A Dual Crypt-Stegano Approach for Information Security

[1]Sanjay Kumar Pal, [2]Bimal Datta, [3] Amiya Karmakar
[1] Dept. of C&A, NSHM Knowledge Campus, Kolkata, [2] Dept. of CSE, Budge Budge Institute of Technology, Kolkata, [3] Dept. of CSE, Maulana Abul Kalam Azad University of Technology, WB
[1] sarbojay@gmail.com,[2] bkd_hetc@yahoo.co.in, [3] amiya.karmakar@gmail.com

Abstract

Data secrecy has reached a different dimension and the presence of a cipher is not enough for assuring that a particular message is safe. Further, a technique for hiding the cipher inside an image has also been implemented so that the presence of a message can be denied. This paper presents an encryption technique using multiplier method to generate cipher text. Vedic Mathematics in itself offers widespread method for encryption message that is even includes concepts of the elliptical curves, Vedic multiplier etc. [8]. The Vedic Multiplier scheme is utilized here for encoding and decoding process. It has used to encrypt plain texts later this has hidden inside an image. The objective of this research work is continuously resound for development of an identical method which will guarantee confidentiality and authenticity for the private communications between two entities. The proposed paper can be used in order to develop applications on both Cryptography and Steganography(Crypt-Stegano) using Encoded Multiplier Technique(EMT) with least time complexity.

Index Terms: Cryptography, Decryption, Decoding, Encryption, Encoding, Steganography.

I. INTRODUCTION

With the development of human civilization over the last century, the need for data secrecy has attained a new dimension by virtue of topics like cryptography, encryption, digital signatures and so on. Since the advent of encrypting devices like ENIGMA during the Second World War, the world has never looked back on its part and each specialized key has found its decrypting counterpart with time. Encryption has been at its highest peak over the past few decades as a result. The concentration from just cryptographic approach has laid forward a significant problem that indicates the presence of a message that is somehow altered on the basis of a hash key. Hence, there is a need for eliminating this problem and having a full proof system where the presence of a confidential piece of information is completely erased. Such techniques are widely used now but the presence of a cipher generated on the basis of a random number sequence on each printable character of the keyboard is what, that makes our system secured and compromising of either the image or cipher keeps the system intact as brute force required to break the system remains cumbersome. Traversal to the various section of this paper will ascertain the utilization and improvements on previous methods.

II. MOTIVATION OF WORK

There are many network security algorithms developed using the concept of cryptography where random numbers are used. Some of those examples are:

- Key conveyance and equal confirmation plans: In this plans, two communicating objects team up by trading messages to circulate keys as well as validate one another. Much of the time, nonces are utilized for handshaking to keep away from replay assaults. The use of arbitrary numbers for the nonces exasperates a rival's endeavors to decide or foresee the nonce.

- Session key creation: A secret key is creäting for the symmetric encryption and it will be use for a tiny time. This secret key is usually named a session key.
- Construction of keys for the RSA encryption. A remarkable enhancement over the actual algorithm.
- Formation of a bit stream for the symmetric key encryption.

The application provide turnaround two distinct and not essentially likeminded necessities for a sequence of the random numbers: randomness and impulsiveness [11].

The Rijndael algorithm utilized in another methodology for encryption strategy involving aggregate procedures; it takes random number for every single person. The random key is different for each message. The expressed work carries out the safe keeping level through various stages. Here, algorithm is sorted into three stages. In each stage a moderate cipher is delivered at the cycle end. The encryption algorithm is delivered two halfway ciphers at the first interaction, last cipher is come at the third cycle. The explained algorithm has long bits of hidden message in any event, for the little size input. For instance, 8-bit string input string gives least of 24-bit characters encoded data. Rijndael AES algorithm is involved to substitute each plain text into one more character by utilizing salt values. The salt values changes or stir up with the plain text characters to produces long modified characters [10].

