Article can be accessed online at http://www.publishingindia.com

SECURE SATELLITE IMAGE COMMUNICATION USING DCT, DWT, MEDIAN FILTER AND RSA

Ekta Chauhan

**Department of Computer Science Engineering, Maharana Pratap College of Technology, Gwalior, Madhya Pradesh, India.*
Email: ektachauhan81@gmail.com

Abstract *Secure image communication has it's own importance right from the present days of computing. Communication which is based on satellite is a way to the digital data transmit from various geographic location with utilizing satellites Satellite as communication medium to transfer information vulnerable many information security threat types, and require a new methodology for safe and secure data transmission over satellite. In this paper, for secure satellite image communication using median filter for remove impulse noise, RGB image convert into an HSV image, satellite image using DWT for decompose into sub-bands LL, HL, LH and HH and apply DCT on HH band and RSA using for encryption purpose.*

Keywords: *DWT, DCT, RGB, Median Filter, etc.*

Introduction

Satellite communication is used in various fields, e.g. to provide trunk links for network service providers and temporary communication systems in emergency & disasters. In this situation the benefits contain global coverage, capability of anti-disaster, immediate & flexible network configuration, and satellite can act as a backup link [1].

The communication of satellite industry has established tremendously and various professionals and activities range has developed as well [2]. This has altered in response to instant need to serve clients burgeoning entertaining programming TV demand, mobile communications and high bandwidth Internet data access demand. The industry is inserting novel methodology into satellites at fast pace.

In the secure communication is when two objects are communicating each other and they do not want this communication listen by another person. Secure communication conclude means through which user can be share knowledge with varying certainty degrees that another parties cannot interrupt what was said. Watermarking methods advanced for information cannot be straight useful to satellite images because the analytic data integrity, rather than perceptual feature, is of primary significance. Hence satellite images need effective watermarking systems. The encryption procedure is useful in confirming certain security types for example confidentiality, integrity, authentication and identification of data. For attaining above mentioned types, appropriate cryptographic method combination is essential [3].

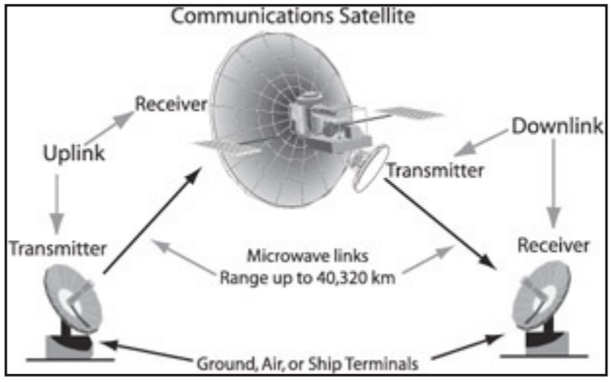


Figure 1: Satellite Image Communication

Discrete Wavelet Transform (DWT)

The DWT is sub-band coding based, is generate to yield a Wavelet Transform fast computation. It is easily to generate and computation time decreases. The size N1 x N2 of 2-D DWT of image functions (n1,n2) can expressed as [4]

$$W_{\varphi}(j_0,k_1,k_2)=\frac{1}{\sqrt{N_1N_2}}\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}s(n_1,n_2)\varphi_{j_0,k_1,k_2}(n_1,n_1)$$

$$W_{\varphi}(j_0,k_1,k_2)=\frac{1}{\sqrt{N_1N_2}}\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}s(n_1,n_2)\Psi^{i}{}_{j_0,k_1,k_2}(n_1,n_1)^{(1)}$$

(2)

Where i = {H, V, D} indicate the wavelet function direction index. As in 1-D case. Shows any initial scale, which may treat as =0. Above two different equations are 2-D DWT.

