Performance Evaluation of Stream Ciphers for Efficient and Quick Security of Satellite Images

Haroon Ibrahim and Khurram Khurshid
Electrical Engineering Department, Institute of Space Technology, Islamabad, 44000, Pakistan
Email: haroon.ibrahim@ist.edu.pk, khurram.khurshid@ist.edu.pk

***Abstract*—It has been seen that cipher techniques have proved to be very useful in the analysis and design of stream cipher analysis techniques. This paper summarizes the current situation of the stream cipher analysis in Satellite imagery. Furthermore, the paper analyzes and compares several classic analysis techniques such as Shift Cipher, Permutation cipher, Affine Cipher, Hill Ciphers, Rivest Shamin Adleman (RSA) Ciphers, Pseudo Random (PR) cipher and Substation ciphers. The paper explores the efficient cipher techniques among above ciphers for quick and efficient security in satellite imagery in real time onboard data processing.**

***Index Terms*—shift, permutation, affine, hill, Rivest Shamin Adleman (RSA), Pseudo Random (PR), substation, Consultative Committee for Space Data Systems (CCSDS)**

I. Introduction

With the increase in size of storage and sharing of information, the scope of digital data is beyond any ambiguity. It is easy to store the digital data in form of pictures, audio and video on small chips with speed and reliability. The communication of this digital data has many advantages over the traditional analog methods. The most important application is the data security. There are many known methods which have been adopted for data encryption in all the three stated above. All these encryption schemes have common aims that include high security, speed and accuracy with less design complexity.

These aims may vary according to the type of application like simple social media bids to highly confidential military or remote sensing purposes. Encryption is simply a way to secure the data using a key, which makes the data unreadable to others [1]. On the other side, decryption is used to retrieve the original data by using a decryption key.

Packet Telemetry is an idea which encourages the transmission of room obtained information from source to client in an institutionalized profoundly mechanized way [2]. Parcel Telemetry gives an instrument to executing regular information transport structures and conventions which may upgrade the improvement and activity of room mission frameworks.

Fig. 1 Below shows the format of the telemetry transfer frame headers and data fields as specified by CCSDS. Since this communication structure provides the best quality satellite communication in term of reliable transmission from space to ground. The only thing which has been left to the researchers is to explore some sophisticated ciphering technique which should provide high level of security for space-born data with suitable downlink speed. Since, large number of encryption techniques are available in for securing either archived data or real time communication contents. Among them, AES is considered as the best encryption technique. Ciphering algorithms come in two different fashions namely, Block Ciphers & Stream Ciphers.

