International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Data Security Using Private Key Encryption System Based On Compression

Anjali Jivtode; Pratiksha Wankhede &Dnyaneshwar Nagrikar
Department Of Computer Technology, Mata Mahakali Polytechnic,Warora

Abstract
Problem confronted by today's communicators is security as well as the pace of correspondence and size of the substance. In the present paper, a plan has been proposed which utilizes the idea of pressure and information encryption. On the first stage the center has been made on information pressure and cryptography. In the following stage we have underscored on pressure cryptosystem. At long last, proposed procedure has been examined which utilized the idea of information pressure and encryption. In this first information is compacted to diminish the measure of the information and expand the information transfer rate. Thereafter compress data is encrypted to give security. Consequently, our proposed system is powerful that can decrease information size, build information exchange rate and give the security amid correspondence.
Keywords—Arithmetic coding; cryptography; skimming point number; one time cushion; compression crypto.

1. INTRODUCTION

The present system situation requests trade of information with more security and diminishment in both the space prerequisite for information stockpiling and the time for data transmission. This can be proficient by pressure and encryption, such sort of framework is called pressure –crypto framework. Encryption is in fact a safe coding method and information pressure is likewise a coding strategy, whose reason for existing is to diminish both the space necessities for information stockpiling and the ideal opportunity for information transmission[1]. In proposed framework i.e information security utilizing private key encryption framework encoded string is created by a model from a data series of images and in light of math coding that can be utilized to accomplish the present system situation for trade of data with more security and compression[2].

Information pressure offers a using so as to allure methodology for diminishing correspondence costs accessible transfer speed viably. Pressure calculations lessen the repetition in information representation to diminish the capacity required for that information. Over the a decade ago there has been an extraordinary blast in the measure of advanced information transmitted by means of the Internet, speaking to content, pictures, video, sound, PC programs, and so on [3] In the more present day model based paradigm for coding, where, from an data series of images and a model, an encoded string is delivered that is a compacted adaptation of the info. The decoder, which should have entry to the same model, recovers the definite data string from the encoded string.

2. RELATED WORK

In the 21st century the significance of data and correspondence frameworks for society and the worldwide economy is escalating with the expanding worth and amount of information that is transmitted and put away on those frameworks. In the meantime those frameworks and information are likewise progressively helpless against an assortment of threats, for example, unapproved get to and use,

misappropriation, change, and annihilation. Inside of the connection of any application to application correspondence, there are some particular security prerequisites including:-

1.Authentication: - The procedure of giving one's character.

2.Confidentiality:-Ensuring that no one can read the message aside from the expected recipient.

3.Integrity:-Assuring the beneficiary that the got message has not been adjusted at all from the first.

4.Non-repudiation:-A instrument to demonstrate that the sender truly send this message. There are two sorts of cryptographic plans: symmetric (private key) cryptography, and deviated cryptography, each of which portrayed below[10].

Symmetric Key Cryptography [12] In symmetric key cryptography (otherwise called private-key cryptography), a mystery key might be held by one individual or exchanged between the sender and the receiver of a message. If private key cryptography is utilized to send mystery messages between two gatherings, both the sender and receiver must have a duplicate of the mystery key. Be that as it may, the key might be bargained amid travel. One strategy is to send it by means of another secure channel.

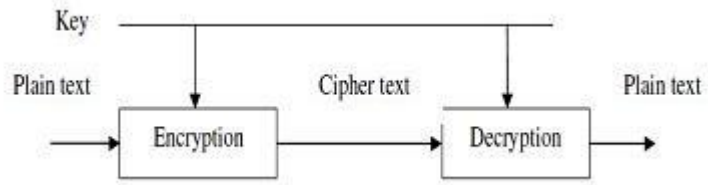

Figure 1. Symmetric Encryption.

2.1.1Stream figures [10];-Stream figures scramble plaintext one byte or one piece at once. Illustrations of Stream figures are RC4 figure and the one-time cushion.

2.1.2 Block figures [10]:-Block figures scramble plaintext in pieces. Regular piece sizes are 64 and 128 bits. Samples of Block figures are DES and the AES.

2.2 Asymmetric Key Cryptography [11]:-In the two-key framework, (otherwise called the general population key framework) one key scrambles the data and another, numerically related key decodes it. The PC sending a scrambled message utilizes a picked private key that is never shared as is known just to the sender. In the event that a sending PC first scrambles the message with the proposed collector's open key and again with the sender's mystery, private key, then the accepting PC might decode the message, first utilizing its mystery key and after that the sender's open key. Utilizing this public-key. Cryptographic strategy, the sender and beneficiary can confirm each other and ensure the mystery of message.

