# A Model for Performance Enhancement of Steganography through Dynamic Key Cryptography

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

-----ABSTRACT-----

In Today's, Security are a big and challenging issues, for where the information has been transmitted. There are lots of techniques come in existence, but most of them are struggle against hackers and unauthorized users from last many decades. There are two most popular and reliable techniques has been used for security, these are Cryptography and Steganography, but now a days hackers are become more advanced and they have a lot of tools to break it. Therefore we have the requirement for more advance and trusted techniques, that have more strength compare to Cryptography as well as Steganography. This paper is based on a model for performance enhancement of Steganography techniques through new advance technique Dynamic key Cryptography.

Keywords - Steganography, Dynamic key Cryptography, Cryptography, Information Hiding.

Date of Submission: February 01, 2012	Date of Acceptance: April 24, 2012
---------------------------------------	------------------------------------

# I. INTRODUCTION

 $\mathbf{T}_{he}$ faster growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary both at the final user level and at the enterprise level, especially since the massive utilization of personal computers, networks, and the Internet with its global availability. Throughout time, computational security needs have been focused on different features: secrecy or confidentiality, identification, verification, non-repudiation, integrity control and availability. This has resulted in an explosive growth of the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alterative solution in hiding information. [1]

There are a number of ways for securing data. One is cryptography, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is steganography, where the secret message is embedded in another message, thus the existence of message is unknown.

#### 1.1 Cryptography

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 [2].

#### Methodology for transforming plain text to cipher text

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

#### Methodology for number of keys used

If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as symmetric, two keys, or public-key encryption.

# Methodology for processing plain text

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

#### 1.2 Steganography

There are a lot of techniques for information hiding, so of them are shown in fig 1.1, this fig show the hierarchy of information hiding techniques



Fig. 1 A Classification of Information hiding tech. [3]

Covert Channels is a sponging communication channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of letter channel's designer, owner or operator. [4][16]

Anonymity is a technique where creator of message undisclosed his/her Identity, therefore attacker and unauthorized user does not get the idea about owner of message. [4]

Copyright marking contrasting to steganography, has additional requirement of robustness against possible attacks. In Copyright marking it is not necessary to hide the information. [4]

Steganography is the art and science of hiding the fact that communication is taking place. Steganographic systems can hide messages inside of images or other digital objects. To a casual observer inspecting these images, the messages are invisible.

Steganography literally means, "covered writing" and encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the existence of the embedded messages is undetectable. Carriers of such messages may resemble innocent images, audio, video, text, or any other digitally represented code or transmission. The hidden message may be plaintext, ciphertext, or anything that can be represented as a bit stream.

#### **Steganography techniques**

Steganography is an art of delivering secret messages without being detected. There are two requirements to steganography. First, the secret messages should not be recovered by any party other than the supposed recipients. Secondly, the stegano-texts should not incur any suspicion. 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-image, a so called stego image is obtained. [5]



Fig. 2 Steganographic Model [4]

Cover media (object) is a carrier medium, like text, image, audio, video, or even the network packet. Secret message is a private message that is to be hidden in the cover media. When combined, the cover object and the embedded (secret) message make a stegoimage (object). A stego-key (a type of password) may also be used to hide and then later decode the message. The algorithms for creating stegotext with an embedded message and for decoding the message are collectively called a stegosystem. A stegosystem should hide the embedded message. Steganography technique is the algorithm applied to the cover media and secret message, to hide the message inside the cover media. [6]

#### Steganographic techniques used for image are

- 1. LSB Technique: hide secret message in the LSB of Cover file.
- 2. Masking and filtering techniques: like watermarking, first mark the location for hiding information then apply filter on it.
- 3. Algorithms and transformation techniques: using this technique we can use algorithm. [7]

#### Techniques for data hiding in audio and video file are

- 1. Low bit coding: Low-bit coding is the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, we can encode a large amount of data in an audio signal.
- 2. 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.
- 3. 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. [8]

#### 1.3 Dynamic key Cryptography

In modern security models, cryptography plays a fundamental role in protecting data integrity and information congeniality in systems. However, cryptography itself is subject to cryptanalysis attacks. To reduce the cryptanalysis attack risk, a dynamic key theory is presented and analyzed in this paper. Because these dynamic keys are one-time used symmetric cryptographic keys, they can significantly improve the security of cryptographic systems. The dynamic key theory generation scheme and key update mechanism are formally analyzed to demonstrate balance between security and performance. The theory can be applied to enhance the security and performance of cryptographic systems, especially those used in wireless networks communication. [9][15]

In Dynamic key cryptotography both party sender and receiver share very few information, basis of these shared information they generate many dynamic key at both end by using some functions. Sender and receiver use one key only for one message transmission. The Dynamic key cryptography is similar the cryptography technique but the Dynamic key cryptography use different key for different message encryption.

#### **II. PROPOSED WORK**

This work is based on how increase the performance of steganography against steganographic attackers, this work used the concept of dynamic key cryptography. The proposed work are use two algorithms one for steganography and other for dynamic key generation.

