section give an idea about proposed integrated synchronized protocol. Section III is focus on analysis of proposed integrated synchronized protocol. Section IV gives detail about merits and demerits of the protocol. And in the last section conclude the paper.

#### II. PROPOSED INTEGRATED SYNCHRONIZED PROTOCOL

This protocol is derived from multilevel steganography and dynamic cryptography; the combined and synchronized efforts of both makes this protocol more secure compare to other technique. This section is divided into three sub sections: first for establishment of secure channel by which either initial information are shared for dynamic key generation or final stego-file transmitted, second for dynamic key generation and third for multilevel steganography algorithm.

#### A. Algorithm for secure channel establishment

This algorithm is used the concept of IP address, port no and key, because if an application is running on a machine then no other application will run on same port even at the same machine that have same IP address.

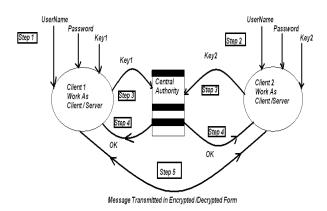


Fig. 1. DFD for secure connection establishment

In this model when two clients want to communicate to each other, first they send a request to center authority for connection establishment, in this request they send their IP Address, Port number and secret key. The center authority server verifies all the details and then send ok signal to the client. After getting ok signal, clients start the communication now there is no role of Central authority and Initial message for dynamic key generation are transmitted in Encrypted by using Hash function. We can use this channel not only for initial information used in dynamic key generation but also used for stego-file transmission.

#### B. Algorithm for dynamic key generation

In the dynamic cryptography, a message is divided into many subparts and each part is encrypted or decrypted by different key, these are dynamically generated by both communicated parties. The dynamic key generation algorithm required initial information sharing between both parties.

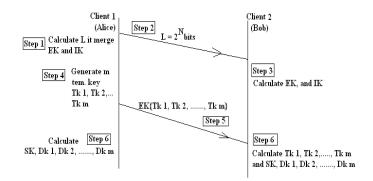


Fig. 2. DFD for dynamic key generation

Step 1 and 2 : In this step client 1 choose Encryption Key (EK) and Initial Key (IK), after it merge both key and prepare a  $L = 2^n$  bits size message, send it by secure channel to other communicated client 2. Here n is number of dynamic key that we want to generate.

Step 3: Client 2 extract EK and IK.

Step 4: Now client 1, generate m temporary key Tk1, Tk2, ...., Tkm. The value of m is also calculated by help of L and n.

Step 5: Client 1 encrypt these temporary key by EK and send to client 2 again use secure channel for it.

Step 6: Client 2 decrypt it by EK and get temporary key Tk1, Tk2, ....., Tkm . Now both client know value of EK, IK and Tk1, Tk2, ....., Tkm, and ready for n dynamic key.

One more step is required for seed key (SK) before generation of first dynamic key.

SK = IK (XOR) TK1 (XOR) TK2 (XOR)..... (XOR) TKm.

### Steps for First Dynamic key

Calculate

SK (XOR) TK1 (XOR) TK2 (XOR) .... (XOR) TKm. The result of it is string of 0 and 1, for example if result is 1010 on the basis of it. We can write an equation of X:

$$X^{3} + X^{1}$$

now put X = IK in the above equation, suppose this value is Y then  $DK1 = Y \mod 65536$ 

Steps for Second Dynamic key Calculate

SK (XOR) TK2 (XOR) ... (XOR) TKm. (XOR) DK1 The result of it is string of 0 and 1, on the basis of it. We can write an equation of X, and put X = DK1 in the above equation, suppose this value is Y

then  $DK2 = Y \mod 65536$ 

Similarly we can write the steps for Nth Dynamic key

Steps for Nth Dynamic key Calculate

SK (XOR) TKn-m (XOR) .....DKn-3 (XOR) DKn-2 (XOR) DKn-1 The result of it is string of 0 and 1, on the basis of it. We can write a equation of X, and put X = DKn-1 in the above equation, suppose this value is Y then DKn = Y mod 65536

Both clients store all the Dynamic keys in an array DK of N Size. This array is used in for encrypting and decrypting secret message.

# *C. Multilevel Steganography using Dynamic Cryptography Algorithm*

Multilevel steganography algorithm uses two algorithm one for hiding information and other for extracting information.

