NEW CRYPTOGRAPHIC TECHNIQUE FOR ENHANCING SECURITY

Aamir Mohammed Suhail[1], Anuraag Vyas[2], Meghana Gudivada[3], Prof.T.Venkat Narayana Rao[4]

Abstract— As we are aware in today's world, we rely heavily on the internet for almost every activity we perform. Using the internet we perform many tasks such as - banking, shopping, ticket booking, etc. The Internet is the primary medium for communication which is used by number of users all over the world. Simultaneously, its commercial nature is causing increased vulnerability and enhancing cybercrimes. The data which we use should be secured from hackers. Data security is currently the pressing issue that touches areas like computing and communication. In this paper, we present a new cryptographic technique which can be used for providing high security by encrypting data while communicating across the network.

Index Terms— Algorithm ,Cryptography, ciphertext,Decryption ,Encryption,Plaintext ,Public-key,Private-key.

1 INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form so that only those concerned can read and process it. The term is most often associated with scrambling plaintext into cipher text then back again through encryption. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data [7]

Cryptography is a word with Greek origins, means "secret writing." However it is the science and art to transform the messages to make them secure and immune against security attacks. It is the technique to provide secure communication in presence of adversaries to maintain information securities such as data confidentiality, data integrity, authentication and non-repudiation. The process to convert ordinary information or the plain text into unintelligible text or the cipher-text in cryptography is called encryption. The cipher-text is understandable only to someone who knows how to decrypt it. The message or information is encrypted using an encryption
algorithm. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm which usually requires a secret decryption key. Encryption schemes are divided into two groups:

1.1 Symmetric-key Algorithm

In this scheme the same key is used for encryption and decryption. It is also known as the secret key-encryption. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.

SYMMETRIC ENCRYPTION PRINCIPLES:

PLAIN TEXT : original message or data that is fed into algorithm as input.[1]

SECRET KEY : the exact substitutions and transformations performed by the algorithm depend on the key.

CIPHERTEXT: scrambled message produced as output.

1.2 Asymmetric key Algorithm

In this scheme different keys are used for encryption and decryption. It is also known as the public-key. Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives public and private key pair from a certificate authority. Any other user desiring to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message and send it to the recipient. When the recipient receives the message, he/she decrypts it with a private key, to which no one else should have access.

ASSYMMETRIC ENCRYPTION PRINCIPLES:

PLAIN TEXT : original message or data that is fed into algorithm as input.[1]

PUBLIC KEY: The key that is used to encrypt the plain text by sender of the plain text .

PRIVATE KEY: The key that is used to decrypt the plain text by the receiver of the cipher text .

CIPHERTEXT: scrambled message produced as output from the algorithm.

2. WHY CRYPTOGRAPHY?

Attacking people is more dangerous and expensive so hackers choose a less expensive way to do this and that is by using their personal information, they steal their information which is shared across the network on the internet.

By using cryptography people can send their messages without any fear of deceit or cheat. Cryptography allows us to create secure websites. Cryptography allows people to do business electronically without worries of deceit and deception. As millions of people use e-mails, etc on a daily basis, the security of information has become a big concern and thereby leads to the increased reliability on cryptography. In today's world, e-commerce has become a trend and is increasing rapidly on a daily basis as billions of dollars are transacted every year and this level of activity should be accompanied by good cryptographic security. Cryptography is also used in access to cable TV and satellite. In TV set up, it is used in a way where people can only watch the channels for which they paid for. Without cryptography the intruders or the hackers can easily tap our phone calls or e-mails or televisions and can break into our bank accounts. There are many conventional cryptographic algorithms which are used for encryption and decryption. In this paper, the algorithm we proposed will provide high security and because of its pattern it will be difficult for the intruder to crack the cipher-text.