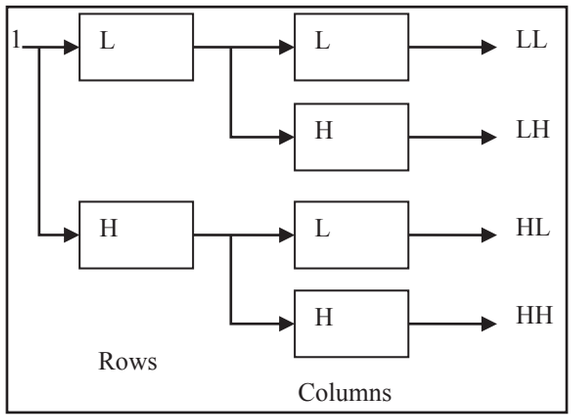


Figure 2. Discrete Wavelet Sub-band Decomposition

The DWT [4] comparing another transforms is characteristics of frequency or time used in various application fields. The DWT Sub band flow chart for digital image is present in figure 1, where L represents to component of low frequency, H represents to high frequency represents to decomposition level of the DWT. The sub image LL is element of low frequency, it is the approximate usual image sub image; sub image HL is the low frequency component in horizontal course and high in direction of vertical, it manifests long-established image horizontal side. LH sub image is high frequency factor in horizontal course and in the vertical direction, it manifests original image vertical edge; sub image HH is component of high frequency, it manifests original image oblique edge. It is present that original image energy is contained in the LL2 low frequency region.

DWT is based on the specific time and varying frequency is small waves [2]. This is the method frequency domain in which initially transformed cover image into frequency domain altered in accordance with transformed watermark watermarked image and coefficients is found which is the most robust. It decomposes an image in essentially three spatial directions, i.e., horizontal, diagonal and vertical in the outcome separating an image into different components that is LL, HL, LH and HH. Here the first letter refers to using either frequency of the low pass operation or frequency of the high pass operations to rows and other letter refers to filter valuable to the cover image columns.

_ LL level is the lowest resolution level, which conclude of the approximation cover image part,

_ Rest three levels, i.e. HL, LH, HH presents the full cover image knowledge.

Decomposition is another level in any one sub-band is selected and is additional decomposed into four levels. Maximum the decomposition level, watermarked image is in maximum strength. At all decomposition levels, the DWT magnitude coefficients are higher in lower bands (LL), and are smaller in three bands (LH, HL, and HH). The larger wavelet coefficient magnitudes present their advanced importance in comparison with smaller magnitude wavelet coefficients. HVS (Human Visual System) is additional sensitive to the low frequency parts (the LL sub-band), so the watermark is rather placed in other three sub-bands to retain the original image value.

The DWT is applied on the host image to decompose the image into four non overlapping multi resolution coefficient sets. The coefficients are [28]:

$$W_{LL}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}g(x)g(y)W_{LL}^{J-1}(2u-X)(2v-y) \quad (3)$$

$$W_{LH}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}g(x)g(y)W_{LL}^{J-1}(2u-X)(2v-y) \quad (4)$$

$$W_{HL}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}g(x)g(y)W_{LL}^{J-1}(2u-X)(2v-y) \quad (5)$$

$$W_{HH}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}g(x)g(y)W_{LL}^{J-1}(2u-X)(2v-y) \quad (6)$$

Where J is the level of the 2-D DWT, h (n) and g (n) are the impulse response. Figure 6 shows the schematic diagram of 2D wavelet transform. By using this figure we can analyses in which way the 2D wavelet transform are performed.

Discrete Cosine Transform (DCT)

The excellent and still most prominent space for picture preparing is that of DCT. The DCT permits an image to be separated into distinctive frequency groups, creating it much simpler to embed watermarking information into the center frequency picture groups. The center frequency groups are picked such that they dodge the most visual imperative parts of the picture (low frequencies) without over-presenting themselves to support by compression and noise attacks. One such procedure uses the center band DCT coefficients to encode a solitary bit into a DCT square [5].