1) Steganography Hiding information

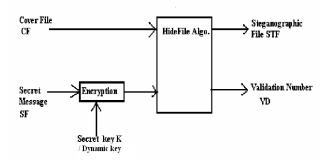


Fig. 3. DFD for information hiding

StegoHideFile (CF, SF, K)

*Input:* CF is innocent cover file, SF is secret text message/ secret message file / setgo file, and K is secret key/Dynamic key.

Output: STF stego file and validation number.

Procedure: // STF is location where we store stego file.

Step1: Open STF in write mode and CF in read mode.

Step2: Write all content of CF into STF.

Step3: Close CF and add some random space into STF and generate validation no. and return validation no.

Step4: Open SF in read mode and encrypt all content of SF, using shared key K and write into STF.

Step5: Close SF and STF.

2) Stehanography Extracting Information

StegoUnHideFile (STF, VD, K)

*Input:* STF is file name or location for stego file, TF is file name or location to save secret message file, VD is validation number and K is secret key/Dynamic key.

Output: TF secret message file.

Procedure:

Step1: Open STF in read mode and TF in write mode.

Step2: Start read STF from value of validation number until end of file.

Step3: Decrypt the content of STF using shared key K and writes it into TF file.

Step4: Close STF and TF.

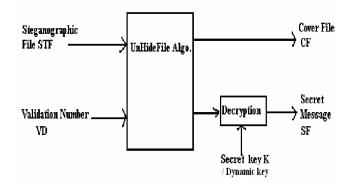
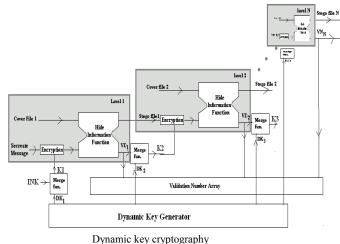


Fig. 4. DFD for extracting information

3) Multilevel steganography using dynamic cryptography: hiding information

Fig. 5. DFD for Hiding Information using Multilevel Steganography &



Dynamic Key eryptography

#### Multilevel Hiding Information (N) //here N is level

*Input:* N Cover File stored in array CF[N], N Dynamic key stored in array DK[N] and Secret Message/ Secret message file location STF.

*Output:* one steganography file SF and N validation number that is stored in array VD[N].

Procedure:

For I = 1 to N do

{ STF = StegoHideFile (CF[I],STF,DK[I});

above statement also return validation no. we encrypt this value by Dk[I] and stored in VD[I] location.

}

Return a stego file STF and Validation no. array VD [N].

4) Multilevel steganography using dynamic cryptography: Extracting information

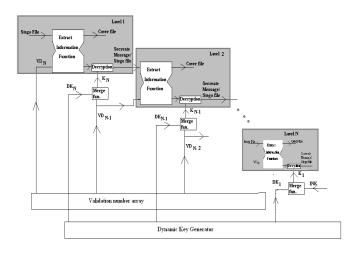


Fig 6. DFD for Extracting Information using Multilevel Steganography & Dynamic key cryptography

Multilevel Extracting Information (N) //here N is level

*Input:* Stego file STF, N Validation no. stored in array VD[N], and N Dynamic key stored in array DK[N].

Output: secret message file/ secret message SM.

Procedure: For I = N to 1 do

{ decrypt the value of VD[I] using DK[I] key and stored in VD[I]

SM = StegoUnhideFile(STF, VD[I], DK[I});

}

Return Secret message file SM.

In this protocol, the multilevel steganography applied stegofile can be send either by simple email or by a secure channel it is depends on how much level security we required. But we will prefer secure channel only for information sharing required for dynamic key generation.

## III. ANALYSIS OF PROPOSED INTEGRATED SYNCHRONIZED PROTOCOL

This work is based on multilevel steganography and dynamic cryptography, therefore strength of this work also based on both of these factors. This section is divided into three subsections.

## A. Analysis for secure channel

Let Alice and Bob are authorized user want to communicate over this framework. They want to prevent Oscar (the bad guy or unauthorized user) from listening. There are many ways for Oscar to enter in secure channel and listen to the secret message. All these ways are mentioned in following cases.

