Naipunnya®
To reach the unreachable

Naipunnya Institute of Management & Information Technology

Affiliated to the University of Calicut, ISO 9001-2015 Certified
Accredited by NAAC with B++ grade

FACULTY ENHANCEMENT PROGRAMME

Date of event: 27/10/2022

Faculty In-charge: Ms. Midhula Sekhar

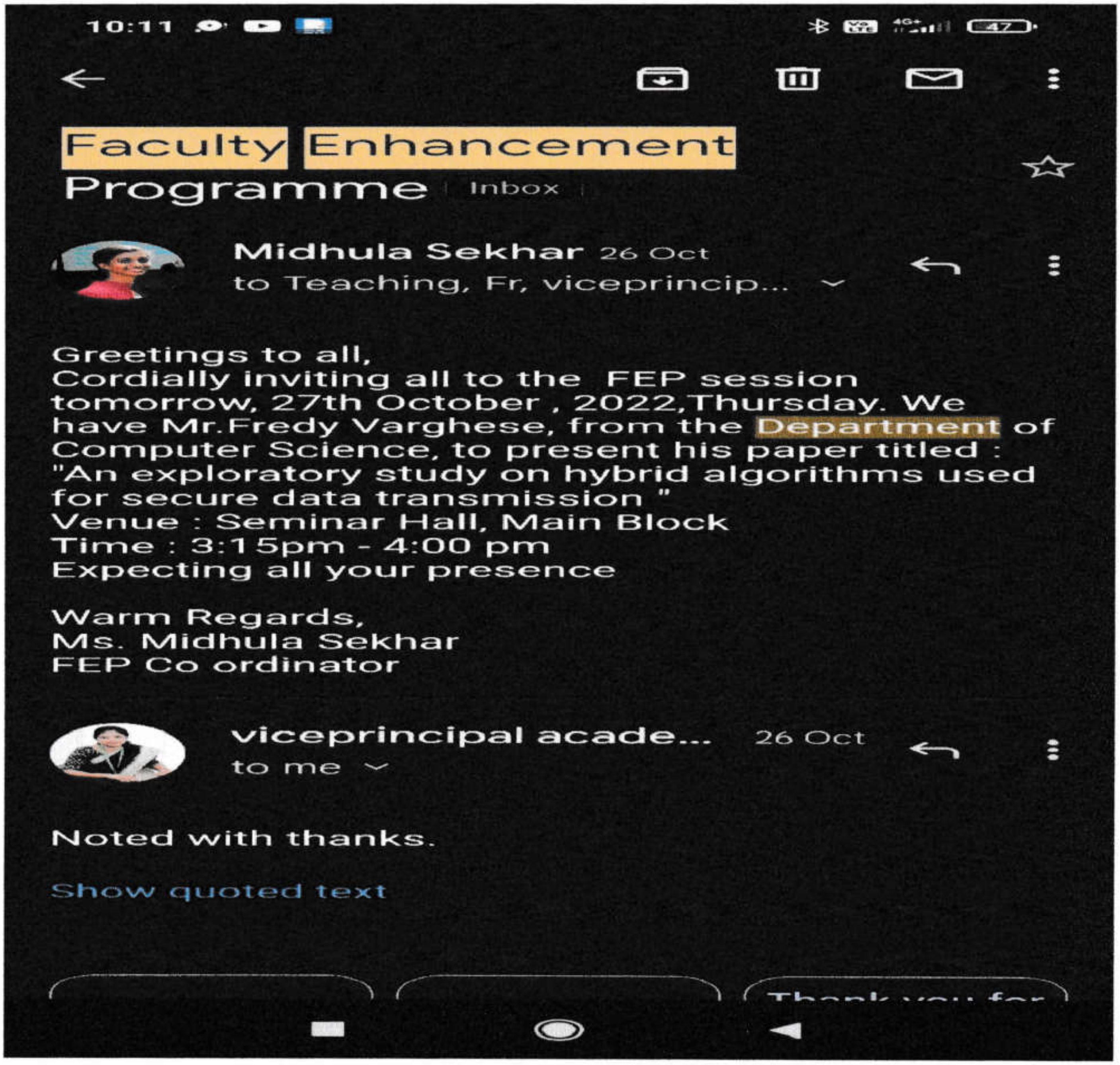
NAIPUNNYA INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY
Naipunnya
To reach the unreachable
Pongam, Koratty East
Thrissur District
Kerala-680 308

REPORT

The Faculty Enhancement Program for the month of October was conducted on 27/10/2022, Thursday at 3:15 pm at Seminar hall, Main block. Mr. Fredy Varghese of the Computer Science Department presented his paper titled "An Exploratory study on hybrid methods used for Secure Data Transmission". 44 faculty members from various departments attended the program. Dr Joy Joseph, Dr. Sabu Varghese, Dr. Sarika and Ms. Saritha raised queries and made the session more interactive. The program concluded at 4:00 pm with a thanks note by Ms. Midhula Sekhar, FEP Coordinator.

Prepared by:	Verified by:	Approved by:
Ms. Midhula Sekhar	Dr. Sabu Varghese	Rev.Fr. Dr. Paulachan K J
(Faculty In- charge)	(Director, IT/HRD Cell)	(Principal)

SCREENSHOT OF E-MAIL



Faculty Enhancement Programme

Midhula Sekhar 26 Oct
to Teaching, Fr, viceprincip...