The Percon8 algorithm for generation of random number is a well-known algorithm which was published in May 2014. The PERCON8 is named so as its uses permutation and concatenation to produce eight random numbers in each round. PERCON8 Algorithm provides advantages of 'Mid Square Random Number Generation' method and Linear Congruential Generator method while take advantage of their limits to its use. It is multi-round algorithm which is used to generates Random Numbers. The numbers of rounds are dynamic, that is they rest on the values of seed as inputs in every round until seed becomes zero. In to each round algorithm produces a sequence of eight 8-digit random numbers. This method employs Linear Congruential Generator which produces serially correlated random values. A permutation matrix has use to de-correlate the sequence, thus rendering the estimation almost impossible [11].

A secure least significant bit (LSB) method for image steganography has been proposed in a paper, "A Novel Secure Image Steganography Method Based On Chaos Theory in Spatial Domain", using the idea of non-linear dynamic system (chaos). The chaotic system is enormously sensitive to initial values and constraint of system. The explained algorithm provides added security to the basic steganography. Application of separate chaotic sequence for encryption of each part of secret image provides an additional protection from attacks. The proposed method uses host image files in spatial domain to hide the existence of sensitive information regardless its format. Performance analysis of the proposed method after comparing with 3-3-2 LSB technique is quite encouraging. The presented method is applied to a JPEG files; but it can work with other file formats. Further work includes familiarizing the free parameters of the logistic chaotic map using soft computing techniques as chaotic systems are extremely sensitive to initial conditions [15].

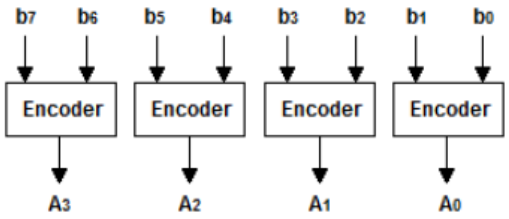

Fig. 1: Bits grouping with Encoder.

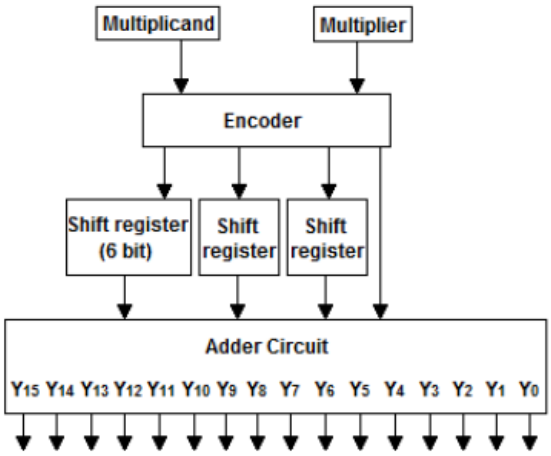

Fig. 2: Architecture of the 8-bit Encoded Multiplier.

The Multiplier utilizing encoder procedure has been explained in the paper "Ecc Encryption System Using Encoded Multiplier and Vedic Mathematics" by the scientists Bonifus PL and Dani George. The Vedic Mathematics procedure characterizes, how one can get the result of two numbers without really duplicating them by simply creating the fractional results of the parallel reciprocals of the comparing numbers and adding them subsequent to moving of bytes. The procedure may not be contrived for real multiplication but rather for repulsive device of encoding. The thought regarding the examined method has been made sense of in subtleties in a later stage.

III. TERMINOLOGY

A. Cryptography

The art of keeping messages safe using some technique in context of encrypting for generation cipher; later it will be decrypt to retrieve original information is called cryptography [6].

B. Private Key Cryptography

In private key cryptography a single secret key is share to the sender and receiver. If secret key is revealed the system is then said to be compromised. In this case the system does not inhibit the receiver from falsifying. This is likewise named the Symmetric key or private cryptography [2].

C. Public Key Cryptography

Public key cryptography encompasses of two dissimilar keys; a public key use for encryption and a private key use for decryption. The decoding is extremely impossible to compute if private key is unknown [2].

D. Cipher

The encoded form of the plain text is termed as cipher text.

E. Plain Text

The actual message which will be transfer to the recipient end is plain text. A secret key is use on with plain text to obtain cipher text.

F. Encryption

Encryption is process of transformation original message into a form which cannot understandable if do not use of applied secret key [3]. The process to create the cipher text using secret key is named encryption.

G. Decryption

Decryption is the process of retrieval of the original message from a cipher text using some function and

secret key.

