International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Insight of Information Security: A Skeleton

Yash Shah, Soham Joshi, Parita Oza, Smita Agrawal

Abstract*: In this age of growing and developing information and technology, data security, integrity and confidentiality are essential aspects related to shared data over some network or medium. Many techniques over the years have been developed for securing the messages from attack or theft or breach of very sensible and essential data when shared over a network. The security threats to data have been ascending, so are the data hiding or securing techniques. This is where Information Security has a role to play. Development of techniques and methods that prevents the essential and secret data being stolen and thus providing security to the data. This paper discusses the significance of Information Security, its evolution since its infant stage and study about various subdomains of the same. This paper also shows a comparative study of various Information Security Techniques, their pros and cons and the applications in various domains. This paper analyses various Information Security methods or techniques based on their various characteristics and effectiveness on securing the data from any adversaries. This includes a study of some benchmark techniques and their subsidiaries along with it. The techniques under focus for analyzing were Watermarking, Digital Signatures, Fingerprinting, Cryptography, Steganography and latest being CryptoSteganography Information Security Technique. The characteristics focused were security-related properties, data or message-related properties, their objectives, drawbacks, applications and algorithms.

***Index Terms*: Information Security, Cryptography, Steganography, CryptoSteganography.**

I. INTRODUCTION

Information Security is the practice of avoiding or preventing any unauthorized access, its use, its disclosure, modification, analysis or inspection, or destruction of the information. In other words, Information Security is securing the information from any unauthorized or suspicious action, which can be harmful to the data as well as the organization taking care of that data. Information security and its growing development have been into existence since the era of information and communication. Its principle is to balance the integral three security triads – confidentiality, integrity and availability while keeping the focus on effective implementation of the techniques without hampering productivity and efficiency.

Manuscript published on 30 September 2019
* Correspondence Author
Yash Shah*, Information Technology, Institute of Technology, Nirma University, Ahmedabad, India.
Soham Joshi, Information Technology, Institute of Technology, Nirma University, Ahmedabad, India.
Prof. Parita Oza, Information Technology, Institute of Technology, Nirma University, Ahmedabad, India.
Prof. Smita Agrawal, CSE Department, Institute of Technology, Nirma University, Ahmedabad, India.

Preventing the data from theft, damage or altering from natural disasters, computer system/server malfunction or physical theft. Information Security has many areas wide open due to its spectrum of techniques and their development.

Information Security has evolved over the years developing various security techniques which are described further in this paper. [1]-[8] The specializations offered by Information Security can be named as securing networks, allied infrastructures, security applications and databases, security testing, information system auditing, penetration testing, record protection and discovery, digital forensics. Due to the inefficiency of the information security techniques, threats to information and data hiding has become overhead. The threats faced by the information sharing organization and the transmission medium are theft, software attacks which includes viruses, Trojans, phishing, malware protection and security, masquerading, denial of service, etc. For overcoming these, various techniques have been developed to secure the data. It all started with Caesar Cipher, The Enigma Machines, Asymmetric key Encryption, The Affine Cipher, Alphabetic Ciphers, Transposition Techniques, Substitution Techniques, Data Encryption Standards (DES), Advanced Encryption Standard (AES), Watermarking, Digital Signatures, Stream Ciphers, Cryptography, Steganography and CryptoSteganography. All the previous techniques have their pros and cons and their characteristics. This paper includes a detailed study of the significant Information Security Techniques and their sub-branches as well.