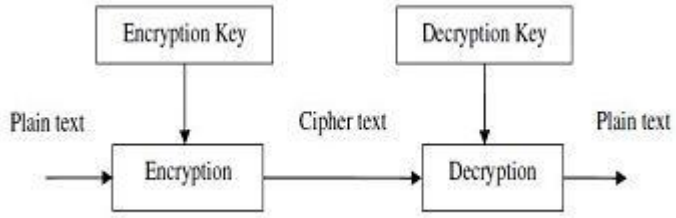

Figure 2. Asymmetric Cryptosystem.

3. DATA COMPRESSION:- Data pressure offers a using so as to allure methodology for decreasing correspondence costs accessible transfer speed viably. Pressure calculations diminish the repetition in information representation to diminish the capacity required for that information. Over the a decade ago, there has been an uncommon blast in the sum of digital information transmitted through the Internet, speaking to, content, pictures, video, sound, PC programs, and so on [3] Compression is accomplished by transmitting the more likely images in fewer bits than the less plausible ones. Number juggling coding can be seen as a speculation of Huffman coding.

3.1 Arithmetic Coding:-Today, for data pressure there exist numerous strategies. The most popular one is Arithmetic Encoding. This encoding method has been created broadly for its presentation a very long while prior and is prominent for offering to a great degree high coding effectiveness. Number juggling coding, imagined by Jorma Rissane and transformed into a handy technique by Witten, Neal and Cleary, accomplishes better Compression than the better known Huffman calculation. [1] In reality, number-crunching coding is a system to guarantee lossless information pressure. It is undoubtedly a form of variable length entropy encoding. On account of other entropy encoding systems, the info message is isolated into its segment images and every image is supplanted by a code word. Be that as it may, number-crunching coding encodes the whole message into a solitary number, a portion n where (0.0_n< 1.0) [2]. The coding calculation is image savvy recursive; i.e., it works upon and encodes (decodes) one information image per iteration or recursion. On every recursion, the calculation progressively segments an interim of the number line between 0 and 1, and holds one of the segments as the new interim. In this way, the calculation progressively manages littler interims, and the code string, saw as an extent, lies in each of the settled interims.

4. COMPRESSIONCRYPTO SYSTEM: The answer for both the thickness and the security issues has been to just utilize software based pressure procedures to decrease the number of tapes expanding capacity thickness and encryption to secure the information on the tapes. The pressure cryptosystem can be comprehended with the assistance of figure [8].

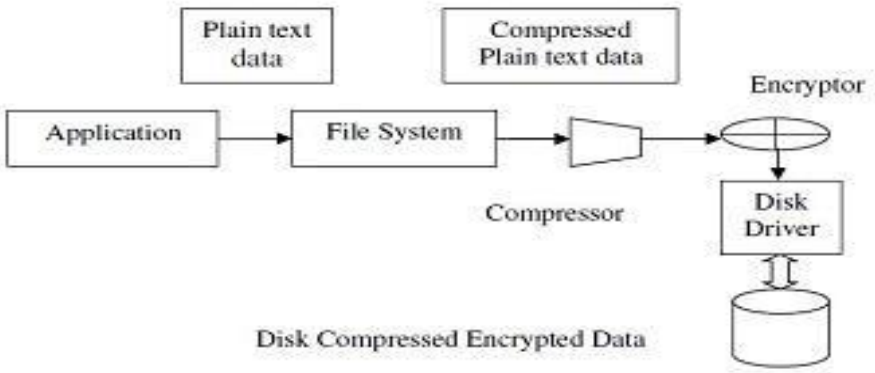

Figure 3: Compression and Encryption processing flow

Figure 3. Compression and Encryption processing flow.

3. EXISTING SYSTEMS

One of the current framework utilized pressure alongside encryption utilizing RSA calculation. This framework is essentially utilized for mobile correspondence. This framework gives an answer for this SMS security issue. The methodology that is utilized as a part of this framework is to secure the SMS message utilizing Hybrid Compression Encryption (HCE)system. This framework packs the SMS to diminish its length, then encodes it utilizing RSA calculation [7]. Yet, this framework is utilizing RSA. RSA is a Public Key Encryption technique. A weakness of utilizing public-key cryptography for encryption is velocity.