3.CONVENTIONAL CRYPTOGRAPHIC TECHNIQUES

Dahua Xie and Jay Kuo have proposed an encryption technique with enhanced Multiple Huffman Table (MHT) by key hopping method. The previously developed Multiple Huffman Table (MHT) has good desirable properties but it was highly vulnerable to the chosen plaintext attack (CPA). Whereas this enhanced MHT encryption method faces all such limitations. As the result have shown, that the algorithm is secure for the chosen plaintext attack and proved mathematically by the key hopping method.[8]

- *Aamir Mohammed Suhail is currently pursuing Bachelors degree program in computer science engineering in SNIST, INDIA, PH-8121579505. E-mail: aamirsuhail01@yahoo.com*
- *Co-Author name is currently pursuing masters degree program in electric power engineering in University, Country, PH-01123456789. E-mail: author_name@mail.com*
(*This information is optional; change it according to your need.)*

3.1 PERMUTATION BASED IMAGE ENCRYPTION TECHNIQUE:[2]

Seshapallaviindrakanti and P.S. Avadhani proposes a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provides confidentiality to color images with less computations Permutation process is much quicker and more effective. The key generation process is unique and is a different process.

3.2 Image Encryption Based on the General Approach for Multiple Chaotic Systems, 2011:[3]

Qais H. Alsafasfeh and Aouda A. Arfoa proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed. Image Encryption Using Differential Evolution.

3.3 Modified AES Based Algorithm for Image encryption, 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki[4] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance.

3.4 A Novel Image Encryption Algorithm Based on Hash Function, 2010

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [5] proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.

3.5 A Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, 2010

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab[6] introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. In the proposed image encryption scheme, an external secret key of 104 bit and two chaotic logistic maps are employed to confuse the relationship between the cipher image and the plain image. Further, to make the cipher more robust against any attack, the secret key is modified after encrypting of each pixel of the plain image. The robustness of the proposed system is further reinforced by a feedback mechanism, which makes the encryption of each plain pixel depends on the key, the value of the previous cipher pixel and the output of the logistic map (data dependent property).

3.6 Image Encryption Using Differential Evolution Approach In Frequency Domain, 2011

Ibrahim S I Abuhaiba and Maaly A S Hassan present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. They havecarried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security ofthe new image encryption procedure.

3.7 A New Digital Image Scrambling Method Based on Fibonacci number[5].

Jiancheng Zou , Rabab K. Ward , Dongxu Qi presented a method for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in realtime situations. The scrambling effect is very sensible, the data of the image is re- distributed randomly across the whole image. The method can endure common image attacks, such as compression, noise and loss of data packet .They developed a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

3.8 Lossless Image Compression and Encryption Using SCAN. [5]

S.S. Maniccam and N.G. Bourbakis have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

3.9 New Encryption Algorithm for Image Cryptosystems.[5]

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

4. PROPOSED ALGORITHM:

The algorithm which we proposed gives a different encrypting technique which can be used to encrypt data while communicating across networks.

The sender and receiver across the network must know the pattern which is used in this algorithm. By using this pattern the sender encrypts and sends the data, whereas receiver receives the data and he decrypts it using the same pattern. At this stage, the pattern should be confidential. We have a different pattern for alphabet and digits.

4.1STEPS TO BE FOLLOWED:

The alphabets from A to Z, a to z, digits 0-9 are encrypted and sent across the network.

The encoded data can be sent through:

- Conversion to ASCII Form and sent.
- Conversion into binary form.