The most common DCT definition of a 1-D sequence of length N is [27]:

$$c(u)=a(u)\sum_{x=0}^{N-1}f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (7)$$

For u=0, 1, 2, 3...., N-1. Similarly, the inverse transformation for 1-D sequence of length N

Is

$$f(x)=\sum_{u=0}^{N-1}a(u)c(u)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (8)$$

For both the equations α (u) is defined as

$$x(u)=\begin{cases}\sqrt{\frac{1}{N}}, & u=0\\ \sqrt{\frac{2}{N}} & u=0\end{cases} \quad (9)$$

In DCT the first transform coefficient is DC coefficient and all others are AC coefficients. The 2-D DCT transform is extension of 1-D DCT and is given by [16]:

$$c(u,v)=a(v)a(u)\sum_{u,v=0}^{N-1}\sum f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (10)$$

For u, v=0, 1, 2, 3....., N-1 and α (u) and α (v) defined in equation (3). The 2-D DCT inverse transforms is given by:

$$f(x,y)=\sum_{u,v=0}^{N-1}\sum a(v)a(u)c(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (11)$$

Median Filter

Median filter is a nonlinear digital filtering technique, often used to the remove noise. The common concept of median filter is run through signal entry by entry, eliminating every entry with neighbouring entries median. Note that if window has an odd number of entries, then median is simply to define: it is just middle value after all entry in window are sorted numerically. For an even various entries. The median filter is a non-linear digital filtering method [30]. It is regularly used to eliminate noise. It is best used for eliminating salt and pepper noise and impulse noise. In median filter, each entry is supplanted with the middle of the neighboring sections. The example of neighbors is called window, its inside is moved entry by entry, supplanting every section with the middle of neighboring pixels.

Function examines an $N \times N$ matrix centered on all matrix cell, discovers N by N cells median value, and replaces the value of central cell with median value.

For example

$$\begin{pmatrix}2345\\3456\\4567\\5678\end{pmatrix}$$

Source matrix:

For a 3 X 3 filter matrix, centered on cell (2,2), the matrix is:

$$\begin{pmatrix}2 & 3 & 4\\ 3 & 4 & 5\\ 4 & 5 & 6\end{pmatrix}\rightarrow(\widehat{2,3,3},4,4,\widehat{4,5,5},6) \quad (12)$$

The median value of the filter matrix is 4; therefore cell (2,2) in output matrix remains 4.

When using filtering to source matrix edge the filter may fall matrix outside. Here we can area pad the outside source matrix with zeros (Zero Padding), through reflection padding (Map Padding), or through repeating edge values (Repeat Padding) [6].

Spatial Median Filter is a new noise elimination filter. Spatial Median Filter growth results quality, a different parameter will be presented and experimental data is present demonstrating the amount of improvement. The Spatial Median Filter is a smoothing procedure with eliminating noise purpose and image data fine points while maintaining edges around larger shapes [7].

RSA Cryptography

A new cryptography, ideas to upturn encrypted cloud data security in the cloud servers with minimum consumption of cost and time at both decryption and encryption processes. In this algorithm, the various proponents will be increased to three. The two different Key Generation Encryption Algorithm has the succeeding steps:

Key Generation Procedure [8]

1. Select two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculated: phi (n) = (p - 1) (q - 1).
4. Select an integer e such that 1<e<phi(n)
5. Compute d to satisfied the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.
6. The public key is (n, e) and private key is (n, d). Keep each values d, p, q and phi secret.

3.1.2 Encryption

Plaintext: P < n

Cipher text: C= Pe mod n.

3.1.3 Decryption

Cipher text: C

Plaintext: P=Cd mod n.[8]

Literature Survey

Panduranga H T (2013) et al present, defines a selective image encryption concept in two different ways. First technique divides a single image into sub blocks, then particular blocks are useful to encryption procedure. Second technique automatically detects objects positions, and particular objects are useful to encryption procedure. On sattilight and medical image [9].

Abdullah Sharaf Alghamdi (2011) et al present a technique for satellite imagery encrypt and decrypt in order to securely transmit it at the time of war. The methodology used here for encrypt and decrypt process is that of chaotic maps. The research work is carried out through applying the Henon and logistic maps [10].

Boukhatem Mohammed Belkaid (2015) et al present, securing Meteosat images transmission on Internet, in local or public networks. To increase the Meteosat transmission security in communication of network, an advance encryption algorithm based on AES and RSA algorithms is proposed [11].

Ashkan Masoomi (2013) et al present a new model to the correct or detect Single Event Upsets in on-board AES algorithm implementations, which is based on Hamming error correcting code. The encrypt satellite image can become corrupted before the ground station reaching because of numerous faults. One main faults source is the harsh radiation atmosphere, Therefore any electronic systems used on-board satellites for example processors, memories are most susceptible to faults induced through radiation. Single Even Upset (SEU) faults can happen on-board through encryption because of radiation [12].