4. PROPOSED COMPRESSIONCRYPTO SYSTEM

The proposed system depends on the idea of number-crunching coding in which an expression of content is changed over into drifting point number that lie in reach somewhere around 0 and 1. This skimming point number is changed over into paired number and after that one time key is utilized to encode this double number. At last after encryption, result is again a double number; this number is changed over into decimal number again and sends to the recipient.

6.1Requirements:-

6.1.1 Table

A table contains images alongside the rate of probability of occurrence. By necessities of the user the table is outlined that might contain lower case letters in order, capitalized letter sets and images like %, @ and so on.

6.1.2 One Time Pad:-

It's an one-time key gave by client to securing the substance. This is an arbitrary key that is the length of the message. What's more the way to be utilized to scramble and unscramble a solitary message, and afterward tossed. Each new message requires another key of the same length as another message.

6.2Implementation:-

This system changes over an expression of content into using so as to coast point number-crunching coding. The outcome is packed information. Gotten gliding point number is scrambled utilizing private key encryption procedure, i.e. one time cushion key. The yield is secure and compacted information.

6.3Explanation

6.3.1 Compression and Encryption

Firstly include an image is packed utilizing math coding after that a private key is utilized to scramble the aftereffect of number-crunching coding.

Algorithm
To pack and encode the message Algorithm incorporates taking after steps:-

Step1:-using table encodes the info image.

a) Initialize lower_ bound=0, upper_ bound=1

b) While there are still images to encode Current _range = upper _bound – lower _bound Upper_ bound = lower _bound + (current _range * upper _bound of the new image) Lower_ bound = lower_ bound + (current _range * upper_ bound of the new image)
End while
Step2:-The string might be encoded by any quality inside of the likelihood range and after that change over the yield decimal number into paired arrangement.

Step3:- limit the quantity of bits by utilizing the formula:- No_ of_ bits=log _2/upper_ bound_ last encoded image - lower_ bound_ last encoded image

Step 4:-No _of _bits is utilized to lessen the quantity of bits got in step2.

Step 5:- Select any one time cushion and Xor it with consequence of step4.

Step 6:- Rotate 2 bits right.

Step 7:- Convert the aftereffect of step 6 into decimal arrangement once more.

Output: -output is coasting point, no that is related to the inputted image.

6.3.2 Decompression and Decryption

Getting the coasting point, it's chance now that we change over it into unique content.

Algorithm:-

Step1:-Convert the got information into parallel organization.

Step 2:- Rotate 2 bits to left.

Step3:- Selected one time cushion is Xored with the aftereffect of step2.

Step 4:- Convert the outcome once more into decimal structure.

Step 5:-Encoded_ value=Encoded info While string is not completely decoded Identify the image containing encoded esteem inside of its reach

current_ range = upper _bound of new image – lower _bound of new image

encoded esteem = (encoded _value - lower_ bound of new image) ÷ current_ range

End while
Output: The output is the original symbol.

6.3.4Example
Table1: symbols along with probability of occurrence.

Symbol	Probability	Range(lower_ bound, upper_ bound)
a	30%	[0.00,0.30)
b	15%	[0.30,0.45)
c	25%	[0.45,0.70)
d	10%	[0.70,0.80)
e	20%	[0.80,1.00)

Compression and encryption Data to be encoded and encrypted is "abd"
Step1:- Encode 'a'
current_ range = 1 - 0 = 1

upper bound = 0 + (1 × 0.3) =0.3
lower bound = 0 + (1 × 0.0) =0.0
Encode 'b'

current range = 0.3 - 0.0 = 0.3

upper bound = 0.0 + (0.3 × 0.45) =0.135
lower bound = 0.0 + (0.3 × 0.3) = 0.09
Encode 'd'

current range = 0.135-0.09 = 0.045

upper bound = 0.09 + (0.045 × 0.8)=0.126
lower bound = 0.09 + (0.045×0.7)=0.1215

Step2:-

The string "abd" may be encoded by any value within the range [0.126, 0.1215).
Now output is 0.12375 and its binary equivalent=.000111111010111000010101

Step3:-
No_ of_ bits= log_2/0.0045 = log444.44=8bits

Step4:-
So after reducing number of bits binary value is 0.00011111.

Step5:-
Our One time pad is – 11010100 Data- 00011111 from

Step 4. After Xoring the output is 11001011.

Step6:-
Rotate 2 bits right the result is 11110010

Step7:-.11110010 in decimal is 0.9453125.