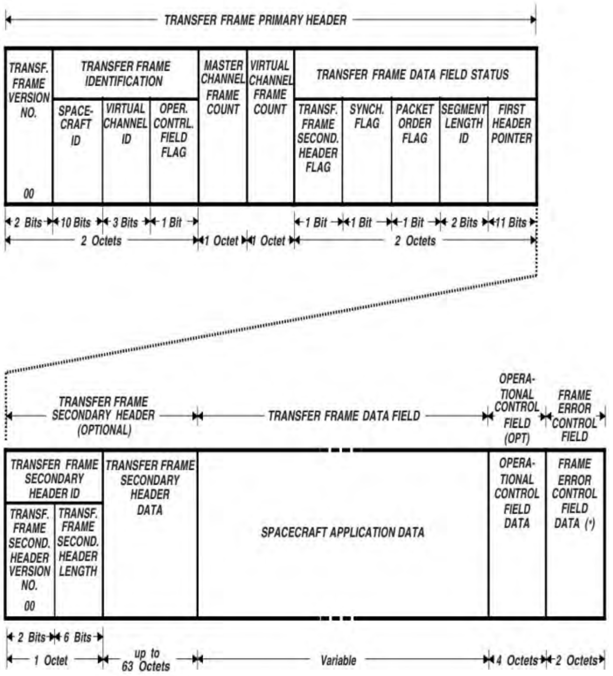

TRANSFER FRAME PRIMARY HEADER
TRANSF. FRAME VERSION NO.
00
TRANSFER FRAME IDENTIFICATION
SPACE-CRAFT ID
VIRTUAL CHANNEL ID
OPER. CONTRL. FIELD FLAG
MASTER CHANNEL FRAME COUNT
VIRTUAL CHANNEL FRAME COUNT
TRANSFER FRAME DATA FIELD STATUS
TRANSF. FRAME SECOND. HEADER FLAG
SYNCH. FLAG
PACKET ORDER FLAG
SEGMENT LENGTH ID
FIRST HEADER POINTER
2 Bits
10 Bits
3 Bits
1 Bit
1 Bit
1 Bit
1 Bit
2 Bits
11 Bits
2 Octets
1 Octet
1 Octet
2 Octets
TRANSFER FRAME SECONDARY HEADER (OPTIONAL)
TRANSFER FRAME DATA FIELD
OPERA-TIONAL CONTROL FIELD (OPT)
FRAME ERROR CONTROL FIELD
TRANSFER FRAME SECONDARY HEADER ID
TRANSF. FRAME SECOND. HEADER VERSION NO.
00
TRANSF. FRAME SECOND. HEADER LENGTH
TRANSFER FRAME SECONDARY HEADER DATA
SPACECRAFT APPLICATION DATA
OPERA-TIONAL CONTROL FIELD DATA
FRAME ERROR CONTROL FIELD DATA (*)
2 Bits
6 Bits
1 Octet
up to 63 Octets
Variable
4 Octets
2 Octets

Figure 1. Primary and Secondary header with data field (CCSDS).

Block ciphers operate upon the chuck of data which is comprised of even number of octets, steams ciphers have the provision of encrypting the data content in both fashion (either chunk or single byte). Fig. 1 Shows the restriction of communication with odd number of octets for example, transfer frame's data field. The block ciphers won't provide an attractive choice of data security as they normally operate upon even number of octets and can leave some crucial part of data which brings the risk of content hacking by an unauthorized source. The block

Manuscript received February 16, 2019; revised August 12, 2019.

doi: 10.18178/ijsps.7.3.96-102

cipher simulates the plain face image and satellite acquired image provided in Fig. 2.

The Fig. 2 Explains the process of the CCSDS based data communication protocol for image transfers then the portion of the chunks left unencrypted, return the poor ciphering results and high risk of content hacking.

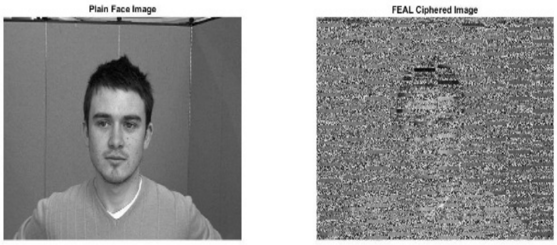


Figure 2. Partially block ciphered image.

The Stream ciphers have the capability to secure the whole transfer frame, but they are not powerful ciphers compared to block ciphers.

Image encryption techniques are used to convert an image into another coded one. One basic method which is used for this purpose is position permutation of pixels. It shuffles the position of the pixels in the image, but the overall histogram remains the same. This method is less secure with less complexity. Another major method of encryption is using value transformation [3] in which it changes the pixel values. To achieve the high accuracy and low complexity, combination of position permutation and value transformation is performed [4].

Satellite innovation has changed interchanges, allowing less demanding and quicker information exchanges between self-assertively far off parts of the world. In such frameworks, a space borne stage gathers logical information and transmits them to a ground station and at the ground fragment, a progression of picture products is associated that can be made accessible to research or business associations for abuse. Cryptography is the art of keeping private data whether conveyed over anchored or unbound channel from unapproved access, of guaranteeing information classification, respectability and verification, and different assignments [5]. They are mainly two ways of symmetric ciphering digital data:

- Block ciphering
- Stream ciphering

Block cipher is a deterministic algorithmic guideline agent on settled length gatherings of bits, called a block, with an unvarying change that is determined by a stellate key. Block cipher work as imperative basic components in the structure of a few cryptography conventions, and are wide utilized to execute encryption of mass data

Stream cipher is a symmetric key encryption where plaintext digits are joined with a pseudorandom cipher digit stream (key stream). In a stream figure, each plaintext digit is scrambled each one in turn with the comparing digit of the key stream, to give a digit of the figure content stream. Since encryption of every digit is reliant on the current condition of the figure. The telemetry Transfer Frame specied in Active Directory (AD1) and Active Directory (AD2) is composed of a primary header, a secondary header, a data field and a trailer with the above-mentioned Fig. 1

The agenda in this research is to explore the stronger stream ciphering technique which could provide almost at the block cipher level security with high throughput of data from space to ground. Since this format (CCSDS) does not support the block ciphering of space-born data which is necessary to protect the data from unauthorized user [6]. This format of data communication can’t be adjusted with block ciphers because of odd number of octets in the protocol structure. Keeping this view, the stream ciphers are utilized as a sophisticated choice for secure telemetry transfer frame. This research will explain different stream ciphering techniques for exploring the best ciphering algorithm. It will not only provide the best security but also an attractive choice of enhancing downlink data rate.