Greetings to all,
Cordially inviting all to the FEP session tomorrow, 27th October , 2022,Thursday. We have Mr.Fredy Varghese, from the Department of Computer Science, to present his paper titled : "An exploratory study on hybrid algorithms used for secure data transmission "
Venue : Seminar Hall, Main Block
Time : 3:15pm - 4:00 pm
Expecting all your presence

Warm Regards,
Ms. Midhula Sekhar
FEP Co ordinator

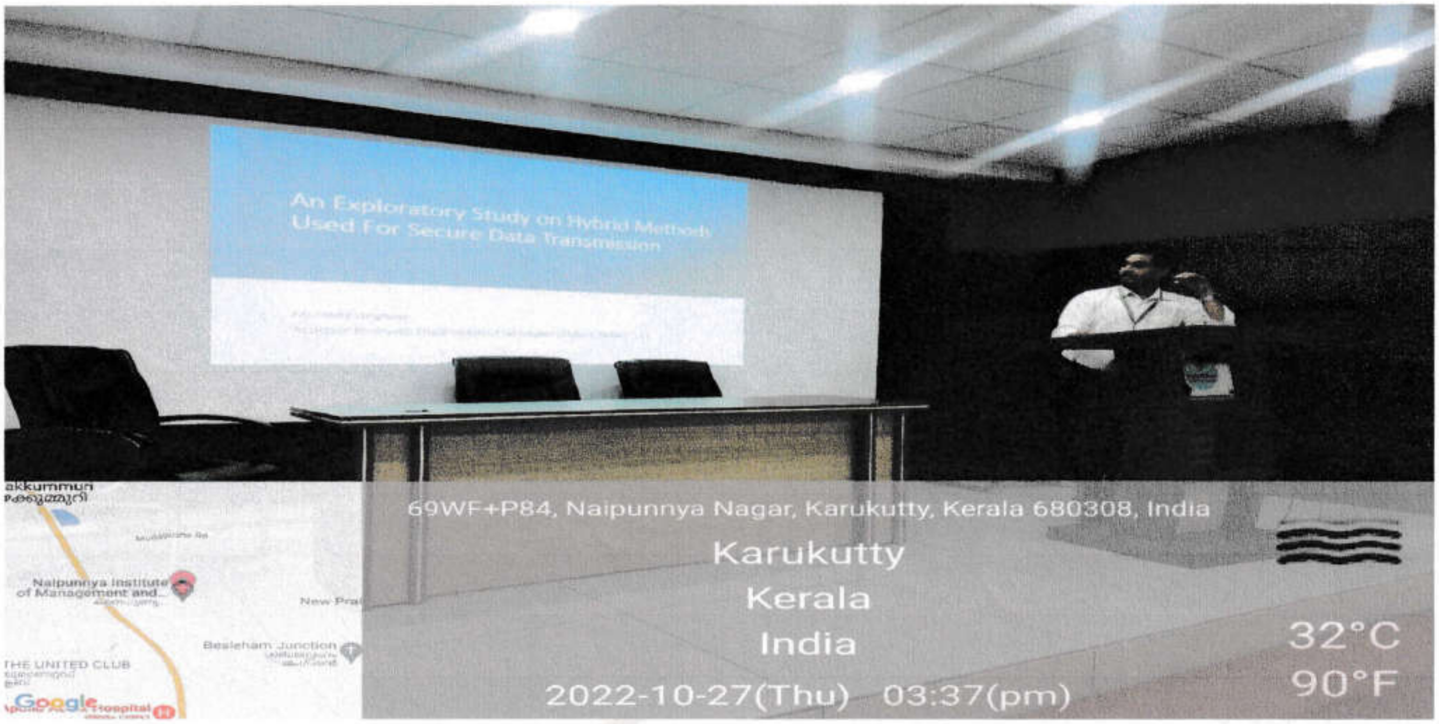
viceprincipal acade... 26 Oct
to me

Noted with thanks.

Show quoted text

NAIPUNNYA INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY
Naipunnya
To reach the unreachable
Pongam, Koratty East, Thrissur District, Kerala-680308