Decompression and Decryption
Step 1:- Received data is 0.9453125 & binary format of received data is .11110010

Step2:- Apply 2 left shifts to result of step1 the result is 11001011

Step3:- Apply selected one time pad and Xored it with the result of step2 the result is 00011111

Step4:-Convert .00011111 into decimal i.e. 0.1210

Step5:- Using the probability ranges from table decodes the three character string encoded as 0.1210. Decode first symbol 0.1210 is within [0.00, 0.30) 0.1210 encodes 'a' Remove effects of 'a' from encode value
Current _range = 0.30 - 0.00 = 0.30 Encoded _value = (0.1210 - 0.0) ÷ 0.30 = 0.4033

Decode second symbol

0.4033 is within [0.30, 0.45) 0.4033 encodes 'b' Remove effects of 'b' from encode value
current range = 0.45 - 0.30 = 0.15
encoded value = (0.4033 - 0.30) ÷ 0.15 = 0.6886
Decode third symbol 0.6886 is within [0.70, 0.80) 0.6886 encodes 'd'.

7. KEY FEATURES

The proposed system having the accompanying key components:

•It is a Private Key Encryption Technique

•Used both information Compression and Cryptography idea.

•Use Less Bandwidth of Secure Channel

• Highly secure

•Cipher content produced for same data constantly diverse because of one- time cushion amid encryption.

•In proposed framework created figure content takes less data transfer capacity of secure channel.

•Provides exactness control to change over whole string or document.

8. CONCLUSION

The proposed system gives a phenomenal reconciliation of information pressure with the cryptography to builds the information security and exchange rate amid information correspondence. In this procedure we can diminish the span of information utilizing the math encoding information pressure system and after that packed information can be scrambled to give the security. The Present system situation requests trade of data with decrease in both space prerequisite for information stockpiling and time for information transmission alongside security. Our proposed strategy satisfies every such prerequisite as this system utilize the concept of data compression and encryption.

REFERENCES

[1] V.Kavitha & K.S Easwarakumar, (2008)

"Enhancing Privacy in Arithmetic Coding" ICGSTAIML journal, Volume 8, Issue I.

[2] J.A Storer, (1988) "Data Compression: Methods and Theory" Computer Science Press..

[3] Dr. V.K. Govindan & B.S. Shajee mohan "An intelligent text data encryption and compression for high speed and secure data transmission over internet".

[4] I.H. Willen, Randford M.Neala & John G.Cleary,(1988) , "Arithmetic Coding for

[5] Data Compression", Communications of the ACM Volume 30 Issue 6.

[6] SHANNON C. E, (1948). "A Mathematical Theory of Communication". The Bell SystemTechnical Journal, Vol. 27, pp. 379–423, 623–656.

[7] Jayant Rajurkar, T.Khan, "A System for Query Processing and Optimization in SQL for Set Predicates using Compressed Bitmap Index", IJSRD - International Journal for Scientific Research &Development| Vol. 3, Issue 02, 2015 | ISSN (online): 2321-0613,pp no 798-801.

[8] Jayant Rajurkar, T.K.Khan," Efficient Query Processing and Optimization in SQL using Compressed Bitmap Indexing for Set Predicates", *IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)*, 623.DOI.10.1109/ISCO.2015.7282354.2015.

[9] Jagdish H.Pujar & Lohit M.Kadlaskar "A new lossless method of image compression and decompression using Huffman coding technique" Journal of Theoretical and Applied Information Technology.

[10] Mamta Sharma, (2010) "Compression Using Huffman Coding" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010.

[11] Mukunda D. Waghmare1, Kailash Patidar," An Efficient Approach to Content Based Image Retrieval" International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015.

[12] Glen G. Langdon, (1984) "An introduction to arithmetic coding", IBM Journal of Research and Development Volume 28, No.2.

[13] Amir Said, (2004) "Comparative Analysis of Arithmetic Coding Computational Complexity," Imaging Systems Laboratory HP Laboratories Palo Alto HPL-2004.

[14] Jayant Rajurkar,T.K.Khan," Review on Efficient Query processing for Set Predicates of Dynamically Formed Group", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 4, Issue 9, ISSN: 2277 128X, Page No.640-643, September 2014.

[15] Whitfield Diffie & Martin E. Hellman,(1979)"Privacy Authentication: An Introduction to Cryptography" proceedings of the IEEE, vol.67, no.3.

[16] Onwutalobi Anthony - ClaretDepartment of Computer Science University of Wollongong "Using Encryption Technique".

[17] http://www.wwpi.com