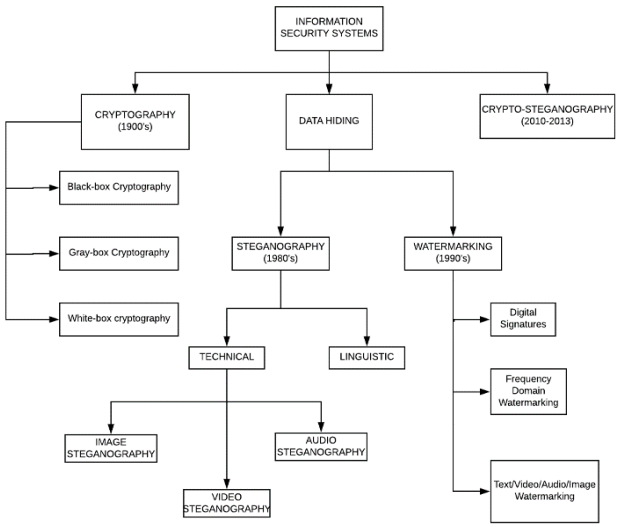

Fig. 1 Evolution of Information Security Techniques

Also, it describes the comparative study of these techniques with various attributes, making it easier for clarification based on the properties a technique possess and its characteristics.

II. TECHNICAL EVOLUTION OF INFORMATION SECURITY

In this section, we discussed the evolution of information security in detail. For better clarity, Fig. 1 shows the evolution of Information Security Techniques since their inception to till date.

A. Watermarking

Watermarking is assurance about the identity of the owner of the data. It holds the integrity and authenticity of the data. It can be a visible or invisible watermark. Watermarking does not hamper the original data; it changes the data (specifically an image, pdf or word file) so that you see some background without corrupting the image [1]. Visible Watermarks are generally logos or text that appears over an image or a file (pdf or doc). Invisible Watermark is for videos, images and audios where one cannot directly perceive. It can be extracted by different means. Audio watermarking techniques [2] highly emphasize on imperfections of the human auditory system. It exposes the fact that the human auditory system is insensitive to small amplitude changes concerning the time domain or frequency domain. Thus audio watermarking is performed and implemented by insertion of low amplitude or low-frequency signals by embedding them into audio waves. Watermarking is diagrammatically shown in Fig. 2.

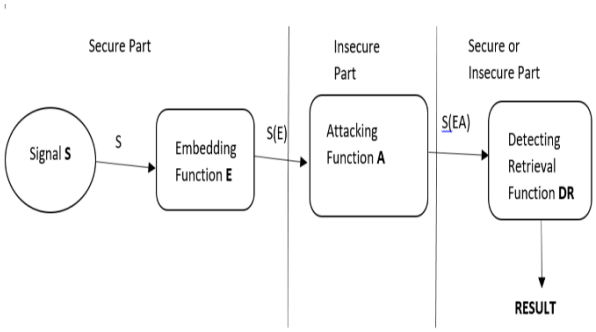

Fig. 2 Watermarking Technique

B. Digital Signatures

Digital Signature is signature-verifying algorithms, which checks the authenticity of the message. For this, message, public key and signature should be provided, and message will be accepted or rejected based on the verification [1]. Two things can be verified from digital signatures, firstly the correctness of private key [3] of the sender and second, the authenticity of the message. It can be used with any kind of messages like text, image or video so that receiver can be sure of the sender's identity. Digital Signature consists of certificate signing authority to check his/her authenticity. It automatically time-stamped so that the sender cannot easily repudiate later. A digital signature procedure is shown in Fig. 3

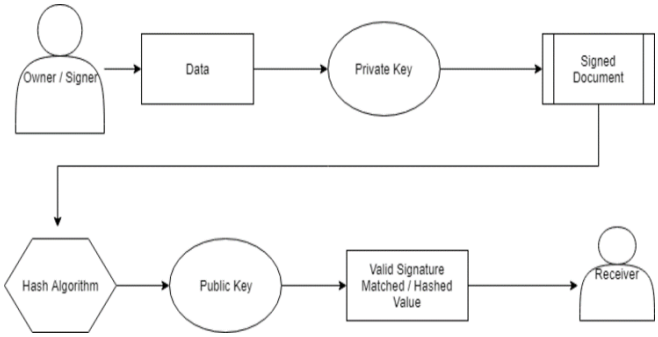

Fig. 3 Digital Signature Technique

C. Fingerprinting

A technique of taking each content and making it a unique one for protecting the data. It uniquely defines the identity of the sender or the receiver. Fingerprinting can be applied to any kind of data. It defines the confidentiality by the unique fingerprint a sender has on a data.