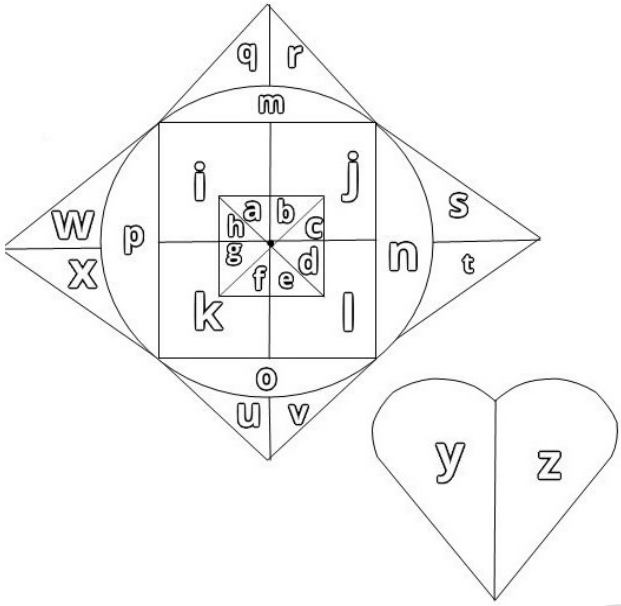
By following any of the above mentioned steps conversion of the data can be done.

The representation of the alphabet is based on the pattern given below but it is different for every character .The alphabets inside the pattern can be placed at different position and used. The pattern shown below is one of the possible way. The characters we used are different these characters are specially designed for special purpose of cryptographic technique.

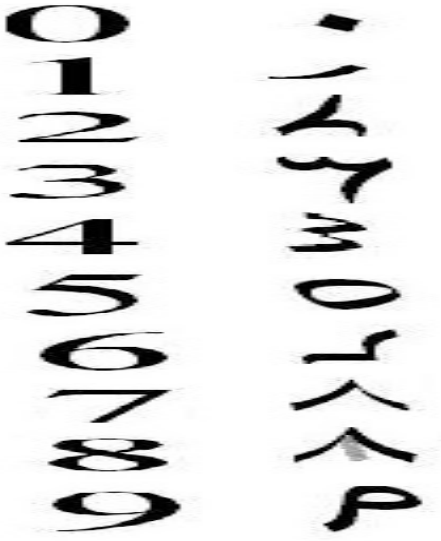
In order to differentiate between the lowercase and uppercase alphabets we used an asterisk (*) over the symbol of uppercase alphabets.

In the cryptography techniques it is very important that the message or data which is to be sent is should be safe from the third party in the communication.

4.2 PATTERN FOR ALPHABET:



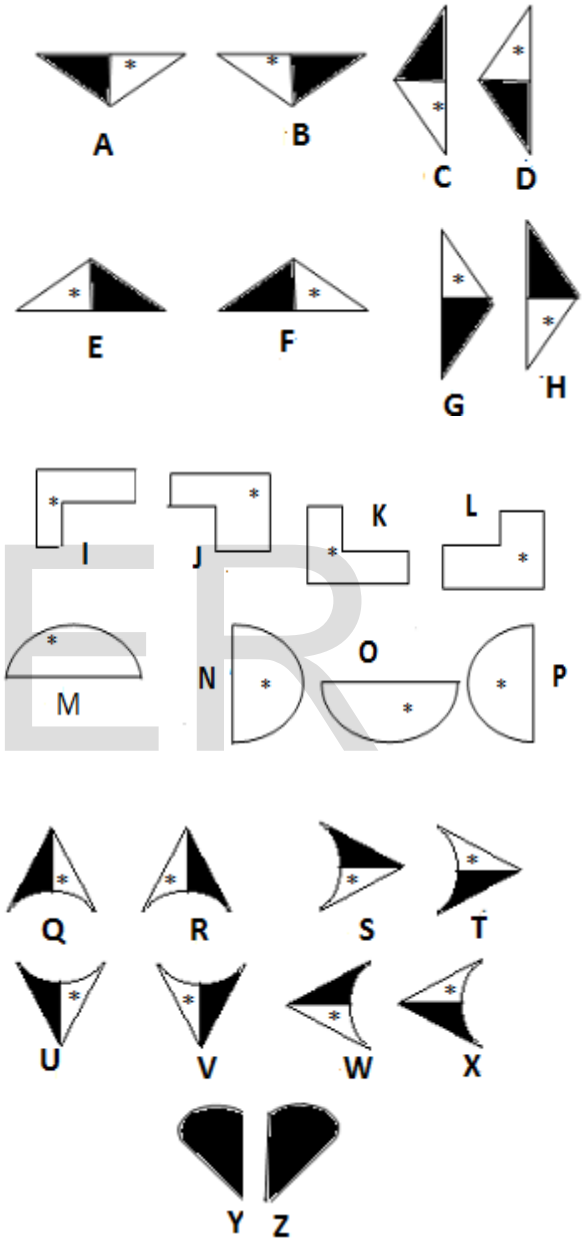
4.3 PATTERN FOR DIGITS:



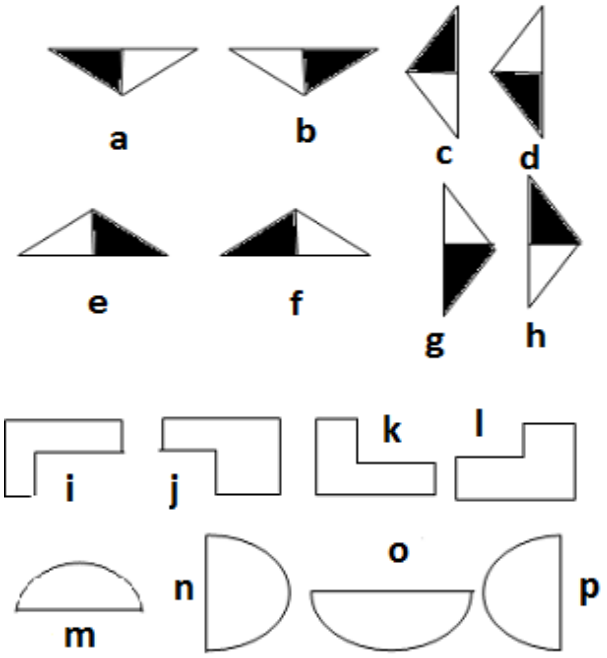
The patterns for Alphabet and digits involving in the encryption algorithm are shown above. The major advantage of the representation is that the cipher-text is very difficult to crack, since the encoding schemes we used here are very secure when compared to some of the existing algorithms.

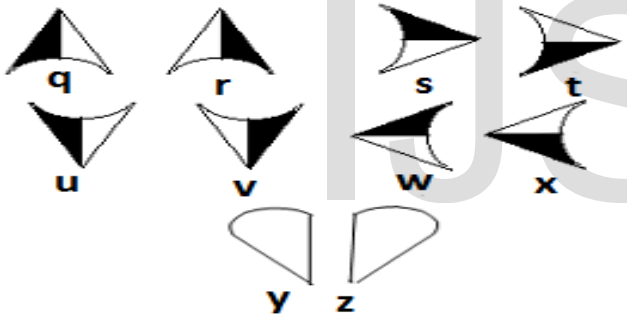
Based on the above patterns, we represent each alphabet and digit as below:

4.4 PATTERN FOR INDIVIDUAL UPPER CASE LETTERS:



4.5 PATTERN FOR INDIVIDUAL LOWERCASE LETTERS:





Let us exemplify:

Consider the sentence:

"My Age Is 19."

The above sentence is encrypted as :