- i) In this case, Oscar tries to find out user name and password of Alice or Bob to run the application because without knowing the user name and password no unauthorized user can run the application software that Alice and Bob used. But this attack is very weak because it is based on personal analysis of Alice and Bob's life. Today's login system provide limited chance (eg. 3 chance to login) to login so that this attack fails to know user name and password of Alice and Bob. This works provides provision if any user does not enter correct user name and password in three time's then central authority denied his request for login.
- In this work, secret key of Alice or Bob is used for ii) authentication. The central authority checks machine address, port number and secret key, if all the values are correct then only the central authority allows for connection establishment otherwise it will denied the request. Alice and Bob will try to choose such a secret key which will be more secure from the security point of view. In a survey it is found that if the key length is more then 256 characters, it will be more secure against brute force attack. In this work, Alice and Bob use key of length 256 and this work uses Unicode value. In Unicode system, each character is represented by 65536 combinations. So if Alice and Bob use the key of 256 lengths, Oscar will try to break it. If Oscar applies brute force attack, it requires 65536 x 65536.....256 times = 6.844E+1237 steps to break this key for 256 length. So this step will not easily broken by Oscar.
- iii) In this work, central authority checks machine address, port number and secret key of Alice and Bob. The aim of Oscar is to listen to the secret message that Alice and Bob is communicating. In a machine total number of ports is 65536, in which 1024 are reserved ports and remaining is free ports. In this framework Alice, Bob and central authority run on fixed port therefore if Alice and Bob communicating each other then it is not possible (or impossible) for Oscar run his application on same port. The central authority does not allow Oscar for communication until he does not run his application on right machine, right port and with right key.
- iv) This work uses two different encryption decryption algorithms. First use when Alice/ Bob send his key to central authority and second use when Alice and Bob communicate each other. Both algorithm use linear mathematical equation for encryption and decryption. So that it is not easy for Oscar to break these algorithms, because one client uses different linear mathematical equation for different client.

The conclusion of the above case study is this channel is secure for short length message transmission; therefore this protocol is used achieving more security.

## B. Analysis for dynamic key generation algorithm

The complexity of any dynamic key generation algorithm are depends on the number of operations required to execution, as well as it also indicate the randomness of dynamic key.

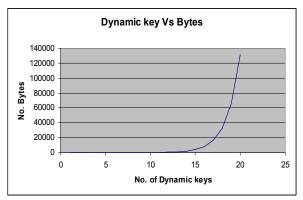


Fig. 7. Dynamic key Vs No. Bytes required to shared

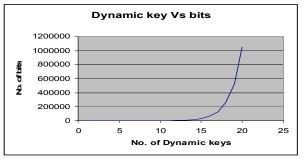


Fig. 8. Dynamic key Vs No. bit required to shared

The graph shown in Fig. 7 and Fig. 8 are not linear but it is exponential, this indicate complexity of dynamic key generation is high compared to other algorithm those graph are linear.

Table I. Operation required generating dynamic key

No. of Dyn amic key	Random Tempora ry key	No. of Encrypt ion & Decrypt ion	No. of Bitwise operation	No. of Modules operatio n	No. of logarith m operatio n
1	1	4	1	1	2
2	3	8	6	2	2
3	5	11	14	3	2
4	6	14	24	4	2
5	7	17	37	5	2
6	9	19	52	6	2
7	10	22	69	7	2
8	11	24	88	8	2
9	12	26	110	9	2
10	13	29	133	10	2

Table 1 indicate the how many operations are required to calculating the dynamic key, this table also indicate strength of key generation algorithm.

#### C. Analysis for multilevel steganography algorithm

The multilevel steganography algorithm is backbone of this protocol. The encrypted secret message is steganographed in a comparatively innocent file. This stego file has almost the same properties as original cover file. Moreover encrypted contents are steganographed multiple times using either same or different steganography approaches. Result of first round of the steganography is given as input to the next round of steganography process with a different cover file. The introduction of multiple phases of steganography process increases the deciphering complexity of the secret message and dynamic key cryptography is also increasing it strength.

Let Alice and Bob use steganography and Oscar try to identify it as well as extracting secret information from it. There are many ways for Oscar to identify it as well as extracting secret information. All these ways are mentioned in following cases:

- Oscar tries to identify the file that has been transmitted as a stego file. He tries to access the original cover file and compare cover file with stego file. With the use of multilevel steganography then this detection is quite complex.
- ii) Stego file detection is not sufficient for extracting secret data from it. Oscar requires validation number, secret key and needs to know the specific steganographic approach. This is quite a complex task in itself since technique of steganography varies with stego file.
- iii) The number of levels of steganography and the specific approach to be used at each level is agreed upon by the Alice and Bob prior to actual transfer. Henceforth detecting the levels of steganography and specific approach of steganography used is difficult to determine.

This multilevel steganography provide registrant against media specific attack applied on stego-file; these are listed bellow.