#### 2.1 Steganography Algorithms

#### **Information Hiding Algorithm**



StegoHideFile (CF, SF, K)

Input: CF is innocent cover file, SF is secret text message/

secret message file and K is 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.

**Extracting Information Algorithm** 



Fig. 4 DFD for 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 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.

#### 2.2 Dynamic Key Generation Algorithms



#### Fig. 5 DFD for Dynamic key generation

1. Alice and Bob exchange two keys EK and IK via a secure channel

	length of EK is $L/2$		lingth of IK is L/2	
$\leftarrow$		Lb	its	$\rightarrow$

Here the value of L is power of 2, so that number of dynamic key we want to generate is equals to N = log2(L)

 Now Alice generate m random (temporary) key in the range of 0 to pow(2,L/2). The temporary keys are following.

TK1, TK2, ..... TKm.

Alice encrypt these keys by using EK key and send to Bob.

EK {TK1, TK2, ..... TKm. }

- Bob decrypt these keys by using EK key and get keys. TK1, TK2, ..... TKm.
- 3. Now Alice and Bob both calculate seed key SK as following.

 $\label{eq:sk=ik} \begin{array}{l} SK = IK \; (XOR \; ) \; TK1 \; \; (XOR \; ) \; \; TK2 \; (XOR \; ) \ldots \ldots \\ (XOR \; ) \; \; TKm. \end{array}$ 

Steps for First Dynamic key

Calculate

SK (XOR ) TK1 (XOR ) TK2 (XOR )  $\dots$  (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 Alice and Bob store all the Dynamic keys in an array DK of N Size. This array is used in for Hiding and Extracting secret information.

# III. ANALYSIS OF PROPOSED WORK

The major solution for enhancing security and reducing the risk of such cryptanalysis attacks was to increase the key size used in the cryptographic systems. However, increasing the cryptographic key size is not always the best solution, since no matter how large the key is, its cryptography is still ultimately breakable. Every cryptographic key is only secure for a certain amount of time. In 2007, Lenstra [10] stated that the 1024 bit RSA encryption used in most banking and e-commerce systems may only be secure for a few more years. In addition, larger keys often require higher computational resources, especially in asymmetric cryptography. In practice, excessively large keys may admit denial of service possibilities whereby adversaries can cause excessive cryptographic processing. Large keys are also clearly unsuitable for mobile devices having slow processing units and/or limited battery powers.[13]

The security of this work is based on the strength of steganography as well as dynamic key generation algorithms, therefore the analysis of proposed work also divided into parts:

# 3.1 Strength of steganography algorithm

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 detect the transmitted file as a stego file

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 Dynamic key Cryptography then this detection is quite complex.

# Oscar tries to find out validation number and secret key

The Stego file detection is not sufficient for extracting secret data from it. Oscar requires validation number, dynamic 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.

A good steganographic algorithm is one that avoids the detection of stego file. Proposed work provides adequate resistance against various medium specific detection techniques in comparison to existing tools. Cover files supported by the framework are image, audio, and video files.

# 3.2 Strength of dynamic key generation algorithm

The strength of any dynamic key generation algorithm will be depend on the two factors first one is less sharing of information between the both communicated parties and second is dynamic key less dependent on other factor ( in ideal case it will random).

# Shared Information

In this algorithm we required only one time information sharing between both parties by a very secure communication channel.

Fig 6 and 7 give idea about how much length of message required to share for generation of dynamic keys.

# Dynamic key generation complexity

The complexity of dynamic key generation are depends on the no. of operation required to execution, as well as it also indicate the randomness of dynamic key.

Table 1 give idea about complexity of dynamic keys, therefore it now easily breakable.



Fig. 6 Dynamic key Vs No. Bytes required to shared



Fig. 3.2 Dynamic key Vs No. bit required to shared

No. of Dynamic key	Random Temporary key	No. of Encryption & Decryption	No. of Bitwise operation	No. of Arithmetic operation	No. of Modules operation	No. of logarithm operation	Total Operation
1	1	4	1	1	1	2	10
2	3	8	6	4	2	2	25
3	5	11	14	12	3	2	47
4	6	14	24	32	4	2	82
5	7	17	37	80	5	2	148
6	9	19	52	192	6	2	279
7	10	22	69	448	7	2	557
8	11	24	88	1024	8	2	1157
9	12	26	110	2304	9	2	2463
10	13	29	133	5120	10	2	5307
11	14	31	159	11264	11	2	11481
12	16	33	187	24576	12	2	24826
13	17	35	217	53248	13	2	53532
14	18	38	249	114688	14	2	115009
15	19	40	284	245760	15	2	246119
16	20	42	320	524288	16	2	524688
17	21	44	358	1114112	17	2	1114555
18	22	46	399	2359296	18	2	2359784
19	23	48	442	4980736	19	2	4981270
20	24	51	486	10485760	20	2	10486343