H. Cryptosystem

A function and secret key are used to transform plain text to cipher and retrieval of information from cipher text to plain text in an unpredictable manner is named cryptosystem [4].

I. Steganography

It is a process of hiding confidential information within some objects like image, video etc. which is seems to be nothing [7, 16]. Steganography create confusion with cryptology because both are likewise similar method used to protect confidential piece of information. The variance between steganography and cryptology is, steganography comprises hiding confidential message so it seems that no information is hidden. Therefore, if a somebody views the object, he or she will have no hesitation that there is any hidden information.

Steganography essentially exploits human perception. The human minds are not trained to look files which contains confidential information embedded into it. Even though, there are many available software that can do, is termed Steganography. It also guarantees that even if an image is traced by an intruder, it will be unaware of the existence of a secret message inside that image.

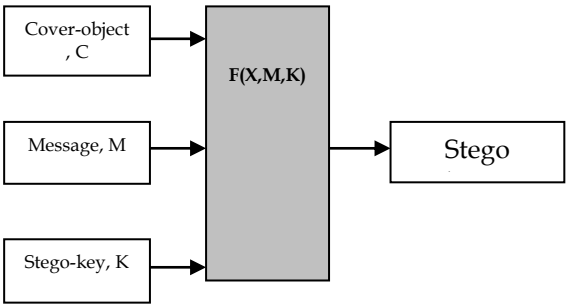

Fig. 3: Sender to receiver message flow.

IV. PRANSFER MESSAGE IN PUBLIC-KEY CRYPTOSYSTEM

Out in the public key crypto system, every member is relegated a couple of converse keys for E and D. Various capabilities are utilized for cipher and decipher of message, one of the two keys can unveiled, given that it is difficult to create one key from other. The key E can be unveiled; however, the key D is kept anonymous. The typical data transmission among shippers and recipients can be supplanted by an open registry of encipher keys containing keys E for all members.

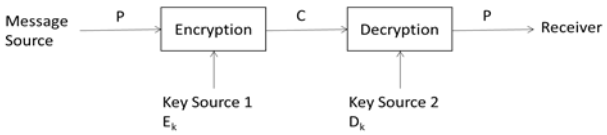

Fig. 4: Sender to receiver message transformation.

At the point when an individual A desires to make an impression to individual C, the encipher key is utilized to make the cipher. There are another individual B, who can intrude and have unapproved admittance to message. There is dependably a likelihood that the data is not any more confidential and runs the possibilities being messed with. Since encipher key is accessible, B can attempt to encipher a message and direct to C, rather first cipher that was actually directed by the source. Notwithstanding, just the decipher key of C, can decipher the first message and any sort of altered insignificant data can be disregarded due to something similar. Indeed, even digital signatures track down a way of security in setting of Public key systems. The accompanying articulations shows use of public key systems to carry out digital signatures.

In this case individual A, signs message m by computing,

$$C = D_A(m) \quad (1)$$

Individual B then validates A's signature by checking,

$$E_A(C) = m \quad (2)$$

Disputes can rule on by checking whether, $E_A(C)$ restores message m, in the same way as individual B.

$$D_K(E_K(m)) = E_K(D_K(m)) = m \quad (3)$$

The confidentiality and legitimacy in public key system has been a worry for the current cryptographic and above notes for the essential idea taken cover behind the upkeep of the equivalent while fostering a public key cryptography [5].

V. CRYPTOGRAPHY Vs STEGANOGRAPHY

The motivation behind cryptography and steganography is to give secret organization correspondence over open channel. In any case, steganography isn't precisely identical as cryptography. Cryptography conceals the items in a classified message from malignant individuals, while steganography covers the presence of the message. The cryptography system is uncovered when the assailant can peruse the classified message. While breaking a steganography system need the aggressor to recognize steganography that has been utilized.

It is feasible to consolidate both the strategies by scrambling message utilizing cryptography and afterward concealing the encoded message utilizing steganography. The subsequent stego-picture can be sent over open channel without uncovering that restricted intel is being traded.