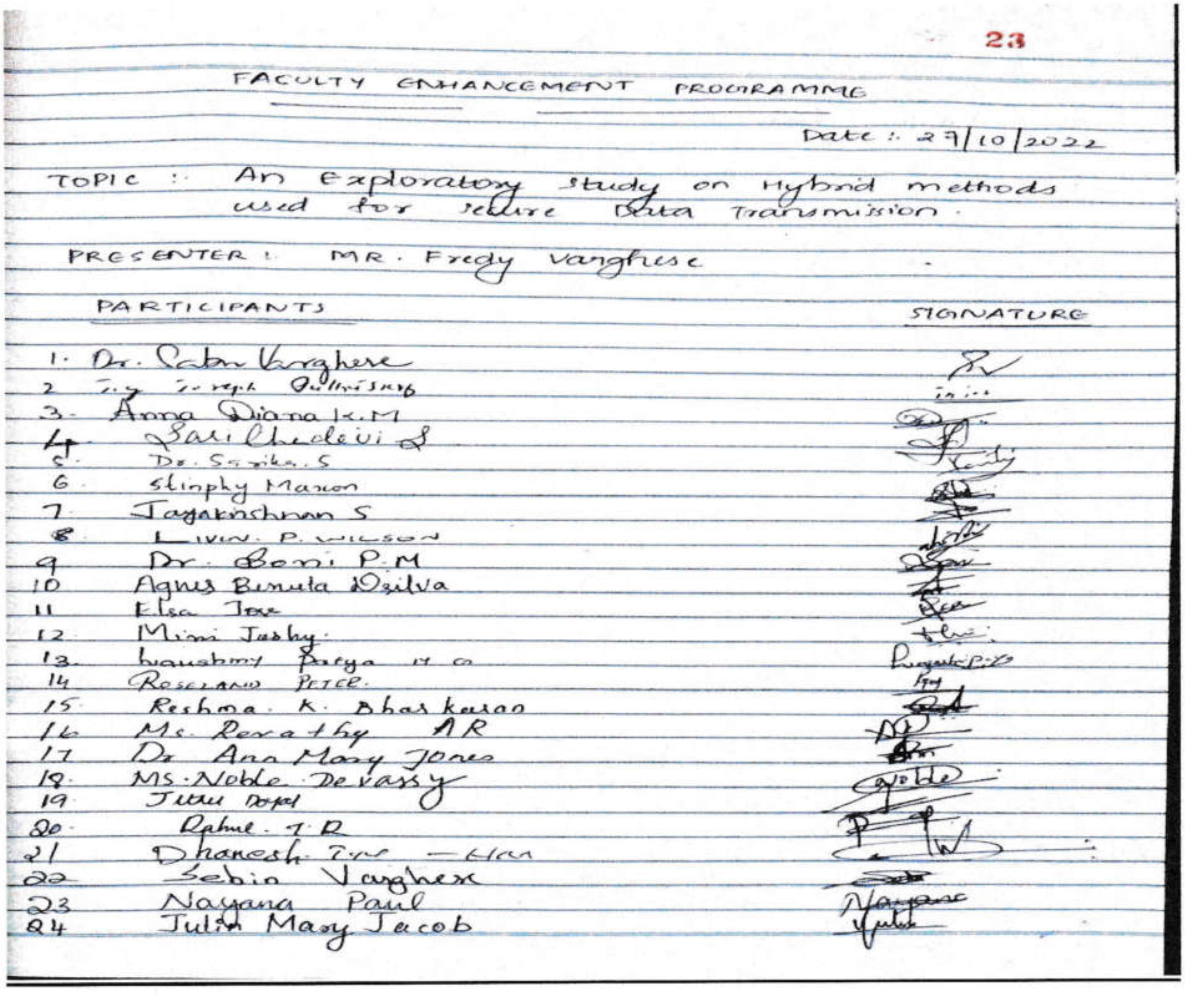
PHOTOGRAPHS /SCREENSHOTS


An Exploratory Study on Hybrid Methods Used For Secure Data Transmission
Naipunnya Institute of Management and...
Besleham Junction
THE UNITED CLUB
Google
69WF+P84, Naipunnya Nagar, Karukutty, Kerala 680308, India
Karukutty
Kerala
India
2022-10-27(Thu) 03:37(pm)
32°C
90°F

Naipunnya Institute of Management and...
Besleham Junction
THE UNITED CLUB
Google
69WF+P84, Naipunnya Nagar, Karukutty, Kerala 680308, India
Karukutty
Kerala
India
2022-10-27(Thu) 03:38(pm)
32°C
90°F

NAIPUNNYA INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY
Naipunnya
To reach the unreachable
Pongam, Koratty East
Thrissur District
Kerala-680 308

