International Journal on Applications in Computers
Volume1: Issue 1: May 2018, pp 3- 6. www.aetsjournal.com ISSN (Online) : XXXX - XXXX

A Survey on Hybrid Cryptography Techniques

J.Poongodir[#1] and S.Sathish[*2]

[#]*Assistant Professor, Department of CSE, Sri Ranganathar Institute of Engineering and Technology, Coimbatore*

[*] *Assistant Professor, Department of CSE, Sri Ranganathar Institute of Engineering and Technology, Coimbatore*

Abstract— *With the continues development of the computer network, information has been exchange in different format like text, image, audio and videos. In today's scenarios security is playing a vital role in networking. Securing all these types of information is most important. There are different types of cryptographic encryption methods are used to send the information through network with security. But still there are some open issues. Each encryption method has its own strength and weakness. The combination of various encryption techniques i.e. hybrid encryption techniques provides the better security. This survey analysis the different hybrid encryption techniques and working principle of those hybrid techniques.*

Index Terms— *Networking; Security and analysis; cryptographic; encryption; hybrid cryptosystem.*

I. INTRODUCTION

In the rapid growth of high performance network technology, digital data exchanging over the communication system is needed better security in storage and transmission of information. In this modern age, information is an asset because information plays a vital role in every aspect of human life, whether it is personal or professional therefore it is required to be protected without any laps. Cryptography, steganography and watermarking techniques are used to securely transmit the information over the network and digital data storage.

According to the William Stallings "Cryptography is branch of cryptology dealing with the design of algorithm for encryption and decryption intended to ensure the secrecy and/or authenticity of messages[1]. Cryptography is a process to convert original data to some jumbled data using key. Original data or information is called plain text and jumbled data is called cipher text. Based on the key value cryptographic algorithm can be classified into two broad categories called as conventional key cryptographic and public key cryptography. Conventional key [2] cryptosystem algorithm used only one secret key for both encryption and decryption process. Public key cryptography method used two different pair of related keys, one for encryption and another one for decryption process. Both conventional and public key cryptosystems having different types of algorithm to perform the encryption and decryption process. Some of the conventional algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), XOR cipher and important public key algorithms are RSA, Hill cipher and

Elliptic Curve Cryptography (ECC).

Steganography [3] is the process of hiding the messages and information in media effectively. There are various techniques are available to implement the steganography. The most important used steganography techniques are Least Significant Bit (LSB) , Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT). The steganography is implemented through two different types of domains, such as spatial domain and frequency domains. In spatial domain the encryption process is done directly on the pixel values of the image, in frequency domain, first transmitted the pixel values and then applied processing on the transformed coefficients.

Digital watermarking is a science of hiding information invisible in the cover image. Digital watermarking is to hide the huge existence of the message in the host image. It is used to hide information within the host image, in which cannot able to be retrieved by the third party or any other unknown persons. In general, watermark is appears behind the original document and will not harm the original content of the document. Watermarking is classified into two types one is visible and another one is invisible. Visible watermarking us embedded image which is able to be perceived by human eyes but it continuous to provide the copy right protection. Invisible watermarking is great embedded image which is not able be perceived by human eyes.

Each security algorithms have own its advantages. But still we are facing some security issues in networking. A hybrid encryption techniques is new approach to overcome the drawbacks of existing security algorithms and mechanisms. The idea behind the hybrid techniques are combines the two or more encryption techniques and improves the existing algorithms to get a new approach for encryption by extending the advantages of individual methods and rectify the drawbacks of other methods.

The main objective of this paper is to provide a complete survey on hybrid encryption techniques. There are several hybrid approaches has been proposed to improve the efficiency of the security. In this survey, we analyze the strength and weakness of all the prior approaches.

This paper organized as follows. In section 2, related work in the network security mechanisms. In section 3, we analyze the various hybrid encryption techniques. Finally this paper is concluded in section 4.

II. RELATED WORK

Cryptography is a technique to hide the data over communication channel. It is an art to hide the data to strangers. There are so any cryptography algorithms and methods has been proposed to maintain the security. In [4], the RSA algorithm is combined with Diffie Hellman key exchange algorithm. In this approach Diffie Hellman algorithm is used to generate the secret key for both encryption and decryption. RSA algorithm provides more security as compared to other algorithm. Article [5], proposed to describe a hybrid system where encryption algorithms are used in a predefined order on the same set of data one after the other to finally obtain in encrypted data form. This [5] cryptosystem combines the AES, DES and MD5 algorithms and forms a hybrid cryptosystems.