M. Sithi Benazir (2015) et al present embraces a new encryption technique for satellite based images which are versatile composition combined. The encrypt for satellite images here image division consists into matrix and then, elementary column and row operations are considered. The results present performance improved in parameters variety. The grouping of common matrix form and elementary row operations yields good outcomes and improved image encryption techniques compared to present works [13].

Comparison of various cryptography algorithms

Table 1: Comparison of Various Algorithms on the basis of Different Parameters [14]

	DES	3DES	AES	RSA	BLOWFISH	TWOFISH	THREEFISH	RC5	ECC	IDEA
DEVELOPMENT	In early 1970 by IBM and Published in 1977.	IBM in 1978.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993	Bruce Schneier in 1998	Bruce schneier, Niels Ferguson, Stefan Lucks in 2008	Ron rivest in 1994	Victor Miller from IBM and Neil Koblitz in 1985	Xuejia Lai and James in 1991
KEY LENGTH (Bits)	64 (56 usable)	168,112	128,192, 256	Key length depends on no. of bits in the module	Variable key length i.e. 32 – 448	128, 192, 256	256,512, 1024	0 to 2040 bits key size(128 suggested)	Smaller but effective key	128
ROUNDS	16	48	10,12,14	1	16	16	For 256,512 key = 72 For 1024 key = 80	1 to 255(64 suggested)	1	8
BLOCK SIZE (Bits)	64	64	18	Variable block size	64	128	256,512 and 1024	34 , 64, 128(64 suggested)	Stream size is variable	64

	DES	3DES	AES	RSA	BLOWFISH	TWOFISH	THREEFISH	RC5	ECC	IDEA
ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attack	Key recovery attack, Side channel attack	Brute force attack, timing attack	No attack is found to be successful against blowfish	Differential attack, Related key attack	Improved Related-Key Boomerang attack	Co-relation attack, Timing attack	Doubling attack	Linear attack
LEVEL OF SECURITY	Adequate security	Adequate security	Excellent security	Good level of security	Highly secure	Secure	Secure	Secure	Highly secure	Secure
ENCRYPTION SPEED	Very slow	Very slow	Faster	Average	Very fast	Fast	Fast	Slow	Very Fast	Fast