D. Cryptography

Cryptography is a technique of data hiding which transforms the original message into completely meaningless and nonsensical language. This requires some specific algorithms, which are Encryptions Algorithms, and corresponding Decryption Algorithms [3]. Cryptography ensures confidentiality, integrity, authentication and non-repudiation. Cryptography can be applied to text data. It is of two types: Symmetric key cryptography and Asymmetric key cryptography. Symmetric key cryptography deals with sharing only a single key or a private key between the two parties and data are shared over the same common key. Asymmetric key cryptography [4] deals with a public key between a sender and receiver, but each particular holds a private key of themselves. A message is operated as a bock of data or as a stream of data. Implementation techniques are converting plain text into cipher text (encryption) and on the receiver end, converting the obtained cipher text to plain text (decryption). These techniques are widely categorized into Transposition techniques, Substitution techniques and Product Techniques (the combination of both). Encryption and Decryption procedures are shown as in Fig. 4 and Fig. 5 respectively.

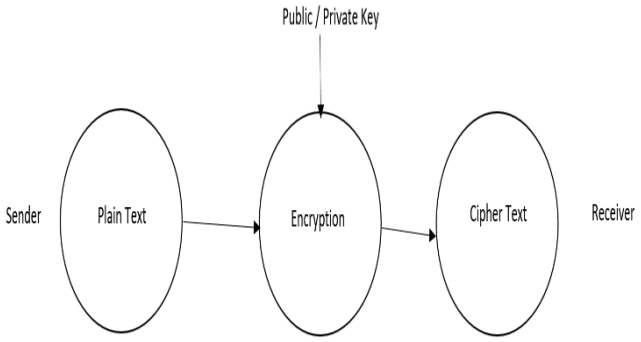

Fig. 4 Encryption in Cryptography Technique

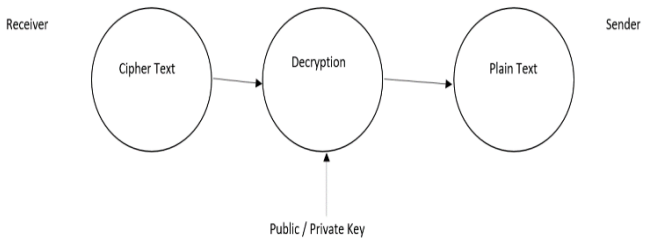

Fig. 5 Decryption in Cryptography Technique

E. Steganography

Steganography [5] does not change the data, but it hides the data under some cover (carrier) message. Therefore, it vanishes the very existence of the data being transmitted. It applies to text, image, audio and video type of data [5]. Steganography satisfies the need of the security triad that is Confidentiality Integrity and Availability.

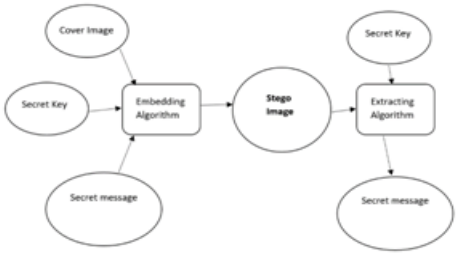

Fig. 6 Steganography Technique

In text steganography [5], [7], the text is embedded within a piece of another text such that it appears like a normal text when read by the third party. In image steganography [5], bits of images are substituted with the secret bits of the message. In video steganography [5], bits of frames are altered, and secret information is passed onto them. In audio steganography [5], the frequencies or amplitudes are altered, and data is transmitted over a network. All these techniques hide a secret message under some cover of higher frequency (bandwidth). Implementation techniques are LSB Insertion [8], Discrete Cosine Transform [9] and Spread Spectrum technique [10]. Many techniques are related to specific areas or domains of applications of Steganography. Steganography has three types. Secret key Steganography, where communication happens over a public network and dependent upon the secret key chosen by the communicating parties. Public Key Steganography [6], where the sender uses the receiver's public key and only receiver can recover the message using the corresponding private key. Pure Steganography [6], where no prior communication happens between the parties and relies on secrecy through obscurity. Here the key is not given or even decided between the communicating parties and extraction of a message from the given data or information is to be done by trial and error. Due to confusion and randomness of the message, it is discontinued in use. Steganography procedure is shown in Fig. 6.