In [6], hybrid encryption algorithm is proposed for maintain the high level of security in cloud based services. It combines AES, BLOWFISH and TWOFISH algorithms. [6] includes the following procedure

1. Sender must register with correct login information
2. Select a file which you want to upload.
3. Apply ECDH for key generation.
4. Apply AES with Towfish or AES with Blowfish on selected file that will generate encrypted file.

III. LITERATURE SURVEY ON HYBRID TECHNIQUES

The challenges of maintaining the network security have been emphasized in many papers. As of today's usage of networking increases, hence the effective method of maintaining secrecy is more important in order to make the communication faster and reliable.

A. Hybrid Scheme for Cryptography and Watermarking

To enhance the security and copyright protection of digital data, the cryptographic and watermarking approaches are combined together and presented some new method. In this hybrid cryptosystems [7] the message is divided into five different parts and encrypts them with five identical encryption methods. Once the encryption is done, then the encrypted data is hidden by using watermarking approaches. The encryption and decryption process includes the following procedure.

1. The input data is segregated the five different parts.
2. Apply the five different techniques for each part.
3. After used these algorithms , the messages is concatenated and encrypted message is obtain as output.
4. Select the host image
5. One bit LSB watermarking, 2 bit LSB watermarking and three bit LSB watermarking are utilized to hide the encrypted message.

The fig.1 shows the hybrid encryption process which combines the process of cryptography and LSB watermarking. The same five cryptography algorithms and keys are used to decrypt the encrypted message at receiver side. At the receiver side, the process of decryption is performed, that is reverse of the encryption process.

The main advantages of this scheme is increased security of the data by combines the five different encryption algorithm along with LSB watermarking techniques.

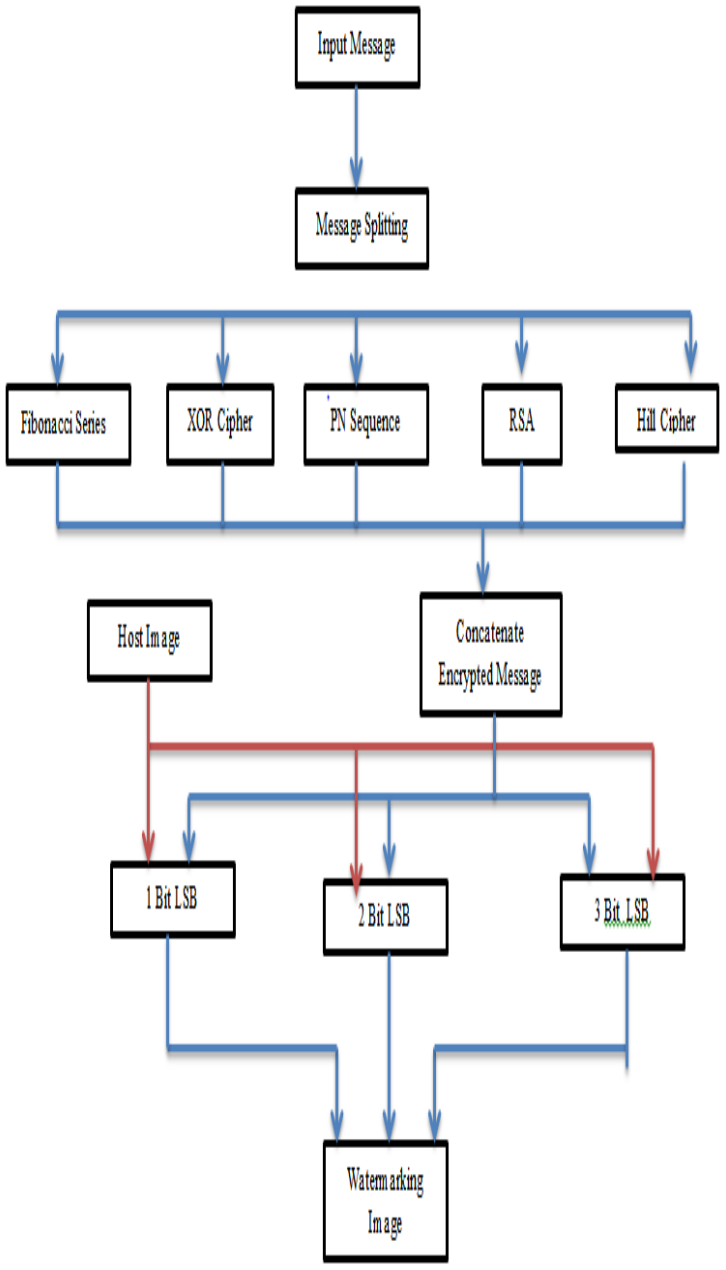

Fig. 1. Block diagram of Encryption Process

The security of the information is increased by three levels.