PARTICIPANT'S LIST



23

FACULTY ENHANCEMENT PROGRAMME

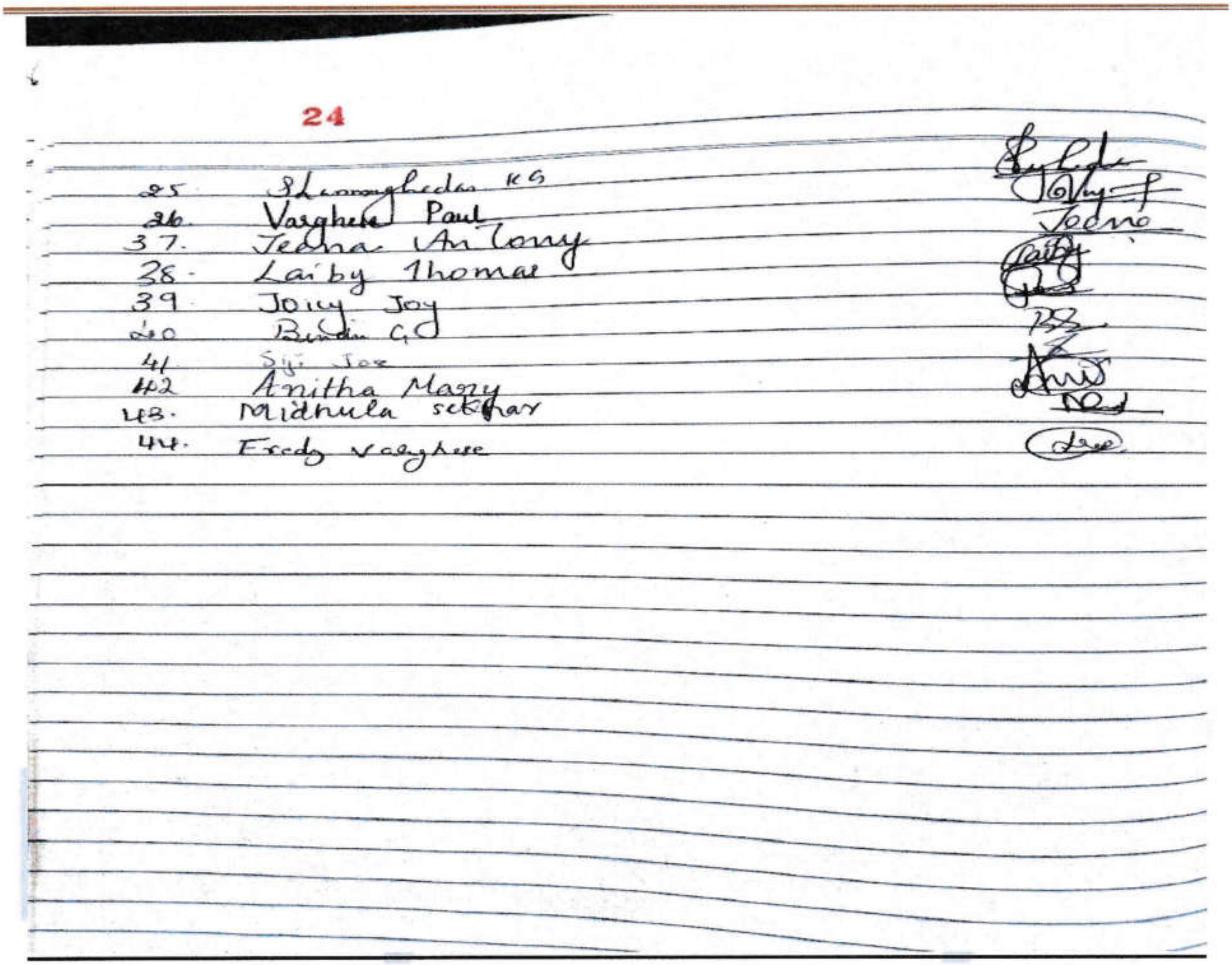
Date : 27/10/2022

TOPIC : An Exploratory study on Hybrid methods used for secure Data Transmission.

PRESENTER : MR. Fredy Varghese

PARTICIPANTS	SIGNATURE
1. Dr. Sabu Varghese	
2 Jiy Joseph Pulliyssery	
3. Anna Diana K.M	
4 Sarithadevi S	
5. Dr. Sarika. S	
6. Stinphy Maxon	
7. Jayakrishnan S	
8. LIVIN. P. WILSON	
9 Dr. Boni. P.M	
10 Agnes Benita D'silva	
11 Elsa Jose	
12. Mini Joshy.	
13. Lakshmy Priya M G	
14 ROSELAND PETER.	
15. Reshma. K. Bhaskaran	
16 Ms. Revathy AR	
17 Dr Ann Mary Jones	
18. MS. Noble. Devassy	Noble
19. Jithu Gopal	
20. Rahul. T. R	
21 Dhanesh. T.M — HOD	
22 Sebin Varghese	
23 Nayana Paul	Nayana
24 Julia Mary Jacob	

NAIPUNNYA INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY ★
Naipunnya
To reach the unreachable
Pongam, Koratty East
Thrissur District
Kerala-680 308



24

35	Shanmughadas KG
36.	Varghese Paul
37.	Jeena Antony
38.	Laiby Thomas
39.	Joicy Joy
40	Bindu G.C
41	Siji Jose
42	Anitha Mary
43.	Midhula sekhar
44.	Fredy Varghese

NAIPUNNYA INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY ★
Naipunnya
To reach the unreachable
Pongam, Koratty East
Thrissur District
Kerala 680 308

An Exploratory Study on Hybrid Algorithms Used For Secure Data Transmission

Mr.Fredy Varghese
Assistant Professor, Department of Computer Science Naipunnya Institute of Management and Information Technology, Pongam, Thrissur, Kerala 680308
E-mail:fredy@naipunnya.ac.in

Abstract

During last few decades, digital communication plays a vital role for various sectors such as healthcare departments, banking sectors, information technology companies, industries and several other fields. Nowadays, all data are transmitted over internet, which needs high protection for transmitting the original data from source to destination. In order to secure digital communication, cryptography and steganography methods are used to achieve data security over insecure and the open networks like internet. Cryptography is the method to encrypt the secret information in an unreadable structure. On the other hand, steganography is the technique to cover the secret data such as audio, image, text, and video. It can hide the message while transmitting the original information from one end to other end. In this paper, it gives an analysis based on the concept of cryptography and steganography. It also presents several data hiding approaches and its merits and demerits.

Keywords: Security, cryptography, steganography, data hiding.

1. Introduction

The fast progression of science and technology makes the task of data searching and transmission on the Internet much easier [1]. The digital multimedia documents including texts, images, videos and audios are more susceptible to hack due to the advancement of the internet. This problem increases the necessity of data security machineries for protecting the data from illegitimated access via shared medium. Nowadays, the cryptography and data hiding approaches play an important role in data security machineries. In cryptography, the secret data is converted into a cipher text without any meaning and hence it allows the authorized user to decrypt the data [2]. However, the meaningless of the transmitting message indicates the presence of secret info in the message and hence it is susceptible to unauthorized persons to decode the secret data. Alternatively, data hiding approaches conceal the secret information into multimedia files that reduce the doubt of the presence of secret data [3].

One of the famous methodologies employed for the protection of secret data is known as data hiding. This hiding approach utilizes distinct media (e.g. digital images, audio and video files) as cover elements for hiding secret data to generate stego-media [4]. A secured transmission system allows the transmitter to embed the data and the receiver to extract the data. The digital images are broadly utilized on the internet for different applications. Hence, one can utilize the digital images to make secure transmission. The data hiding approaches are utilized in the applications of military and medical data transmission for avoiding the third-party intervention or foraging [5].

For providing more data security, cryptography is utilized together with steganography technique. Both methods play an important part in information security. The encryption process is needed to be performed when the sensitive data is transferred from one device to another. This encryption technique helps to protect the data from hackers [6-7]. Some of the main goals of cryptography are integrity, authentication and confidentiality. Then, steganography process hides the encrypted data so that nobody can suspect that there exists a secret data. The Steganography approach seems to be a good one if it considers three parameters for processing which means capacity, security and image quality. Cryptosystem is required to implement a cryptographic method specifically for security services. The basic block of secure data transmission that used both cryptography and steganography is illustrated in Figure 1.