PROPOSED WORK

Fig. 3: Watermark Embedding

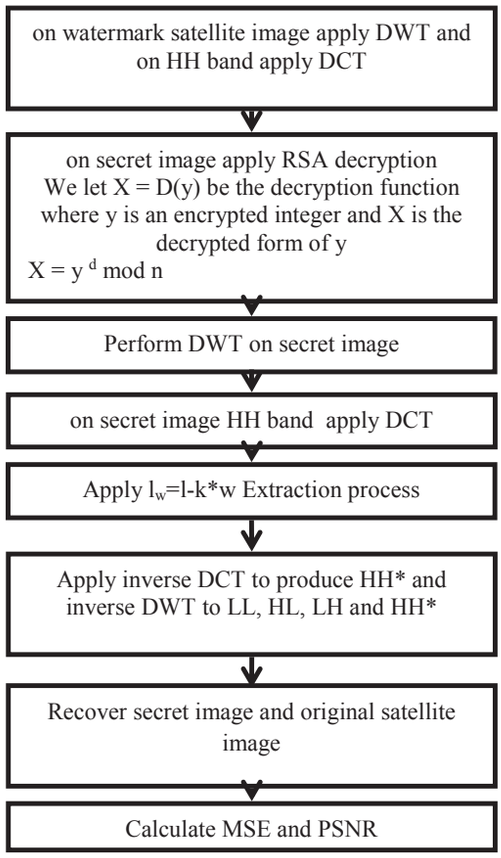


Fig. 4: Watermark Extraction

$l_w = l + k*w$

I - DCT transformed matrix of satellite image

W - DCT transformed matrix of secret image

k - Embedding strength varies from 0 to 1

Iw - embedded matrix

Result Simulation

Table 2. Base Work Encryption and Decryption Time

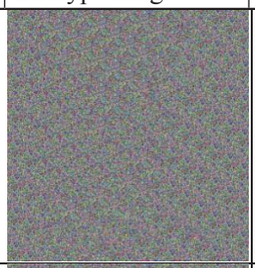
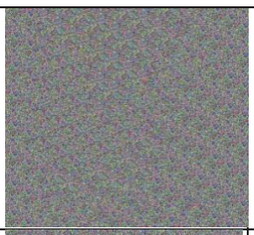
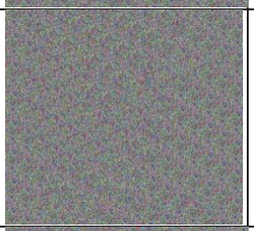
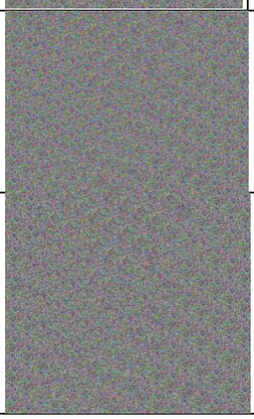
Original image	Encrypt image	Total time
		990247863 ns
		245678413 ns
		263651222 ns
		456328640 ns
		236825386ns
		438629348ns

Table 3. Proposed Work Encryption and Decryption Time

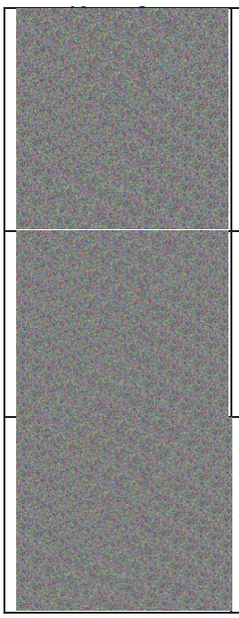
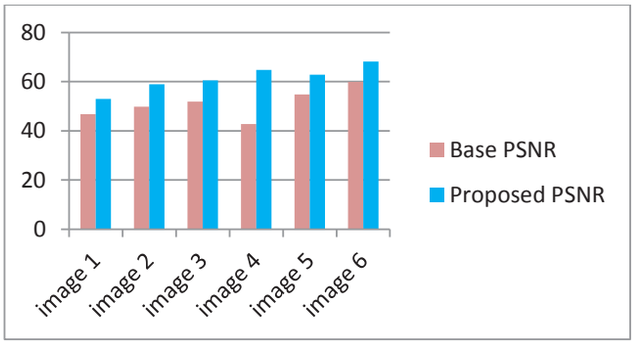
Encrypt image	Original image	Total time
		256432493 ns
		91711973 ns
		46546653 ns

Table 4. Comparison of Base and Proposed PSNR

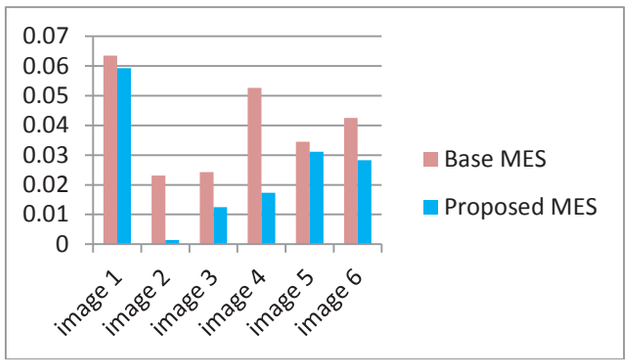
Image	Base PSNR	Proposed PSNR
1	46.746	52.947
2	49.826	58.911
3	51.836	60.524
4	42.764	64.837
5	54.847	62.846
6	59.947	68.132