Rest of the paper is organized as follows: the proposed methodology is provided in section II, results are provide in section III, Conclusion is given in section IV followed by Future works in section V.

II. Methodology

The comparison of the different types of stream ciphers are evaluated on their performance in terms of feature hiding (security), mathematical complexity, processing speed etc. All the techniques are applied over satellite acquired imagery provided in Fig. 3.

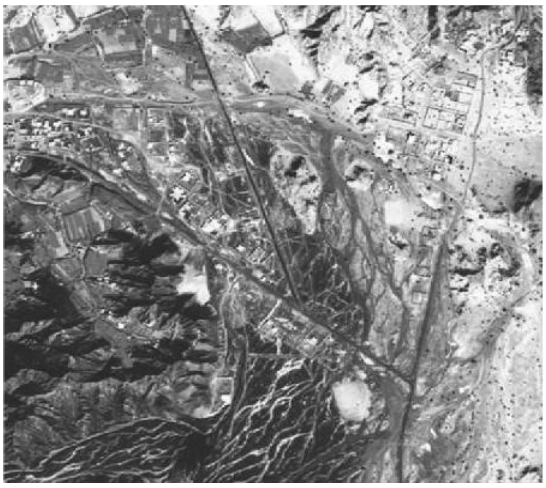


Figure 3. Original test image.

A. Shift Cipher

Shift cipher is one of the simplest block/stream ciphers which can be used in both block and stream ciphering which depends upon the requirement and choice of the user. Eq. (1) shows the mathematical formula for shift cipher.

$$C = (P + K) \bmod n, \tag{1}$$

$$P = (C - K) \bmod n, \tag{2}$$

P is the user provided plain text, *K* is the secret key, *C* is the cipher text and *n* is the user dependent viable which defines the limits of plain text. For example, if over plain text is comprised of four bits then the value *n* would be *24 = 16*. Similarly, for 8 bits plain text the value of *n* would be 256. Suppose, the key for a shift cipher is *K = 15*, and the plain text is taken as *P=18*, Using the above equation for ciphering the plain text we get

$$C = 15+18 mod\ 32$$

$$C = 1$$

The plain text has been converted from *18* to *1*. The deciphering is applied to retrieve the original plain text using eq. (2).

$$P = 1 - 15\ mod\ 32,\ P = 18$$

The extracted original text is shown in the equation above. The suitability of the cipher for securing satellite imagery can be retrieved by applying the equations on the images in Fig. 4.

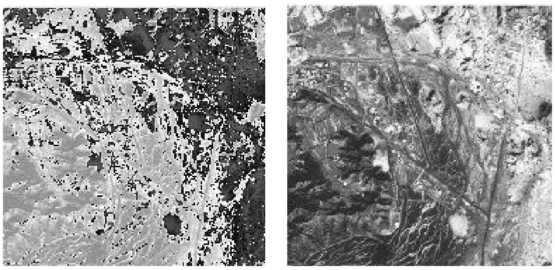

(a) (b)

Figure 4. Shift ciphering (a) Cipher image (b) De-ciphered image

B. Affine Cipher

Affine cipher is the special case of shift cipher which includes either two another special perimeter along with shifting index this special parameter is known as multiplicative index [7]. The mathematical formula of this cipher provided in Eq. (3) - (4).

$$C = (Ax + B)\ mod\ n, \tag{3}$$

$$x = A-1(C - B)\ mod\ n. \tag{4}$$

x is the user's provided plain text and (A, B) that will be acting as a secret key and C is the cipher text and *n* is the user's dependent viable which defines the limits of plan text as described earlier. The choice of B could be anything within the boundaries of shifting index limit. However, the choice of A cannot be any random number, but those numbers should be substitute in this variable whom multiplicative inverse exacts in the vector space [8].