1. Finding the different algorithms which are implemented different segments of the message which is difficult by the intruder.
2. Encryption of the data is using key, finding the keys ar difficult by any other third party.
3. In this approach the information is hiding by LSI watermarking, recovered the message by third party i extremely difficult.

B. Hybrid Encryption based on Block Cipher and Chaos Generator

In this hybrid encryption technique combines the two video encryption techniques such as Advanced Encryption Standard (AES) and Chaos Generator. This article [8] presented the importance of maintains the security in many digital multimedia applications while storing and transferring the videos and audios. Video encryption is widely used to ensure the security of the network. Most of available encryption algorithms are suitable for text data but not well suited for multimedia data. And also video encryption algorithm, security and time efficiency are important factor in real time multimedia applications. Video encryption techniques can be classified as Naïve algorithm, Selective encryption, perceptual encryption and permutation based encryption. A cryptosystem which combine chaotic encryption technology with traditional AES encryption provides the high security for video encryption. The hybrid video encryption system is used to improve the existing algorithms and extending the advantages of individual methods to rectify the drawbacks of other methods.

In this method the encryption and decryption data path is based on three rounds implementation of the AES algorithm. The first, second and third AES round perform the four different steps of the AES algorithm namely sub bytes, shift rows, mix columns and add round key. Therefore it takes a total of eleven cycles to encrypt or decrypt the data. The input and the output interfaces units have also been integrated in order for the new hybrid cryptosystems to communicate efficiency with the external cryptosystems to take care of reading input data and writing encrypted and decrypted output.

The performance of this hybrid scheme is increased the power consumption, increase the level of security and providing a faster data encryption and decryption time. This hybrid encryption system shows extreme sensitivity on the plaintext and hence it is not vulnerable to the different attacks.

C. Text and Image Based Hybrid Encryption

This hybrid technique [9] proposed for text and image based hyper chaotic system. The main goal of developing a system for hyper chaotic encryption to improve the performance of security algorithms. This algorithm offers four methods of encryption in which two for image based techniques and two for text based encryption.

I. Text to Text Encryption

In this algorithm, the input and output both are text.

1. Add a text
2. Loop n number of times
   (i) Change the values of each character
   (ii) Change the place of each character.

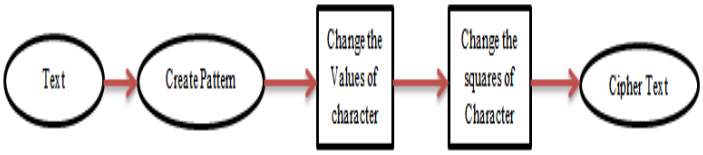

Fig.2: Text to Text Encryption

II. Text to Image Encryption

1. Add a text
2. Loop n times
   (i) Change the values of each character
   (ii) Change the places of each character
3. Create the image from text.

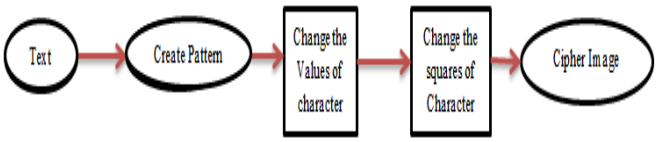

Fig. 3: Text to Image to Text Encryption

III. Image to Image Encryption

In this algorithm, first to change the RGB values of each pixel and their places then repeat that multi times before adding the pattern.

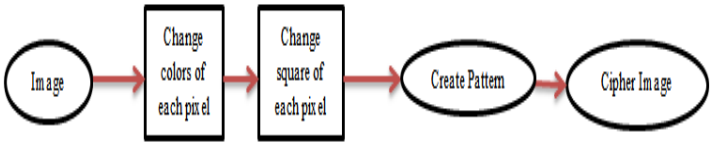

Fig. 4: Image to Image to Image Encryption

IV. Image to Text to Image Encryption

This is similar to image to image techniques but this algorithms additionally includes the process of creating the text from the image.

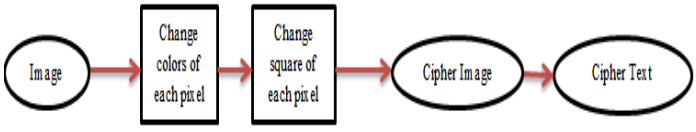

Fig. 5: Image to Text to Image Encryption

This text and image based hybrid algorithm is used to decreases computation cost, improve permutation efficiency and also difficult to analyze and gives a high performance.