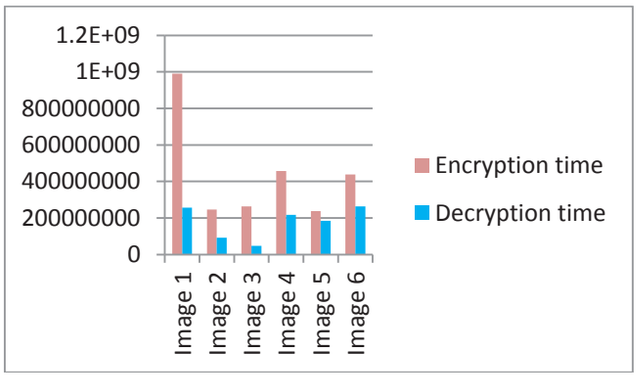
Graph 1. Comparison of Base and Proposed PSNR

Table 5: Comparison of Base and Proposed MES

Image	Base MES	Proposed MES
1	0.0635	0.0593
2	0.0231	0.0014
3	0.0243	0.0125
4	0.0526	0.0173
5	0.0345	0.0311
6	0.0425	0.0283



Graph 2: Comparison of Base and Proposed MES



Graph 3: Comparison of Base and Proposed Encryption and Decryption Time

Conclusion

Communication using satellite is a way to transmit digital data from various geographic location. Encryption procedure is useful in confirming various security features for example confidentiality, integrity, authentication and data identification. In this paper, for secure satellite image communication with the help of median filter for eliminate impulse noise, RGB image convert into an HSV image, satellite image using DWT for decompose into sub-bands LL, HL, LH and HH and apply DCT on HH band and RSA by for encryption purpose.

References

Vanzara, R. D., Sharma, P., & Bhatt, H. S. (2015). Satellite based data communication: A Survey. *International Journal of Electronics and Communication Engineering & Technology*, January, 6(1), 86-99.

Misra, D., Misra, D. K., & Tripathi, S. P. (2013). Satellite communication advancement, issues, challenges and applications. *International Journal of Advanced Research in Computer and Communication Engineering*, April, 2(4), 1681-1686.

Barukab, O. M., Khan, A. I., Shaik, M. S., Murthy, M. V. R., & Khan, S. A. (2012). Secure Communication using Symmetric and Asymmetric Cryptographic Techniques. *International Journal of Information Engineering and Electronic Business*, 2, 36-42.

Yatindrapathak., & Satishdehariya. (2014). A More Secure transmission of medical images by Two Label DWT and SVD based watermarking technique. *IEEE International Conference on Advances in Engineering & Technology Research*, August.

Nazmudeen, N. H., & Farsana, F. J. (2014). A new method for satellite image security using DWT-DCT watermarking and AES encryption. *International Conference on Innovations & Advances in Science, Engineering and Technology*, July, 3(5), 69-76.

Gupta, G. (2011). Algorithm for image processing using improved median filter and comparison of mean, median and improved median filter. *International Journal of Soft Computing and Engineering*, November, 1(5), 304-311.

Church, J., Chen, Y., & Rice, S. (2016). A Spatial Median Filter for Noise Removal in Digital Images". IEEE Southeast Conference, April.

Singh, G., & Supriya. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, April, 67(19), 33-38.

Panduranga, H. T. & NaveenKumar, S. K. (2013). Selective image encryption for Medical and Satellite Images. *International Journal of Engineering and Technology*, February-March, 5(1), 115-121.

Alghamdi, A., S., Ullah, H., Khan, M. U., Ahmad, I., & Alnafajan, K. (2011). Satellite image encryption for C4I system. *International Journal of the Physical Sciences*, September, 6(17), 4255-4263.

Belkaid, B. M., Mourad, L., & Mehdi, C. (2015). Meteosat images encryption based on AES and RSA algorithms. *International Journal of Advanced Computer Science and Applications*, 6(6), 203-208.

Masoomi, A., & Hamzehiyan, R. (2013). A new approach for detecting and correcting errors in the satellite communications based on hamming error correcting code. *International Journal of Computer Theory and Engineering*, April, 5(2), 227-231.

Benazir, M. S., & Padmapriya, A. (2015). Elementary Matrix Operation Based Satellite Image Encryption. *International Journal of Advanced Research in Computer and Communication Engineering*, July, 4(7), 367-371.

Bhanot, R., & Hans, R. (2015). A Review and comparative analysis of various encryption algorithms. *International Journal of Security and its Applications*, 9(4), 289-306.