Suppose five-bit number is taken, *n is taken as 26* and *A= 3,* then its multiplicative inverse will be equal to *9*. The resultant comes out as:

$$(3\times9)\ mod\ 26 = 1$$

Now for *A = 2,* the reminder equal to 1 will not be returned if we multiply it with 2. The ciphering of some random number can be achieved as, if we take *A = 3, B = 10* and *x = 14*. The results can be retrieved as

$$C = (3\times14+10)\ mod\ 26\ C=0.$$

Now from the Eq. (4) for deciphering this text is

$$x = 9(0-10)\ mod\ 26,$$

$$x= -90\ mod\ 26,\ x=14.$$

Here it can be seen that same plain text which was ciphered as 0. The same ciphered image is used for the final process in Shift ciphering. The achieved results can be seen in Fig. 5.

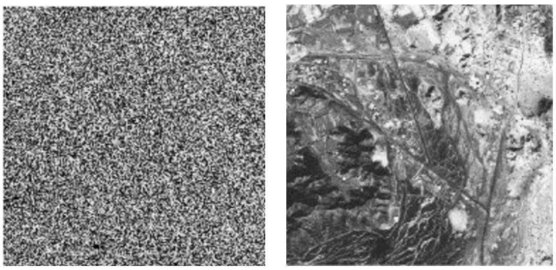

(a) (b)

Figure 5. Affine ciphering (a) Cipher image (b) De-ciphered image.

C. Hill Cipher

The complexity of Hill ciphering depends upon the choice of encryption key. For this ciphering technique, the choice of encryption is the number of words fed into the machine. The secret key will be in the form of two-dimensional matrix with the dimension from 2 × 2 to *n*×*n* [9]. While selecting the secret key for ciphering the plan text it is ensured that the inverse of the matrix must exist. For deciphering the ciphered text, the example of ciphering from four bytes of data using the same secret key.

Suppose out ciphering key is

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

And deciphering key

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

We can see both the keys are inverse of each other and this can be verified from their multiplication which gives us an identity matrix.

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} =$$

$$\begin{pmatrix} 11\times 7+8\times 23 & 11\times 18+8\times 11 \\ 3\times 7+7\times 23 & 3\times 18+7\times 11 \end{pmatrix}$$

$$=\begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The example is provided to illustrate encryption and decryption using Hill ciphering algorithm. Suppose the encryption of the plaintext (9, 20) is shown.

$$(9{,}20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99+60, 72+140) = (3{,}4)$$

To decrypt this message upon receiver end we get:

$$(3{,}4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9{,}20)$$

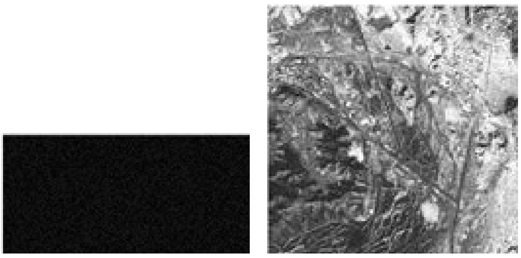

(a) (b)

Figure 6. Hill ciphering (a) Cipher image (b) De-ciphered image.

D. Substitution /Permutation Cipher

This type of a ciphering algorithm, the random sequence of decimal numbers is generated. Depending upon the width (bits required to represent the single word) of encipher data [10]. While working with 8 bits of digits, generation of 256 random numbers is needed which will be used for substation against some specific digits of un-cipher dat. For example, the representation the decimal number 10 against the substation value of 64. The random number with the different combinations is generated in every new pass that is 10 will be represented as a 53 in a new pass. The mathematical formula of substation cipher can be seen in equation below. The ciphering technique has-been celebrated in Table I – II.

$$C = (P), \quad (5)$$

$$P = C^{-1}, \quad (6)$$

TABLE I. SUBSTITUTION CIPHER AND DE-CIPHER

X	1	2	3	4	5
C = (X)	12	4	8	5	9
C	12	4	8	5	9
X = C^{-1}	1	2	3	4	5

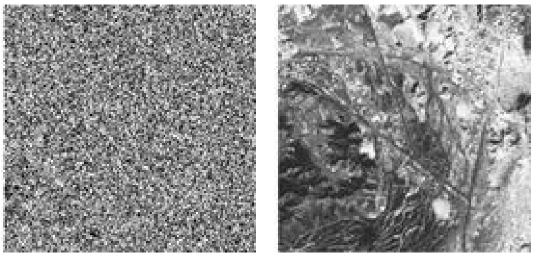

(a) (b)

Figure 7. Substitution cipher (a) Cipher image (b) De-ciphered image.