D. Hybrid Cryptosystem for Secure Communication

In this paper [10] proposed a hybrid asymmetric crypto system algorithm will be implemented which combines the

methods of RSA and El-gamal. Two process are there in cryptography which is encryption and decryption. For encryption plaintext covert into cipher text by level 1 using RSA algorithm and level 2 using elgamal algorithm and final data will be store in database. Similarly for decryption the process covert cipher text into plain text level 1 using RSA algorithm and level 2 using elgamal algorithms.

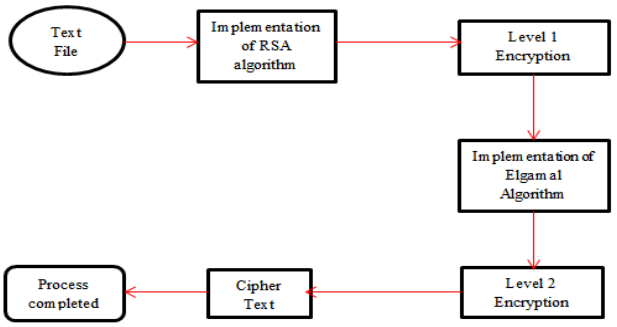

Fig.6: Process of Hybrid cryptosystem for encryption

This hybrid cryptosystem, the RSA algorithm is based on Integer Factorization Problem (IFP). It uses three different prime numbers to generate the related pair of keys faster. The Elgamal cryptosystem is based on Discrete Logarithm problem. This is used for improve the strength of these algorithm and provide the higher level of security.

An RSA and Elgamal hybrid techniques are used for implementing the text data of various sizes. This hybrid techniques increases the efficiency of computation and increased the throughput. It is decreases the time duration of both encryption and decryption process.

IV. CONCLUSION

In a fast growing technological world the today's scenario is smart homes, smart city, smart grid, smart water networks, that connects the world more than we ever thought possible. Security is an essential consideration for communication and networking world. In this survey, we described the various hybrid cryptosystem and its working procedure. Each hybrid encryption and decryption techniques has its own advantages in terms of efficiency, computation time and cost. Compared with traditional encryption techniques, the hybrid cryptosystems improves the security level, increase the speed of encryption, decryption process. The combination or multiple encryption techniques will improve the performance and extending the advantages of existing algorithm through combined with other algorithm. This combined encryption techniques rectify the drawbacks of individual encryption methods. No doubt the time density and complexity of the system is increased due to an involvement of different types of encryption and decryption techniques. The future work will focus on the designing an algorithm for providing higher security level to maintain the secured communication network with low computation cost, improve performance and reduce the complexity of algorithm implementation.

REFERENCES

[1] William Stallings, "*Cryptography and Network Security Principles and Practice*, 5th Edition, Pearson Education.

[2] Ramesh Yegireddi, R Kiran Kumar, "*A Survey on Conventional Encryption Algorithms of Cryptography*", International Conference on ICT in Business Industry & Government, 2016.

[3] Saravanan Chandran, Koushik Bharracharyya, "Performance analysis of LSB, DCT and DWT for Digital Watermarking Application using Steganography," *International Conference on Electricals, Electronics, Signals, Communication and Optimization,*. 2015.

[4] Gaurav R. Patel, Krunal Panchal, "Hybrid Encryption Algorithm", *International Journal of Engineering Development and Research*, vol. 2, Issue 2, 2014.

[5] Sushant Susarla, Gautam Borkar, "Hybrid Encryption System" *International Journal of Computer Science and Information Technologies,*, vol. 5(6), pp. 7563-7566, 2014

[6] Neha, Mandeep Kaur, "Enhanced Security using Hybrid Encryption Algoriths", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, Issue 7, pp. 13001-13007, 2016.

[7] Amandeep Kaur, Rajbir Kaur, "A Hybrid Scheme for Cryptography and Watermarking," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5 Issue 7, pp. 183-188, July. 2016.

[8] S.Kotel, F. Sbiaa, M. Zeghid, M.Machhout, A. Baganne, R. Tourki, "Efficient Hybrid Encryption System Based on Block Cipher and Chaos Generator" *IEEE International Conference on Computer and Information Technology*, pp. 375-382, 2016.

[9] Seddik Hassene, Maalaoui Najm Eddine, "A neew hybrid encryption technique permuting text and image based on hyperchaotic system", *2nd International* Conference on Advanced Technologies for Signal and Image Processing, Tunisia, pp. 63-68, March. 2016.

[10] Ruchita Patil, Veena Kulkarni, " Hybrid Cryptosystem Approach for Secure Communication", *IOSR Journal of Computer Engineering, pp. 21-24, 2017.*