# Table 1: Operation required generating dynamic key

S. No.	Name of Tool	Technique used	Text steg.	Image steg.	Audio steg.	Video
						steg.
1.	EzStego [11]	LSB	Yes	Yes	No	No
2.	S-Tool [12][11]	LSB	Yes	Yes	Yes	No
3.	Steganos [11]	LSB	Yes	Yes	No	No
4.	JSteg [11]	Compression based	Yes	Yes	No	No
5.	Stego DOS [12]	LSB	Yes	Yes	No	No
6.	White Noise Stom	LSB	Yes	Yes	No	No
	[12]					
7.	Hide and seek [11]	LSB	Yes	Yes	No	No
8.	Proposed Model	Algorithms & Transformations	Yes	Yes	Yes	Yes

Table 2: Technique, Feature of Current tools and proposed model

# **IV. ADVANTAGE OF PRPPOSED WORK**

This proposed model has many advantage compared to current available tools and current tools have many limitation these are maintain in table 2.

The another advantage of this proposed work is it based on dynamic key concept, dynamic key have many advantage compared to other cryptographic key like session key, these are mentioned in Table 3.

Issues	Dynamic key	Session Key
Key Exchange	Once	Every Session
Life time	Within a	Within a session
	message	
Key Reusable	No	Yes
Vulnerable	No	Yes
under man in		
middle		
Attack		
From a	Decrypt a	Decrypt all
compromised	message	messages in the
cryptographic		session
key, adversary		
can		
From a	Cryptographic	Cryptographic
compromised	system is still	system and
pair of public	safe	session are
and private keys		vulnerable
of the key		
exchange		
protocol		

Table 3: Comparison between ses	sion key and
dynamic key	

# V. APPLICATION OF PRPPOSED WORK

There are many application of this model, these are listed bellow.

- 1. Military and intelligence agencies require unobtrusive communications.
- 2. Criminals also place great value on unobtrusive communications. Their preferred technologies include prepaid mobile phones, mobile phones which have been modified to change their identity frequently and hacked corporate switchboards through which calls can be rerouted.
- 3. Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.
- 4. Schemes for digital elections and digital cash make use of anonymous communication techniques.
- Recent attempts by some governments to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the net, including anonymous remailers and Web proxies.
- 6. Steganography may be used to communicate over public networks such as the Internet and Private network etc.

# V. CONCLUSION

This paper gives an idea about how dynamic key cryptography will be helpful for performance enhancement. This paper also gives an idea about various information hiding techniques and compares the proposed model with the current steganography tools. This paper also contains the information about complexity of dynamic key generation algorithm and how dynamic key have advantage over the session key. At last this paper gives idea about application of this proposed work. The author is grateful to the anonymous reviewers for valuable comments.

# REFERENCES

- Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar "Cryptography of Video InformationIn Modem communication", Electronics And Energefics, vol. 11, pp. 115-125, 1998
- [2]. Stinsown, D. "Cryptography: Theory and practice"
- [3]. F. A. P. Petitcolas, R. J. Anderson & M. G. Kuhn, "Information Hiding – A Survey", IEEE Journal of special issue on protection of multimedia content, 87(7), pp. 1062-1078, July 1999.
- [4]. 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.
- [5]. C. Cachin, "An Information-theoretic Model for steganography", in proceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318, 1998
- [6]. B. Pfitzmann, "Information Hiding Terminology," Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin, pp. 347-356, 1996.
- [7]. N. F. Johnson & S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, vol. 31, no. 2, pp. 26-34, Feb1998.
- [8]. W. Bender, D. Gruhl, N. Morimoto & A. Lu, "Techniques for Data hiding", IBM Systems Journal, vol. 35, pp. 313-336,1996
- [9]. Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, & Balasubramaniam Srinivasan, "Dynamic Key Cryptography and Applications", International Journal of Network Security, Vol.10, No.3, PP.161-174, May 2010
- [10].J. Kirk, "Researcher: RSA 1024-bit encryption not enough", PC World, IDG News Service, 2007. (http://www.pcworld.com/article/132184/researcher rsa 1024bit encryption not enough.html)
- [11].A.Westfeld & A. Pfitzmann, "Attacks on SteganographicSystem", <u>http://www.ece.cmu.edu</u> /~adrian/487-s06/westfeldpfi tzmannihw99.pdf
- [12].N. F. Johnson & S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, vol. 31, no. 2, pp. 26-34, Feb 1998.
- [13].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
- [14].Xukai Zou, Yogesh Karandikar and Elisa Bertino, "A Dynamic key management solution to access hierarchy", International Journal of Network Management 2007; 17: 437- 450

- [15].S. Kungpisdan, P. D. Le, B. Srinivasan, "A limited used key generation scheme for Internet transactions," Proceeding of Workshop on Information Security Applications, LNCS 3325, pp. 302-316, Springer Berlin, 2005.
- [16].D. Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", Scribner, 1996.

# **Authors Biography**



Navneet Singh Sikarwar is Asst. Prof. & 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 PhD. in Computer Science & Engineering from Bhagwant University, Ajmer (Raj.). He published 19 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.