E. Vigenere Cipher

This ciphering technique is very much like to the Shift ciphering algorithm. [9] In this type of a ciphering algorithm, the chunks of data comprising of multiple words depends upon the user requirement. The length of the key will change according to the chunk length. In this case we can quickly cipher the large amount of data as compare to shift cipher however the mathematical operations are performed in a very much similar fashion as we do in shift cipher the Eq. (9)-(10) elaborate the process of *vigenere* cipher with the *molder value* of *26.*

$$C=(P_1+ K_1)mod26,(P_2+K_2)mod26,(P_3+K_3)mod26, \quad (7)$$

$$P=(C_1-K_1)mod26,(C_2-K_2)mod26,(C_3-K_3)mod26, \quad (8)$$

TABLE II. VIGENERE CIPHER AND DE-CIPHER

P	11	7	10	19
K	13	23	4	12
C	23	4	14	5

C	23	4	14	5
K	13	23	4	12
P	11	7	10	19

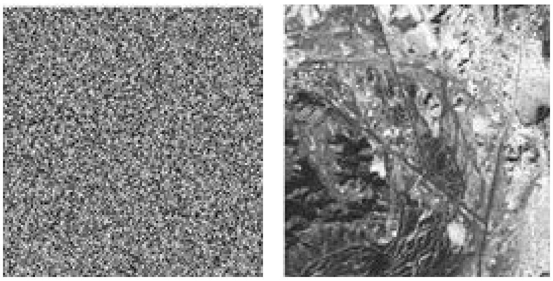

(a) (b)

Figure 8. Vigenere ciphering (a) Cipher image (b) De-ciphered image.

F. Pseduo Random Cipher

This cipher comes in one of the most powerful ciphering Techniques which encrypt single bit in a word by generating strong random bits sequence [11]. This random sequence can be generated using different Galois field polynomials where the length of polynomial can vary from 3 degrees to 24th degree. The choice of polynomial is once again purely dependent upon the user constraints. Below is an example of 3-degree polynomials circuits which generate the random bits of the key as can be seen in Fig. 9. The choice of initial content is restricted to be initialized with all zeroes. However, any other sequence of bits can be used as an initial content. While decryption the care is taken for the massage that initial with content at deciphering side should be same as of initial content of ciphering side.

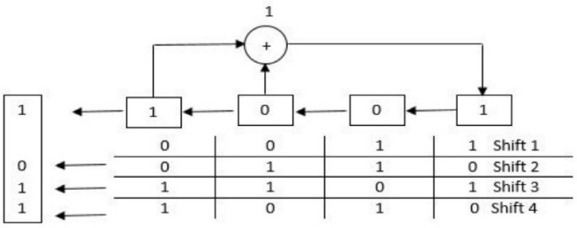
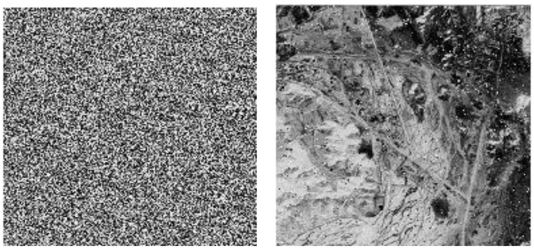


Figure 9. Psedue random bit generator.

TABLE III. VIGENERE CIPHER AND DE-CIPHER

1	1	1	1	0	1	1	0
1	0	0	1	1	0	0	1
0	1	1	0	1	1	1	1



(a) (b)

Figure 10. Pseudo ciphering (a) Cipher image (b) De-ciphered image.

G. RSA Cipher

RSA (Rivest Shamir Adleman) is known open key for cryptosystems and it is in fact, generally utilized for anchored information transmission [12]. In cryptosystem, the encryption key is constantly open, and it is not quite the same as the unscrambling key which is kept mystery (private) [13]. In RSA, this asymmetry depends on the handy trouble of the factorization of the result of two expansive prime numbers, the "figuring issue".