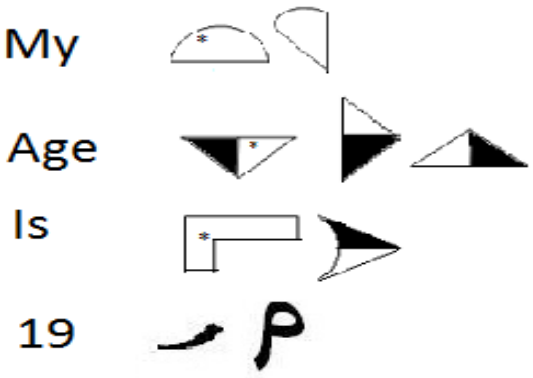
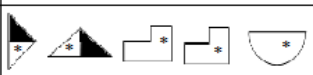
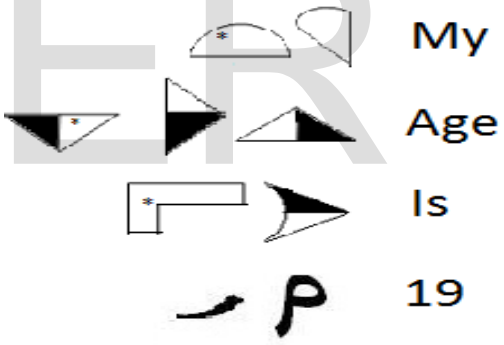


TABLE 1
DETAIL ANALYSIS

PLAIN TEXT	ENCRYPTED TEXT	DECRYPTED TEXT
HELLO		HELLO
May 26		May 26
Good		Good
028147		028147
Street 5		Street 5

At the receiver side the decryption is done as follows:



Thus both sender and receiver can communicate.

5. ADVANTAGES:

There are many encoding schemes for cryptography. but we require a new encoding scheme such that, though the hacker gets a hint, it should be difficult for him to crack.

It is easy to implement the encryption as we have followed a particular pattern.

All symbols are different from each other, so it will be difficult for the intruder to crack.

6. DISADVANTAGES:

As we know, most of the algorithms have their own disadvantages similarly there is a disadvantage for the above algorithm that is, Encryption of symbols is not possible with this algorithm.

7. RESULTS:

The above mentioned algorithm can be very useful in the area of cryptography. The encryption algorithm is designed in keeping in view of the need for strong encryption scheme seeing the attained to the network where the data is hacked on regular basis.

8. CONCLUSION:

In the cause of development of this cryptography encryption scheme we have tried to develop a very strong secure scheme that will definitely be very difficult to break by crackers or by hackers to decrypt the information.

9. REFERENCES:

[1] William Stallings "Network Security Essentials ,Applications and Standards" . Chapter 2.1,page num.28.

[2] Priyanka Gupta, Anupam "Cryptographic Security by New Character Signs",IJCTA,Vol5(6),1868-1872,ISSN:2229-6093.

[3] Komal D Patel, SonalBelani, "Image Encryption Using Different techniques: A Review", International Journal of Emerging
Technology and Advanced Engineering(IJETAE), Volume 1, Issue 1, November 2011.

[4] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007

[5] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, ―A Novel Image Encryption Algorithm Based on Hash Function‖ 6th Iranian Conference on Machine Vision and Image Processing, 2010

[6] Ismail Amr Ismail, Mohammed Amin, Hossam Diab ―A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps‖, International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[7]Freeman J., Neely R., and Megalo L. "Developing Secure Systems: Issues and Solutions". IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998

[8]Dahua Xie and C.-C. Jay Kuo, "Enhanced multiple Huffman table (mht) encryption scheme using key hopping" IEEE Transactions,pp.568-571,2004

AAMIR MOHAMMED SUHAIL,studying ,computer science & engineering in SREENIDHI INSTITUTE OF SCIENCE & TECHNOLOGY.His major interests are BIGDATA ANALYTICS and NETWORK SECURITY.He did couple of projects in PIG and HIVE.His interest in NETWORK SECURITY made him to write this journal.

Anuraag vyas is a B.tech student , Sreenidhi Institute of Science and Technology, Computer Science and Engineering.He had done few projects in Android, Web Designing. His research interest includes network security, android ,web designing, Big data or Hadoop . He can be reached at **anuraagvyas323@gmail.com.**

G.Meghana is B.tech student graduating at Sreenidhi Institute of Science and Technology, Computer Science and Engineering.She had done websites using PHP mysql. Her field of interests are network security, android ,web designing. Her interest towards network security urged her to write this paper.