VI. MODERN METHOD

A. Multiplier Using Encoding

Although considering a most recent encoding procedure in light of multiplier utilizing an encoded algorithm, we have accomplished an imperative approach to concealing text through making partial product [14]. The size of partial product made in this strategy are half draw a distinction with the Vedic and traditional techniques. In the 8-bit multiplier, the quantity of partial product required is four. We get the last cipher by thinking about two characters all at once and by taking into account the way that the UNICODE values should be increased and thus we get four partial products. The halfway items are produced in light of the UNICODE worth of the subsequent string and determined concerning consecutive 2-bit from the last part of the 8-bit. We make cipher text through the four partial products in a random way alongside the main person's UNICODE worth and proceed with this cycle until every characters of plain text are changed to the ideal result. The cipher obtained is then ship off the recipient. While deciphering, every fractional item is then coordinated in the right grouping. The second, third and fourth positioned partial product, halfway item are modified a bit in the accompanying way: The decimal equivalent of,

i. second placed is multiplied by four.
ii. third placed is multiplied by sixteen.
iii. fourth placed is multiplied by sixty-four.

The determined qualities are then accumulated alongside what could be compared to the primary put partial product and afterward it is partitioned by the principal character's UNICODE esteem which was likewise present in cipher text. The result obtained is second person's UNICODE esteem. The pattern of this decoding occasion go on until the whole cipher message is broken and afterward the got values are organized and addressed as characters hence delivering the first message [1].

B. Encoding Algorithm

i. If, $A_i = 0$, then $P_i = 0$.

ii. If, A_i =1, then P_i is the multiplicand.
iii. If, A_i =2, then P_i is obtained shifting the multiplicand value one bit left.
iv. If, A_i =3, then P_i is summation of partial products of A_i, for, i = 1, 2.

C. Encoding Steps

i. Multiplier group into 2-bit each and it is start from the Least Significant Bit.
ii. From encoder table Find out value of A_i.
iii. Based on A_i, find out P_i.
iv. The values of the P_i are assigned thereafter to the adder circuit; shifting of one bit, two bit, four bit, six bit one after the other.
v. The final P_i is outcomes of adder circuit.

The steps 4 and 5, referenced in the encoding algorithm are utilized for decryption of cipher text. This procedure was executed for creation ciphers and afterward decipher through sending the P_i as cipher and decipher done through utilizing the adder circuit to recover a value. Then, at that point, assess the P_i to get two characters all at once. The carried out method is running great whose screen capture displayed in figure-5, and execution time of Encryption and Decryption process is given in Table-1.

VII. PRESENTED TECHNIQUE

The proposed experiment considers a random number hypothesis for each message and later includes a LSB strategy for steganography. We have painstakingly supplanted the utilization of the UNICODE grouping with controlled use of random reciprocals for each character comparing to every individual string. The explained system can play an enormous part to play in official organization correspondences where certain messages should be made profoundly classified and shared secretly. Regardless of whether the string is known to few intruders then the recovery of a comparative sort of altered message is unimaginable on the grounds that speculating the specific random grouping without the message and time is close to inconceivable. Thereafter, we go through the means and procedures engaged with the age of the random numbers, encryption a plain text lastly decrypts cipher at the recipient end.

A. Random Number Generation Algorithm

The uniqueness of explained strategy starts with creation of a random number succession which is relegated to each printable character [12]. As of now have had random number creation procedures engaged with different algorithms yet creating a total succession based on string and time has not been the philosophy behind producing a random number [13]. The creation happens based on a discussion between the source and receiver The specific character is picked based on the initial time of call. Additional value of the digits in the seconds place chooses the place of the character which will be picked. The determined added value of event of character and the length is currently added with the second's worth of the hour of call to give an end-product. The cycle rehashes the same thing until there is an incentive for each printable character. Impediments can be demonstrated with the way that enhancement among the succession accompanies a bigger text conversation and the event that the text based discussion conveys a more extensive scope of characters. This interaction pulls back from the reliance just on time.

Step 1: Declared all variables, cn, in, as integer; fn, A[95], ln, jn, as String data type.
Step 2: Entered conversation message as input and call time.
Step 3: Calculated length of the message and stored in the variable, ln.
Step 4: Added first digit of the second place with, ln value.
Step 5: Determined each character and number of
event as, fn and number of event, cn.
Step 6: update, fn = first digit of second position of text + second digit of second position.