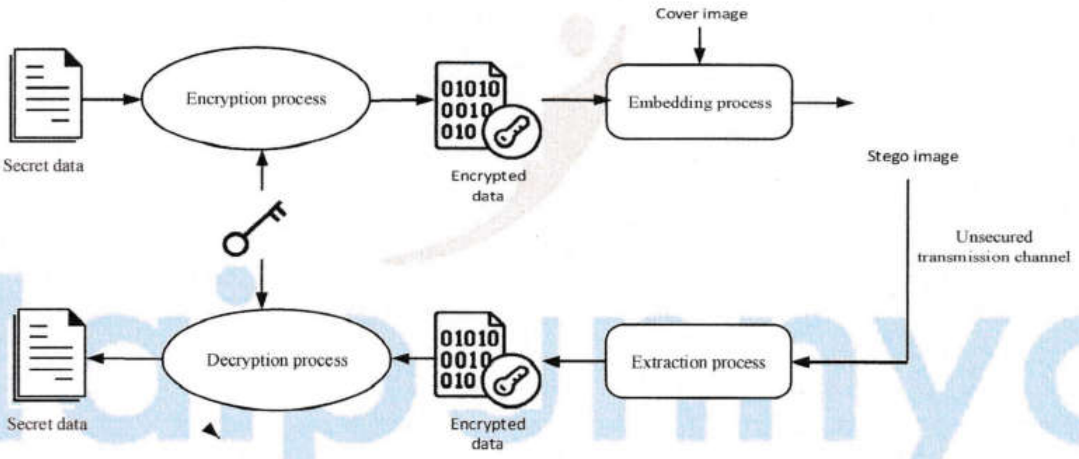


Figure 1 Secure data transission based on intelligent cryptosystem and data hiding process

1.1 Cryptographic algorithms

Cryptography keeps the transferred data more secure in a scientific way. A data encryption is provided by this approach to make secure transmission. Here, the data is encrypted before the transmission and the encrypted data is decrypted after the reception. Cryptography uses secret key to generate cipher text from the plain text and this ciphering approach marks the plain text as unreadable format. Hence, the deciphering process can be performed only by the person who hold the secret key [8-10]. Cryptographic methods can be categorized as symmetric key and public key methods. In symmetric key method, a single key is used to perform both encryption and decryption task [11].

The speed of Symmetric encryption is high even for huge numbers of data as images. But their usage is limited due to the problems of key management and distribution. The key might be intercepted by the adversaries while distributing the key in the network at the time of transmission. Furthermore, the number of keys will be incremented intensely while increasing the number of users, which signifies a trouble on the network. To tackle this issue, an asymmetric key encryption approaches have been developed. They utilized two distinct keys: public key and private key [12-13]. Here, the public and private keys are used for encryption and decryption processes respectively. The derivation of private key from the public key is not an easy task. However, the public key/asymmetric key encryption methods cannot be used for transmitting long-length data. Also, they provide lesser efficiency while handling with random length messages. This issue can be tackled by the use of randomly selected keyed symmetric encryption for encrypting the data and by the usage of a public key encryption method for encrypting the key utilized in the symmetric encryption method. This approach is named as the Hybrid encryption (HE) method [14-15].

Generally, the cryptographic systems use block encryption methods including Data Encryption Standard (DES), Advanced Encryption Standard (AES) and other systems. But the conventional encryption approaches faced complications in scrambling huge quantity of data. Chaos holds several natural relationships with cryptography due to its randomness in nonlinear systems. Chaos system offers a suitable source incredibly to generate abundant pseudo-random sequences and construct nonlinear encryption mechanisms as well [16]. Hence, huge amount of keys can be generated rapidly with the use of chaotic systems. The security of any block cipher system is heavily influenced by S-Boxes (substitution boxes) because this is the nonlinear element in a block cipher system. Applying chaotic system for generating S-boxes and applying them to image encryption is the most promising field of chaos system.

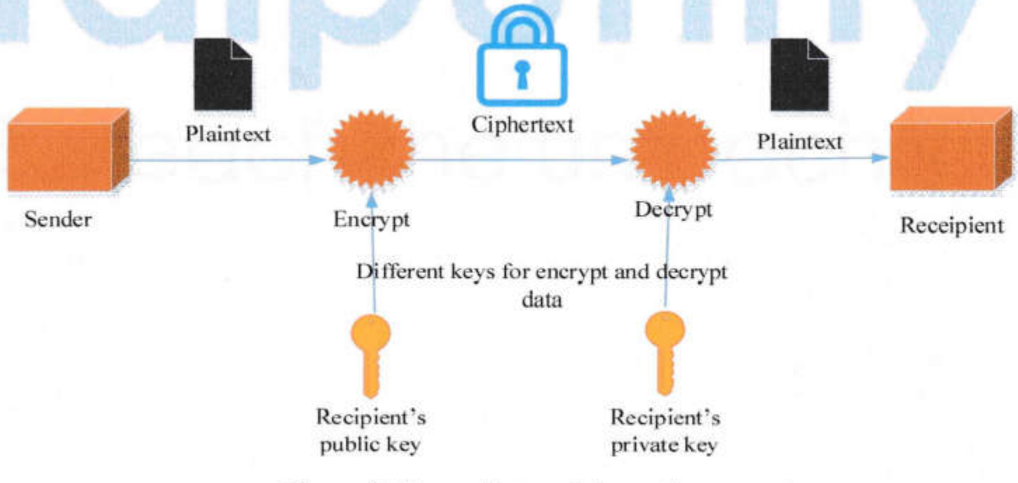


Figure 2. Encryption and decryption process

1.2 Steganography algorithms

Steganography methods embed significant data into regular files for enhancing the security of transmitting data [17]. The secret data is embedded into selected cover image for obtaining the stego-image. The cover and stego-images are identical to each other and hence an unauthorized person is unaware about the presence of secret data on stego-file. Hence, it allows safe transmission between the transmitter and receiver [18]. Generally, the steganography methods such as least significant bits (LSB) conceal equal number of secret bits into each pixels of cover image [19-20]. Hence, they cause equal degree of embedding distortion in the cover image. But, the individual pixels of any digital image exhibit complex statistical dependencies between them. Thus, the quality of image is automatically reduced while performing equal number of bits changes in all pixels of cover image. One of the most popular adaptive embedding process is pixel difference histogram (PVD) steganography [21]. This method embedded more secret data into edge portions and less data into smooth portions. But, the pixel difference histogram (PDH) analysis could attack the PVD methods.