$$C = P^{13} mod\ 77, \tag{9}$$

$$P = C^{37} mod\ 77, \tag{10}$$

where e = *public key* and d = *private key*. Take two different prime numbers p and q and let $p = 7$ and $q = 11$ then

$$n = p = 77;$$

$$\phi = (p -1)\ (q -1) = 60.$$

Calculating d (The Private Key): d must fulfill the following criteria

$$d \times e\ mod\ \phi(n) = 1. \tag{11}$$

Let's move towards Extended Euclidean Algorithm for calculating d. Consider the equation below

$$Ax + By = gcd(a,b) \tag{12}$$

$A = \phi\ B = e$ so equation 12 becomes $\phi x + ey = gcd(\phi,e)$ so $60x + 13y = 1$ as the *gcd (The Greatest Common Divider)* of *(60,13)* is equal to *1*. So here we calculate x and y to make the above equation equal on both sides. Here the value of y will be the value of our private key d. $a_3 = a_1 - (a_2 \times k_2)$. Similarly

TABLE IV. VIGENERE CIPHER AND DE-CIPHER

Sr. No	a	b	D	K
1	1	0	ϕ = 60	-
2	0	1	e = 13	K = d_1=d_2 = 60=30 + 4
3	1	-4	8	1
4	-1	5	5	1
5	2	-9	3	1
6	-3	14	2	1
7	5	-23	1	2

$b3 = b1\ (b2 \times K2)$. All the entries in the above table will be filled using this formula.

The above table as soon as $d = 1$ is achieved, the computation is halted. The very first thing after getting $d = 1$ is to save the value of b which is *-23* and this is the value of our private key. Now, the check for the equality of Eq. (12) is taken after feeding values of ϕ and e. So, *Eq*.13 becomes

$$\phi x + ey = gcd(\phi,e) \tag{13}$$

For $\phi = 60\ x = 5\ e = 13$ and $y = -23$, Eq. becomes

$$60(5) + 13(-23) = gcd(60,13),$$

$$300 - 299 = 1,$$

$$1 = 1,$$

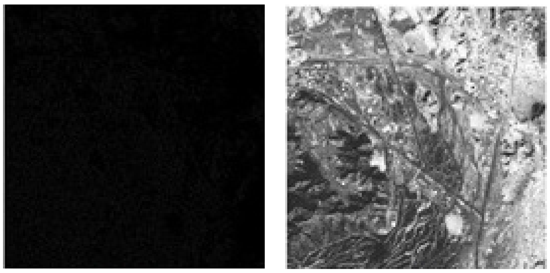
The check for the value of d. If $d > \phi$, where $d = d\ mod\ \phi$ and if $d < 0$ then $d = d + \phi$, now for d, becomes as $d < 0$ so our d will be

$$d = d + \phi = (-23+60) = 37$$

$$C = P^{13} mod\ 77,$$

$$P = C^{37} mod\ 77,$$

where e = *Public key* and d = *Private Key*.



(a) (b)

Figure 11. RSA ciphering (a) Cipher image (b) De-ciphered image.

III. Results

While evaluating the performance parameters against any mathematical algorithm we mainly focus upon four crucial reading like execution time, computational complexity, Algorithms capability of a certain task and invert ability. Here we will be focusing upon these parameters in terms of feature hiding capability of a ciphering algorithms, computational complexity toward the implementation and time constraints. Here we will be having such type of four parameters namely

- Tc (Ciphering time)
- Td (Deciphering time)
- CC (Computational Complexity)
- FHC (Feature Hiding Capability)

Table V Shows the performance of all the implemented ciphers in term of their capability towards ciphering satellite imagery of three different regions (forest, mountains, water and city area). The hill/Pseudo cipher is found to be a suitable candidate for using in security of deep space mission.

TABLE V. Results of Ciphering Comparisons on Different Parameters

Sr. No	Algorithm	Parameters	Image 1	Image 2	Image 3
1	**Shift Cipher**	T_c	0.539603	0.485459	0.140074
		T_d	0.034036	0.028479	0.029108
		CC	Low		
		FHC	Low	Low	Low
2	**RSA Cipher**	T_c	0.874546	0.927301	0.253999
		T_d	0.711959	0.694237	3.534351
		CC	High		
		FHC	High	High	High
3	**Hill Cipher**	T_c	9.549282	9.778532	4.114128
		T_d	7.927327	8.134487	3.534351
		CC	Medium		
		FHC	High	High	High
4	**Pseudo Cipher**	T_c	6.259693	6.249292	2.957655
		T_d	16.753962	16.969243	7.979419
		CC	Low		
		FHC	High	High	High
5	**Affine Cipher**	T_c	0.527290	0.535935	0.143820
		T_d	0.067827	0.068020	0.054933
		CC	Medium		
		FHC	High	High	Medium
6	**Substitution/ Permutation Cipher**	T_c	0.463274	0.469690	0.132381
		T_d	0.318529	0.309978	0.124263
		CC	Low		
		FHC	Medium	High	Low
7	**Vigenere Cipher**	T_c	0.549825	0.548444	0.174115
		T_d	0.139080	0.142541	0.081735
		CC	Low		
		FHC	Medium	Medium	Medium