Step 7: Calculated, cn based on the, fn.
Step 8: update, cn = cn+ln.
Step 9: Allocated a value to each index of the array, A[].
continue these step ladder until, in = 95
update, Jn = jn + cn.
If value of, jn > 95 then,
update, jn = (jn % 94)
end if.
If, A[jn] != NULL
Increase, jn until array, a[jn] != NULL
If value of, jn > 95 then,
value of, Jn = 0.
End if
End if
array, A[jn] = in
Step 10: The random equivalents of array A is displayed.

B. Encryption Technique with Algorithm

The proposed encryption process utilize encoded multiplier procedure referenced before to encrypt string which holds characters having random number reciprocals or in an exact manner, the 8-bit character counterparts in parallel system. The random counterparts of each character have been viewed as here as an option of the UNICODE values. We got the last cipher by thinking about two characters all at once and by taking into account the way that the random qualities should be increased and consequently we get four partial products. The partial products so got and determined regarding consecutive 2-bit from the tail of the 8-bit parallel same. Consequently, got cipher through the four partial products in an erratic way alongside the main character random and carry this step until every characters of the plain text are changed to the ideal result. The acquired cipher is then ship off the recipient. Therefore,

$$\text{Cipher text, } C = E(R(P)) \qquad (4)$$

In equation(4), C is cipher text, R is conversion by the characters, E is encoded multiplier key, and P is plain text.

Step 1: Declared all variables, ar[], ur, ir, as integer; pr[], pr1[], br[], as long integer type; cipher as string data type.
Step 2: Input character of plain text one after another and
kept random equivalent values in the array ar[].
Increase, ir, one for every entry.
Step 3: Keep length of original text, ln
If, value of, ln odd,
Array, A[ir] = random equal for " ",
Increase, ir = ir +1.
Step 4: Alter elements of array ar[] to binary
and kept in another array, br[].
Step 5: Continue until, jn = ir - 1.
Array, pr[0] = 0
Update array, pr[1] = br[jn]
Update array, pr[2] = b[jn]*10 // shift 1 position.
Update array, pr[3] = pr[1]+pr[2] // binary addition

```
Initialize, kr = 0
Continue until, kr < 4
  Update variable, ur = br[jn+1] % 100.
  if, value of, ur = 0 then,
    array, pr1[kr] = pr[0]
  else if, value of, ur = 1 then,
    array, pr1[kr] = pr[1]
  if, value of, ur = 10 then,
    array, pr1[kr] = pr[2]
  else if, value of, ur = 11 then,
    array, pr1[kr] = pr[3]
  end if
  increase, kr = kr+1
  update, br[jn+1] = br[jn+1]\100
  update variable, cipher=cipher + pr1[3] + " " + pr1[1] +
                " " + pr1[0] + " " + pr1[2] + " " + pr[1].
 Increase, jn = jn+2
```

Step 6: variable cipher holds entire cipher text.

C. Encoding Technique with Algorithm

Encoding the cipher in a media (image is used in our experiment) is the next step for our encryption of the original message. Encoding any character within the pixels can be cumbersome as a conversion to its corresponding binary equivalents. In this paper, the actual plain text is first encrypted to a binary form using hash keys, mentioned earlier. An exclusive-OR operation solves our problem and the encoding is performed according to the following algorithm.

Step 1: Select any image.
Step 2: Read total pixels' number and obtained cipher length.
Step 3: if, cipher length > total no. of pixels then, Stop.
Step 4: Store pixel values one by one depleting last 2-bit of red, 3-bit from green and 3-bit of blue and performed exclusive operation on each bit.
Step 5: Stored length of the cipher in the first 5 pixels that are depleted from the image.
Step 6: Continue operation of Step-5, until the entire cipher is stored.

D. Decoding Technique with Algorithm

The Decoding and extracting of cipher from the received media follows a necessary stepwise solution where entire cipher is obtained before applying the decryption algorithm on it. The message extracted is a binary sequence and simply finding the combination of last 2-bit of red, 3-bit of green and 3-bit of blue of each pixel produces the cipher. This process continues till the entire cipher is extracted from the image. The following algorithm is used for decoding the image and extracting the cipher.