In the last few decades, research priority of adaptive steganography has abruptly increased because of its greater undetectability. Nowadays, the steganography approaches are developed by minimizing the additive distortion that allocates an adjustment cost for every cover element and describes the distortion function by summing cost of all the cover elements. Data hiding method can be categorized as reversible data hiding and non-reversible data hiding based on restoration ability of the original image. The non-reversible data hiding approach allows the receiver to extract secret data alone. Hence, the receiver can't use the stego-image for any other purposes due to the distortion of significant data in the image. Alternatively, reversible data hiding method recover both the secret data and original version of cover image. Hence, it can be applied for wider range of applications than that of non-reversible method [22-23].

Furthermore, the data hiding method that generates single stego-image has very less embedding capacity. Hence, the embedding capacity can be improved by producing two stego- images. The data hiding method that generates two stego images are named as dual data hiding method. The total number of bits that are saved in one pixel is represented as embedding rate (stated as bpp). Alternatively, the total number of bits that are inserted into entire image is termed as embedding capacity. When the secret data is embedded into cover image, the visual quality of the cover image will be automatically decreased. Peak signal to noise ratio (PSNR) and structural similarity index measurement (SSIM) metrics are utilized for measuring the visual quality changes.

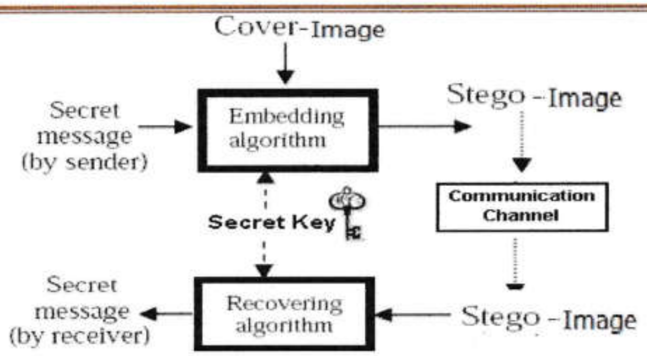


Figure 3 Steganographic approach

2. Literature review

Individually cryptography and steganography provides confidentiality to the data but they have some vulnerability. So as a third option we can go for a combination of cryptography and steganography. Some of the recent research works related to the secure data transmission using hybrid approach to data hiding in image processing are listed as follows:

Patani et al [25] proposed a 3-bit LSB method to embed secret data into cover image. Also, ECC algorithm has been utilized for keeping the data more secure while transmitting the stego images over internet. Wang et al [24] proposed a Compressed Sensing approach to perform joint selective encryption and data hiding for secure transmission. Here, the sign bits of the compressed sensing quantities have been specifically encrypted at the time of its quantization phase. Also, a non-separable histogram-shifting basis data embedding strategy has been proposed for inserting the authenticated data. Here, the sign encryption approach has been considered due to its randomness in Compressed sensing measurements based on random subspace projection.

Zhang et al [26] presented a new data hiding approach by considering a multidirectional line encoding (MDLE) and integer wavelet transform (IWT). Initially, IDWT has been used to separate the image into four wavelet sub-bands. Subsequently, the wavelet bands have been split into 3 ×3 coefficient blocks for exploiting the embedding portions. Then, MDLE model has been developed for embedding data into blocks of 3×3 sizes. In addition, an edge detection approach has been proposed for embedding more data in the edge portions of the image. Kadhim et al [27] proposed a DT-CWT based image steganographic method for embedding the secret data into the suitable coefficient planes of cover image. Here, a super-pixeling and intensity mapping approach have been introduced to increase the embedding capacity without causing any embedding error. The embedding error has been minimized by measuring the similarities of secret data and DT-CWT planes through template matching. They adopted machine learning models to select the optimal cover coefficient planes. The embedding process also generates a secret key to make support for the retrieval of secret data at the receiver.

Zhang et al [28] proposed a spatial image adaptive steganography approach on the basis of Zernike moment. Initially, the cover image has been processed to obtain its Zernike moment. After that dithering process has applied to get alternative cover image. They used Spatial Universal Wavelet Relative Distortion (S-UNIWARD) and syndrome-trellis codes for minimizing the distortion of embedding process. At last, the Zernike moment has been changed based on the altered amplitude of cover image to get stego image. Yeung et al [29] minimized the flipping distortion over the measurement of local texture pattern (LTP) to construct a variable STC code in binary image steganography

Jiang et al [30] proposed an encrypted image-based data hiding (EIRDH) algorithm with homomorphic public key cryptosystem. Here, the image has been encrypted using Paillier homomorphic public key cryptosystem. Also, the cover pixels have been exploited based on difference expansion (DE) approach for the construction of pairs of pixels to hide data. Bhardwaj et al [31] developed a block basis joint EIRDH method that performs the embedding process by considering m secret bits for each block. This improved the embedding rate and visual quality as well. Shaji et al [32] proposed an RDH approach based on dual encoding with sequence folding for the generation of dual stego images. Here, the data has been encoded using two encoding tables which included the index and message intensity based code series. When the previous or following half portion of the encoding tables have coordinated with one another, the code series in the 2nd encoding table would have been folded. Moreover, the extreme intensity of the codes in both encoding tables should be positioned at the most succeeding end to perform folding process. This procedure has been imitated for entire message intensities. Finally, the encoded data has been embedded into cover image to get dual stego images.