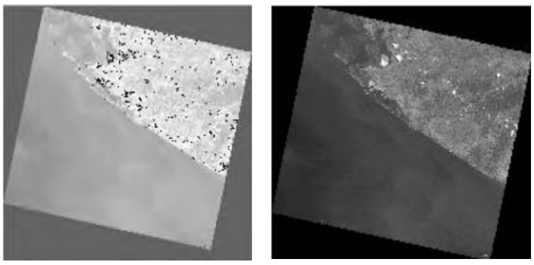

(a) (b)

Figure 12. Ciphered and De-Ciphered Image using Shift Cipher.

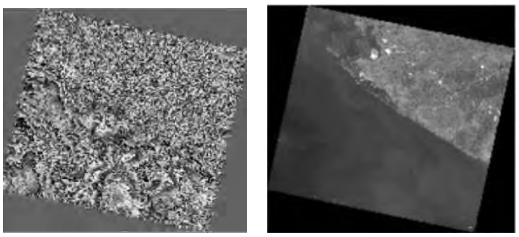

(a) (b)

Figure 13. Ciphered and De-ciphered image using affine cipher.

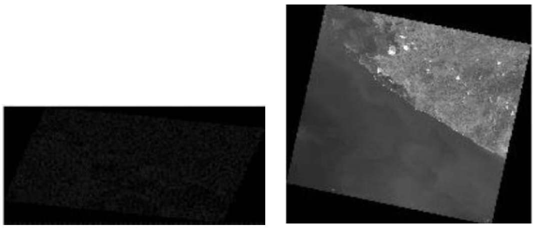

(a) (b)

Figure 14. Figure ciphered and De-ciphered image using hill cipher.

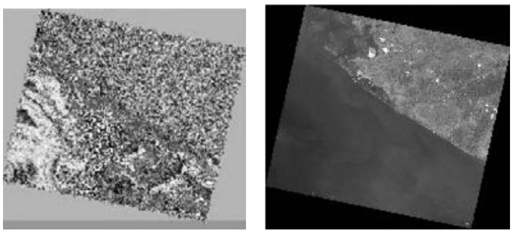

(a) (b)

Figure 15. Ciphered and De-ciphered image using substitution cipher.

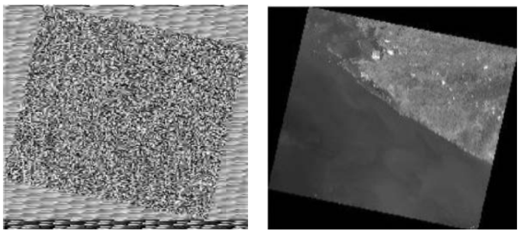

(a) (b)

Figure 16. Ciphered and De-ciphered image using vigenere cipher.

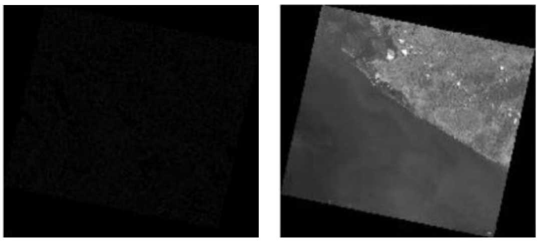

(a) (b)

Figure 17. Ciphered and De-ciphered image using pseudo cipher.

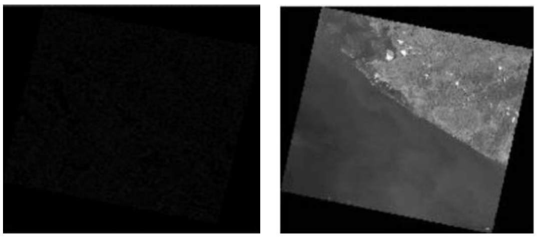

(a) (b)

Figure 18. Ciphered and De-Ciphered Image using RSA Cipher.