Step 1: Find out cipher length by removing the first five pixel from the received image.
Step 2: Deplete pixel and obtain the cipher by holding the last 2-bit of red, 3-bit of green, 3-bit of blue.
Step 3: Repeat Step 3 till we have a cipher equal to the length that was obtained in Step 2.

E. Decryption Technique with Algorithm

During deciphering, every P_i is then coordinated properly aligned. The P_i of second, third and fourth positioned are modified a bit in the accompanying way. The decimal equivalent will be,

i. second placed P_i multiplied by four.
ii. third placed P_i multiplied by sixteen and.
iii. fourth placed P_i multiplied by sixty-four.

The determined qualities are then accumulated alongside what might be compared to the main set P_i and afterward it is partitioned by the first character random equal which was likewise present in cipher. The acquired outcome is the second character random equivalent. The pattern of this decoding occasion continue till entire cipher message is broken and afterward the acquired qualities are organized and addressed as characters accordingly delivering the original message.

Step 1: Declared all variables, ar[], pr[], jn=0, ir=1, ln, integer; br[] long integer type.
Step 2: The input is cipher.
Step 3: Recover every binary sequence considering
separator " " and kept them in array, br[] and increase
jn by 1 for every character entered.
Step 4: Continue until, ir = jn
Transformed, br[ir], binary value to equivalent and kept in array, ar[ir].
Step 5: initialized, ln = 0
Step 6: Continue until, ir = jn-1
Update array, ar[ir] = ar[ir]+ar[ir+2]
Update array, ar[ir+2] = ar[ir]-ar[ir+2]
Update array, ar[ir] = ar[ir]-ar[ir-2]
Update array, ar[ir+2] = ar[ir+2]+ar[ir+3]
Update array, ar[ir+3] = ar[ir+2]-ar[ir+3]
Update array, ar[ir+2] = ar[ir+2]-ar[ir-3]
Update array, ar[ir+1] = ar[ir+1]*4
Update array, ar[ir+2] = ar[ir+2]*16
Update array, ar[ir+3] = ar[ir+3]*64
Update array, pr[lr] = ar[ir+4]
Increase, ln = ln+1
Update array, pr[ln]=(ar[ir]+ar[ir+1]+ar[ir+2]+ar[ir+3])/ar[ir+4]
Increase, ln = ln+1
Increase, ir=ir+5
Step 7: Check character equivalents of array pr[l] for all values consecutively to acquire the plain text.

Any intruder can attempt to comprehend the key utilized for encryption the message and hence can mess with the data. However, random number grouping for each message makes it exceptionally difficult to deliver an ideal altered data without accessibility of the actual system.

VIII. COMPLEXITY ANALYSIS

An essential perspective to data structures is design efficient algorithms. Algorithm states expressly the way that the data will be controlled by legitimate moving through grouping of guidelines [9]. The productivity of algorithms is relying upon its inner construction configuration, software engineer's ability and it is estimated by intricacy investigation. Time intricacy investigation is in many cases taken as fundamental apparatus for evaluating the proficiency of an algorithm. It is a hypothetical examination where individually line of code is

evaluated based on the times that line of code getting executed. By assessing each circle and restrictive explanations and so on, we can look at the intricacy between two distinct methodologies of algorithms for execution of a program. In the comparative methodology, the examination of our whole strategy was performed. We accomplished intricacy, O(n) of the introduced algorithms for age random numbers, encryption, encoding, unraveling and decoding process, make sense of subtleties hereunder.

IX. EXPERIMENTAL RESULT ANALYSIS

The experiments utilized for explore include various types of texts involving a wide range of characters. Messages like, "Encryption Time for Vedic Multiplier Technique", telephone numbers have been utilized for trial examination. The ninety-five plain text characters alludes to the experiment where we have utilized every one of the printable characters and figure out execution time taken by the encoding and decoding process. The recovery of the first message was effectively accomplished in every one of the cases.