- 1. Image file
  - a. Examination of color palette.
  - b. Examination of size of image file.
  - c. Comparison of Stego file format with that of cover file.
  - d. Application of filter to steganogram resulted from stego file.
  - e. Visible representation of statistical data of stego file
- 2. Audio file
  - a. Analysis of patterns in background noise couldn't detect the existence of stego file in the transferred audio file.
- 3. Video File
  - a. Examination of distinguishing movements in video could not point out video file as stego video file.

## IV. MERITS & DEMERITS OF PROTOCOL

There are many advantage of this protocol these are listed bellow.

- 1. This work provides security at machine and port level, so that the framework becomes more secure and difficult to eavesdrop.
- 2. It provides provision for central authority that is used for user authentication.
- 3. It provides facility for secret message transmission using secure channel.
- 4. It provides secret message transmission in full duplex mode.
- 5. It uses the advantage of dynamic key cryptography that is better than cryptography as well as session key cryptography.
- 6. There is no limit about the size of message, on which most of the steganography algorithm face the problem.
- 7. There is no restriction about type of message file in the steganography, this protocol allow all type steganography.
- 8. This work also provide resistant against stirmark attack.

This protocol has one limit, when we use multilevel steganography the size of stego-file become increase, so that it will not be suitable for mobile devices that have low battery.

## V. CONCLUSION

This paper is based on an integrated and synchronized protocol, it a combined effort of secure channel algorithm, dynamic key cryptography and multilevel steganography. This paper also focuses on attack analysis and strength of this work. At last this work also gives detail about its merits and demerits of it.

#### VI. REFERENCES

- Kahn, The Codebreakers the comprehensive history of secret communication from ancient times to the Internet, Scribner, New York (1996).
- [2] C. Cachin, "An Information-theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318, 1998
- [3] Wojciech Frączek, Wojciech Mazurczyk, Krzysztof Szczypiorski, "Multi-Level Steganography: Improving Hidden Communication in Networks", Cornell University Library, Jan 2011, http://arxiv.org/ftp/arxiv/papers/1101/1101.4789.pdf
- [4] Al-Najjar AJ.: The Decoy: Multi-Level Digital Multimedia Steganography Model, In Proc. Of 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece, July 23-25, 2008
- [5] Sikarwar Navneet, "Multilevel Steganography: An Enhancement in Steganography and Comparative Study with Current Tools", International Journal of Computer and Network Security, Vol. 2, No.1, pp. 25-29, Jan 2010.
- [6] D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.
- [7] B. Schneier, Applied Cryptography, John Wiley & Sons, 1996.
- [8] M. Blaze, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, Report of Ad Hoc Panel of Cryptographers and Computer Scientists, Jan. 1996. (http://www.crypto.com/papers/)

- [9] R. Divya & T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks", International Journal of Scientific & Engineering Research Volume 2, Issue 5, May- 2011, ISSN 2229-5518
- [10] Xukai Zou, Yogesh Karandikar and Elisa Bertino, "A Dynamic key management solution to access hierarchy", International Journal of Network Management 2007; 17: 437-450
- [11] Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar, "Cryptography and Steganography of Video InformationIn Modem communication", Electronics And Energetics, vol. 11, pp. 115-125, 1998.
- [12] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3rd ed., Prentice-Hall, 2003.
- [13] W. Stallings, Cryptography and Network Security, 4th ed., Prentice-Hall, 2005.
- [14] B. A. Forouzan, Data Communications and Networking, 4th ed., McGraw-Hill, 2007.
- [15] G. Blelloch, Introduction to Cryptography, online: http://www.2.cs.cmu.edu/afs/cs/project/pscicoguyb/realworld/c rypto.ps, 2000.



Navneet Singh Sikarwar is Assistant Professor & HOD, Department of Computer Science & Engineering at B.S.A. College of Engineering & Technology, Mathura. He did B.E. in Computer Science & Engineering from M.P.C.T., Gwalior (M.P.). He obtained M.Tech. in Computer Science & Engineering from T.I.T., Bhopal

(M.P.).He is pursuing Ph.D. in Computer Science & Engineering from Bhagwant University, Ajmer (Raj.). He published 15 research papers in International, National journals and conferences. He has eight years of teaching experience. His area of specialization includes network security, data base management system, artificial intelligence and data structure. He is member of Computer Society of India, The Institution of Electronic and Telecommunication Engineers and International Association of Engineers. He is also reviewer of IJCNS, IJCIIS, IJNS and IJCA, IJSCE.