Lu et al [33] proposed a JPEG steganographic approach on the basis of auto encoder with flexible Bose-Chaudhuri-Hocquenghem (BCH) encoding. Initially, the autoencoder has been pretrained for fitting the conversion relations among the original and compressed JPEG image. Furthermore, BCH has been flexibly used based on the content of the cover image for decreasing the error rate while extracting the secret data. In addition, the robustness and statistical security have been improved due to the adjustment of Discrete Cosine Transformation coefficients on the basis of the real-time properties of JPEG channel. Lu et al [34] analysed and encoded the secret information by regulating the level of pixel distortion based on two factors namely, NC and MXD. The number of codes required for re-encoding a secret data has been controlled by the factor NC. As a result of this, the amount of code combinations has been limited. Furthermore, the distortion level of every code combination has been specified using

MXD factor. The occurrences of the secret numeric messages were used to assign a digital combination pairs for improving the encoding efficiency.

References	Method	Contribution	Advantages	Disadvantages
Patani et al [25]	Steganography and cryptography	3-bit least significant bits for embedding; ECC algorithm for data security	It improved the security level.	Degrade the stego image quality because it conceal equal number of secret bits into each pixels of cover image.
Wang et al [24]	Steganography and cryptography	Compressed sensing based sign bits encryption; non-separable histogram-shifting based data hiding	Robust against known error concealment attacks.	It degraded the visual quality level while considering image application.
Zhang et al [26]	Steganography	Introduced edge detection approach to embed different number of bits using MDLE	Improved visual quality of the stego image due to the embedding of more bits into edge pixels.	Not minimizing the distortion due to the lack of an efficient distortion cost analysis.
Kadhim et al [27]	Steganography	Introduced DT-CWT, super pixeling, intensity mapping, machine learning for optimised embedding	Reduced the embedding error using super-pixeling and intensity mapping	Extremely complex due to the stacking of more signal and image processing methods
Zhang et al [28]	Steganography	Zernike moment and Dither modulation for cover extraction; minimized distortion embedding using S-UNIWARD	Robust to scaling attack	S-UNIWARD embedded a single bit per pixel. Hence, the detection probability of such approach is increased.

Yeung et al [29]	Steganography	Local texture pattern (LTP) to minimize distortion	Improved embedding efficiency due to the use of STC coding	Not well supported for distortion minimization because LTP didn't consider the statistical characteristics of Uniform Embedding
Jiang et al [30]	Steganography and cryptography	Introduced EIRDH algorithm with homomorphic public key cryptosystem	Increased payload capacity.	Vulnerable to quantum attacks due to the recent improvements in quantum computers
Bhardwaj et al [31]	Steganography and cryptography	Symmetric key cryptosystem for data encryption and block based embedding	Increased visual quality and embedding rate	The key can be intercepted by the adversaries in Symmetric key cryptosystem. Didn't adjust the embedding probability in each and every element
Shaji et al [32]	Steganography	sequence folding for encoding the secret data and minimum index measurement for non-uniform embedding	Improved PSNR, SSIM and payload capcity	Security level is decreased due to the lack of proper cryptosystem and the detection probability of such approach is increased. Susceptible to different attacks.
Lu et al [33]	Steganography	Autoencoder with an adaptive BCH encoding	Provides statistical security.	The embedding is followed by an auto-encoder for image compression While this is extremely complex,

				for the comparison and record.
Lu et al [34]	Reversible data hiding	Controlled the level of pixel distortion using constant parameters	High payload capacity	Not suitable for all kinds of image due to the use of constant parameters. They control image quality.

Table1. Hybrid Methods and its merits and demerits.

Findings

Due to the advancement of technology, data protection is a major factor that cannot be compromised, which leads to multiple hybrid approaches. It clearly denotes the importance of security of data from the source to the destination from various attacks by the intruders. The existing approaches has their own merits and demerits which needs to be improved on every aspects. In future new techniques can be applied for the data protection and safe transmission along with the furtherance of technology.

Conclusion

Cryptography plays a major role to achieve the basic needs of security measures like confidentiality, no-repudiation, authentication and integrity. It has also involved in providing reliable, robust network, strong and data security. On the other hand, this review paper also includes the steganography process for data hiding while transmitting the information. The combination of both cryptography and steganography method has achieved a secure transmission of data with encryption and data hiding. According to this study hybrid approaches are the better choice for secure data transmission.

References

1. Wu, Shaofei, Mingqing Wang, and Yuntao Zou. "Research on internet information mining based on agent algorithm." *Future Generation Computer Systems* 86 (2018): 598-602.
2. Halunen, Kimmo, and Outi-Marja Latvala. "Review of the use of human senses and capabilities in cryptography." *Computer Science Review* 39 (2021): 100340.
3. Hassan, Fatuma Saeid, and Adnan Gutub. "Efficient reversible data hiding multimedia technique based on smart image interpolation." *Multimedia Tools and Applications* 79, no. 39 (2020): 30087-30109.
4. Kadhim, Inas Jawad, Prashan Premaratne, Peter James Vial, and Brendan Halloran. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." *Neurocomputing* 335 (2019): 299-326.

5. Tang, Zhenjun, Shijie Xu, Heng Yao, Chuan Qin, and Xianquan Zhang. "Reversible data hiding with differential compression in encrypted image." *Multimedia Tools and Applications* 78, no. 8 (2019): 9691-9715.

6. Almuhammadi, Sultan, and Ahmed Al-Shaaby. "A survey on recent approaches combining cryptography and steganography." *Computer Science Information Technology (CS IT)* (2017).