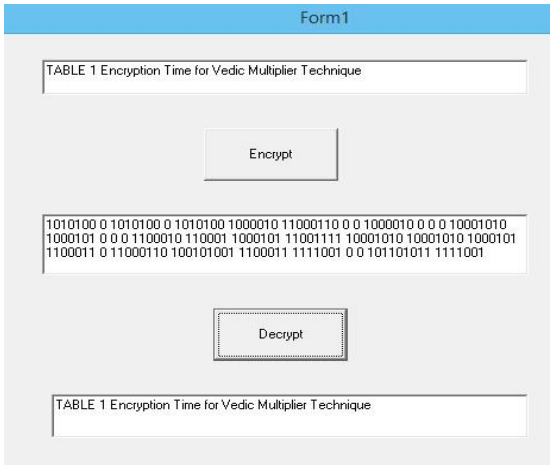

Fig. 5: Screenshot of Vedic Multiplier Implementation

The existing ASCII algorithm published by U. Pujeri et. al. [18], ANN algorithm published by S. K. Pal et. al. [17], and algorithm presented here are examined using the Intel i3, 6th generation processor. The performance analysis has done using experimental data and has represented graphically. The programs were executed considering different input length of the messages (n).

Table 1. Execution time(in second) of three algorithms

Length of Plain Text	ASCII Algorithm [18[	ANN Algorithm [17]	EMT Algorithm
8	0.1413467	0.0101402	0.1236
9	0.1424234	0.008811	0.13
11	0.1471541	0.0336561	0.0675
23	0.1358411	0.0752692	0.1048
24	0.141376	0.0343788	0.1144
25	0.1574321	0.0600448	0.0945
28	0.1620119	0.0528805	0.11235
36	0.1272886	0.0910726	0.1185
39	0.1390269	0.078532	0.105
42	0.2077701	0.0735135	0.14973
43	0.1554613	0.0750353	0.11396

44	0.1551487	0.1098869	0.138
61	0.1473556	0.1011186	0.1545
95	0.6626222	0.4152881	0.245052

The experimental data obtained by execution of three algorithms is used to draw the comparative chart shown in figure 6.

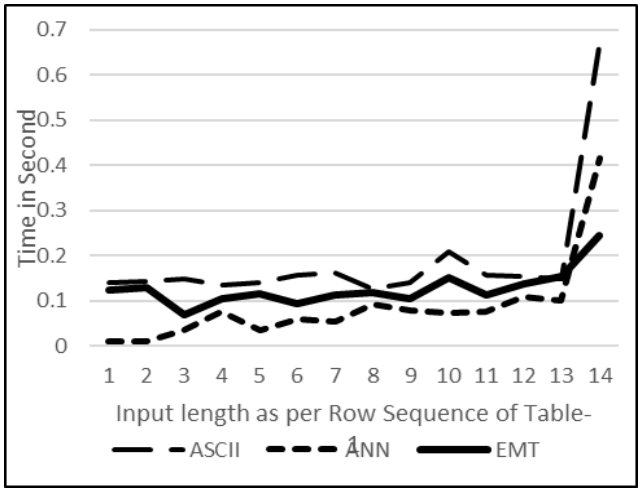

Fig. 6: Comparative chart of three algorithms of Table-1

CONCLUSION

The two most fluctuating ideas of development is considered prior to making the random number succession time and human word. Various exceptional procedures introduced here and shows how this strategy is offers another aspect for encryption and decoding of a mystery messages. The advantage of introduced strategy over the current techniques is only the use of a random number grouping which upgrades vigor and dependability of the algorithm. Regardless of whether, the cipher is undermined by the channel and an intruder impedance the cipher, beast force is supposed to break it. Thus, the presented system more secured and dynamic in nature. Now, the presence of a steganography media (image is used) adds to the already achieved level of security by removing the possibility of interfering of confidential message. Achieving complexity, the order O(n) ensures this algorithm is well acceptable. The incorporation of individual random numbers for every individual message makes it safer contrasting with the current strategies. The utilization of encoded multiplier method gives one more degree of safety. This system unquestionably can be a resource for any official correspondence conventions where inside intruders of the association can be limited for altering of the private and classified messages. The exploratory consequences of the carried out system have given in table-1 to similar examination. A key is protected for however long it isn't uncovered by the intruders. In this paper we have made another key which can be utilized for secure transmission of data aside from brute force attack which will require longer time to break the key.