IV. Conclusion

In this research seven different ciphering algorithm are implemented to evaluate the security level over different satellite acquire images along with exploring the quick data processing technique which is capable of not only hiding image features but also provides with the provision of quick ciphering and deciphering of big data. RSA is found to be the most efficient algorithm which hides the features in an image more efficiently as compare to any other technique, but this technique is more complex/expensive in terms of computational efficiency. Similarly, if technique like Hill/affine cipher is focused then it can be clearly observed that they provide a very good computation efficiency along with a sophisticated method of feature hiding in an image. In this research pseudo random cipher is found to be the best cipher which provide both the phenomena (security and quick data processing) simultaneously. Galois field polynomial of order 8 degrees is used. However, it can also provide the choice the polynomial of even higher degree to gain more redundancy in bit stream which can be used for ciphering plan text.

V. Future Work

This research explores a suitable ciphering technique which can be encapsulated with telemetry unit of OBDH (On-Board Data Handling) system of satellites. The ciphering algorithm is enhancing the downlink speed (data rate) along with providing good security can be selected as a proposal in CCSDS data communication protocol [14]. Nominally, the OBDH system of satellite is based upon some embedded platform. All the proposed ciphering techniques are needed to be implemented upon an embedded platform like FPGA or microprocessor to explore the suitable encryption algorithm which should not only provides the best feature hiding capability but also gives an attractive choice of downlink data rate of telemetry.

Acknowledgment

The authors would like to thank Mr. Zeeshan Abbas from *Pakistan Space and Upper Atmosphere Research Commission* for providing guidance and data for analysis.

References

[1] S. S. William, *Cryptography and Network Security: Principles and Practice*, NJ: Prentice-Hall, Inc, 1999, pp. 23-50.

[2] D. Boneh and V. Shoup, “A graduate course in applied cryptography,” *Draft 0.2*, 2015.

[3] E. Barkan, E. Biham, and N. Keller, “Instant ciphertext-only cryptanalysis of gsm encrypted communication,” in *Proc. 23rd Annual International Cryptology Conference*, 2003, pp. 600-616.

[4] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, New Jersey: John Wiley & Sons, 2010.

[5] T. H. Barr, *Invitation to Cryptology*, NJ: Prentice Hall Upper Saddle River, 2002.

[6] H. H. Kilinc and T. Yanik, “A survey of sip authentication and key agreement schemes,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1005-1023, 2014.

[7] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[8] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, New York: Springer Science & Business Media, 2009.

[9] D. R. Stinson, *Cryptography: Theory and Practice*, Boca Raton: CRC Press, 2005.

[10] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC press, 1996.

[11] E. Bach and J. Shallit, “Algorithmic number theory. Efficient algorithms, vol. 1,” *Lecture Notes in Computer Science*, 1996.

[12] J. Pelzl and C. Paar, “Asymmetrische verfahren basierend auf dem diskreten logarithmusproblem,” *Kryptografie Verstandlich*, pp. 235-271, 2016.

[13] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, New Jersey: John Wiley & Sons, 2007.

[14] D. V. Bailey and C. Paar, “Efficient arithmetic in finite field extensions with application in ellipticcurve cryptography,” *Journal of Cryptology*, vol. 14, no. 3, pp. 153-176, 2001.

Haroon Ibrahim has been associated with Institute of Space Technology (IST), Pakistan since 2016. Currently he is coordinating the Electrical Engineering department and looking after the Signal Image Processing research group. He has completed MS degree recently from Institute of Space Technology Pakistan. Since 2015, he has been involved in various research ventures in the field of RFM, Image Processing, Pattern Recognition, Computer Vision and Cryptography. He is also contributing in HEC funded Research Project High Altitude Platform.

Khurram Khurshid has been associated with Institute of Space Technology (IST), Pakistan since its inception in 2002. Currently He is heading the Electrical Engineering department and looking after the Signal Image Processing research group. He did his PhD from Paris Descartes University, France in 2009. Since then, he has been involved in various research ventures in the field of Image Processing, Pattern Recognition and Computer Vision. He is one of the founding members of Pakistan Pattern Recognition Society (PPRS) and is also the project manager of the small satellite Cube Sat program of IST, the ICUBE. The first cube Sat satellite of this project (ICUBE-1) was successfully launched in November 2013. Apart from that, he is the editor of Journal of Space Technology which is an HEC recognized annual peer-reviewed journal. He is also contributing as reviewer and committee member for various international journals and conferences. He was given the award of ’Best University Teacher’ in Pakistan in January 2016 by the Higher Education Commission.