7. Rashmi, N., and K. Jyothi. "An improved method for reversible data hiding steganography combined with cryptography." In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 81-84. IEEE, 2018.

8. Elhoseny, Mohamed, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, N. Arunkumar, and Ahmed Farouk. "Secure medical data transmission model for IoT-based healthcare systems." *Ieee Access* 6 (2018): 20596-20608.

9. Harba, Eman Salim Ibrahim. "Secure data encryption through a combination of AES, RSA and HMAC." *Engineering, Technology & Applied Science Research* 7, no. 4 (2017): 1781-1785.

10. Reyad, Omar. "Text message encoding based on elliptic curve cryptography and a mapping methodology." *Information Sciences Letters* 7, no. 1 (2018): 2.

11. Malik, Manisha, Maitreyee Dutta, and Jorge Granjal. "A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things." *IEEE Access* 7 (2019): 27443-27464.

12. Yassein, Muneer Bani, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. "Comprehensive study of symmetric key and asymmetric key encryption algorithms." In *2017 international conference on engineering and technology (ICET)*, pp. 1-7. IEEE, 2017.

13. Dijesh, P., SuvanamSasidhar Babu, and Yellepeddi Vijayalakshmi. "Enhancement of e-commerce security through asymmetric key algorithm." *Computer Communications* 153 (2020): 125-134.

14. Çavuşoğlu, Ünal, Sezgin Kaçar, Ahmet Zengin, and Ihsan Pehlivan. "A novel hybrid encryption algorithm based on chaos and S-AES algorithm." *Nonlinear Dynamics* 92, no. 4 (2018): 1745-1759.

15. Ma, Lihong, and Weimin Jin. "Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography." *Optics Communications* 407 (2018): 51-56.

16. Nesa, Nashreen, Tania Ghosh, and Indrajit Banerjee. "Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map." *Journal of Information Security and Applications* 47 (2019): 320-328.

17. Saravanan, M., and A. Priya. "An Algorithm for Security Enhancement in Image Transmission Using Steganography." *Journal of the Institute of Electronics and Computer* 1, no. 1 (2019): 1-8.

18. Wazirali, Ranyiah, Waleed Alasmary, Mohamed MEA Mahmoud, and Ahmad Alhindi. "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms." *IEEE Access* 7 (2019): 133496-133508.

19. Heidari, Shahrokh, and Ehsan Farzadnia. "A novel quantum LSB-based steganography method using the Gray code for colored quantum images." *Quantum Information Processing* 16, no. 10 (2017): 1-28.

20. Banharnsakun, Anan. "Artificial bee colony approach for enhancing LSB based image steganography." *Multimedia Tools and Applications* 77, no. 20 (2018): 27491-27504.

21. Hameed, Mohamed Abdel, M. Hassaballah, Saleh Aly, and Ali Ismail Awad. "An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques." *IEEE Access* 7 (2019): 185189-185204.

22. Lu, Tzu-Chuen, Shi-Ru Huang, and Shu-Wen Huang. "Reversible hiding method for interpolation images featuring a multilayer center folding strategy." *Soft Computing* 25, no. 1 (2021): 161-180.

23. Yin, Zhaoxia, Youzhi Xiang, and Xinpeng Zhang. "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding." *IEEE Transactions on Multimedia* 22, no. 4 (2019): 874-884.

24. Wang, Jia, Leo Yu Zhang, Junxin Chen, Guang Hua, Yushu Zhang, and Yong Xiang. "Compressed sensing based selective encryption with data hiding capability." *IEEE Transactions on Industrial Informatics* 15, no. 12 (2019): 6560-6571.

25. Patani, Kinjal, and Dushyantsinh Rathod. "Advanced 3-Bit LSB Based on Data Hiding Using Steganography." In *Data Science and Intelligent Applications*, pp. 383-390. Springer, Singapore, 2021.

26. Zhang, Hua, and Liting Hu. "A data hiding scheme based on multidirectional line encoding and integer wavelet transform." *Signal Processing: Image Communication* 78 (2019): 331-344.

27. Kadhim, Inas Jawad, Prashan Premaratne, and Peter James Vial. "Improved image steganography based on super-pixel and coefficient-plane-selection." *Signal Processing* 171 (2020): 107481.

28. Zhang, Yue, Xiangyang Luo, Yanqing Guo, Chuan Qin, and Fenlin Liu. "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection." *IEEE Access* 7 (2019): 24282-24289.

29. Yeung, Yuileong, Wei Lu, Yingjie Xue, Junjia Chen, and Ruipeng Li. "Secure binary image steganography based on LTP distortion minimization." *Multimedia Tools and Applications* 78, no. 17 (2019): 25079-25100.

30. Jiang, Cuiling, and Yilin Pang. "Encrypted images-based reversible data hiding in Paillier cryptosystem." *Multimedia Tools and Applications* 79, no. 1 (2020): 693-711.

31. Bhardwaj, Rupali, and Ashutosh Aggarwal. "An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem." *Pattern Recognition Letters* 139 (2020): 60-68.

32. Shaji, C., and I. Shatheesh Sam. "Dual encoding approach with sequence folding for reversible data hiding in dual stego images." *Multimedia Tools and Applications* 80, no. 9 (2021): 13595-13614.

33. Lu, Wei, Junhong Zhang, Xianfeng Zhao, Weiming Zhang, and Jiwu Huang. "Secure robust JPEG steganography based on autoencoder with adaptive BCH encoding." *IEEE Transactions on Circuits and Systems for Video Technology* (2020).

34. Lu, Tzu-Chuen, Ting-Chi Chang, and Jau-Ji Shen. "An Effective Maximum Distortion Controlling Technology in the Dual-Image-Based Reversible Data Hiding Scheme." *IEEE Access* 8 (2020): 90824-90837.