REFERENCES

[1] Bonifus PL and Dani George, “Ecc Encryption System Using Encoded Multiplier and Vedic Mathematics”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, pp. 5531-5538, 2013.

[2] Dwi Liestyowati, “Public Key Cryptography”, Journal of Physics, vol. 1477, pp. 1-7, 2020. https://doi.org/10.1088/1742-6596/1477/5/052062.

[3] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, “Rotation, scale, and translation resilient public watermarking for images,” IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

[4] R. Raja Kumar, R. Pandian, T. Prem Jacob, A Pravin and P. Indumathi, "Cryptography using Chaos in Communication Systems", Journal of Physics, vol. 1770, pp. 1-7, 2021. https://doi.org/10.1088/1742-6596/1770/1/012096.

[5] Young-Chang HOU, A-Yu TSENG, Zen-Yu QUAN and Hsin-Ju LIU, "An IPR protection scheme based on wavelet transformation and visual cryptography", Turkish Journal of Electrical Engineering & Computer Sciences, vol. 24, pp. 4063-4082, 2016. https://doi.org/10.3906/elk-1405-180.

[6] B. Schneier, "Applied Cryptography: Protocols, Algorithms", Available in the website: https://www.researchgate.net/publication/245452241_Applied_cryptography_protocols_algorithms, Access time: 08, February, 2022.

[7] Sanjay Kr. Pal, Samar Sen Sarma, "Graph Coloring Approach for Hiding of Information", Procedia Technology, Elsevier, vol. 4, pp. 272-277, 2012. https://doi.org/10.1016/j.protcy.2012.05.042

[8] Jai Skand Tripathi, Priya Keerti Tripathi, Deepti Shakti Tripathi, "An Efficient Design of Vedic Multiplier Using New Encoding Scheme", International Journal of Computer Applications, vol. 53, pp. 6-10, 2012.

[9] Complexity Analysis. Available in the website: www.cs.utexas.edu/users/djimenez/utsa/cs1723/lecture2.html, Time Accessed: 08, February, 2022.

[10] S.Devi, K.Kanagaram, V.Palanisamy, "A New Approach for Encryption Method using Collective Techniques with Rijngdael Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, pp. 7030-7036, 2014.

[11] Mrs. Saylee Gharge, Mr. Honey Brijwani, Mr. Mohit Pugrani, Mr. Girish Sukhwani, Mr. Deepak Udherani, "Percon8 Algorithm for Random Number Generation", Int. Journal of Engineering Research and Applications, vol. 4, pp. 54-60, 2014.

[12] S G Srikantaswamy, Dr. H D Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security, vol. 2, pp. 39-49, 2012. https://doi.org/10.5121/ijcis.2012.2405.

[13] Mina Mishra, V.H.Mankar, "Text Encryption Algorithms based on Pseudo Random Number Generator", International Journal of Computer Applications, vol. 111, pp. 1-6, 2015. https://doi.org/0.5120/19507-0756.

[14] A.V.N.Krishna, "Probabilistic Encryption Based ECC Mechanism", International Journal of Advancements in Technology, vol. 2, pp. 257-267. ISSN 0976-4860, 2011.

[15] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain", International Journal of Security, Privacy and Trust Management, vol. 3, pp. 11-22, 2014. https://doi.org/10.5121/ijsptm.2014.3102.

[16] Indradip Banerjee, Souvik Bhattacharyya, Gautam Sanyal, "A Procedure of Text Steganography Using Indian Regional Language", I. J. Computer Network and Information Security, vol. 8, pp. 65-73, 2012. https://doi.org/10.5815/ijcnis.2012.08.08.

[17] S. K. Pal, B. Datta, and A. Karmakar, "An ANN Approach of Twisted Fiestel Block Ciphering", Emerging Technologies in Data Mining and Information Security, Lecture Notes in Networks and Systems, Springer Nature, vol. 3, pp. 47-56 2021. https://doi.org/10.1007/978-981-15-9774-9_5.

[18] U. Pujeri, and R. Pujeri, "Symmetric Encryption Algorithm using ASCII Values", International Journal of Recent Technology and Engineering, vol. 8, pp. 2355, 2020. https://doi.org/10.35940/ijrte.E5980.018520.