CryptoSteganography

Cryptography is the art of hiding the messages by changing the message in order to introduce secrecy, while Steganography [8] is an art of hiding the existence of the message itself. CryptoSteganography [11] is an amalgamation of both these techniques for better Information Security. Implementation technique involves LSB (Least Significant Bit) insertion to embed encrypted messages into cover (carrier) files while MSE [11] (Mean Squared Error) and PSNR [11] (Peak signal-to-noise ratio) is used to acquire the quality of images. CryptoSteganography provides more security to the data and solves the problem of robustness and capacity. It provides two level security for the data, level one by cryptography (encryption) and level two by steganography (cover image diffusion). The Fig. 7 shows the procedure for CryptoSteganography.

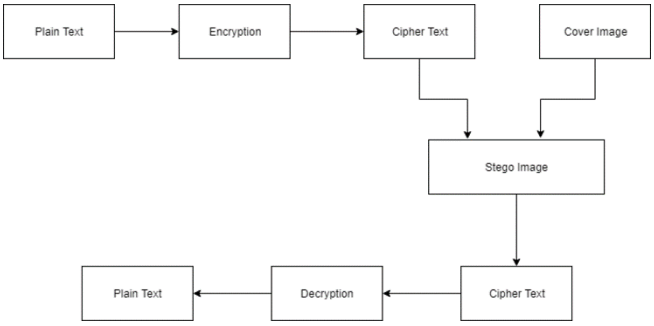

Fig. 7 CryptoSteganography Technique

III. COMPARATIVE STUDY OF INFORMATION SECURITY TECHNIQUES

The Table – I compares the techniques on the basis of confidentiality, integrity and availability capacity of the methods, which are generally known as CIA Triad of Information Security Services. [12] - [14]. Also, techniques are compared in the Table–I based on non-repudiation, authenticity and identity assurance of the owner, which are very important as a security aspect. [12] - [14]

Table I. Security aspects of various Information Security Techniques

INFORMATION SECURITY TECHNIQUES	Confidentiality	Integrity	Availability	Non-repudiation	Authenticity	Identity Assurance
Watermarking	-	√	-	-	√	√
Digital Signatures	-	√	-	√	√	-
Fingerprinting	√	-	-	-	-	√
Cryptography	√	√	-	√	√	-
Steganography	√	√	√	-	-	√
CryptoSteganography	√	√	√	√	√	-

Security techniques affect the data, as well. So a particular

technique can change the data into some unreadable text, or it can just hide the data under some cover file. The Table -II depicts the data related aspects of Information Security Techniques. [12] - [14]
All these techniques have some or the other drawbacks due to various reasons such as data, feasibility, forging, attacks, etc.

A technique can be identified upon its objective. Based on the objective(s), its sub-disciplines, sub-methods, or algorithms can be generated, invented or found. The Table-II and their drawbacks describes in Table-II [12] – [14]. Not only on technical aspects, but also on many other aspects, a technique / method can be classified, such as what outcome does it deliver, what is needed for encryption or for assuring the security of data, etc. The table gives an idea about these aspects described. [21][22][24]

describes the main objective(s) of the earlier discussed Information Security techniques and also what algorithms are used under each is mentioned. [21][22][23]

Table II. Comparison based of Information Security Techniques on Data related, Algorithmic and drawbacks aspect

INFORMATION SECURITY TECHNIQUES	Changes Data	Type of Data	Secret Data	Outcome / Output	Key / function required to secure the data	Objective	Techniques / Algorithms	Drawbacks
Watermarking	No	Image, Audio	Watermark	Water-marked image	Embedding function	Authentication of the owner of document	Visible and Invisible, Spatial domain and Fragile Watermarking	• Watermark size should be less than data size. • Watermark is embedded physically. Thus it is less secure.
Digital Signatures	No	Text, Image, Video	Digital Signature	Signed document	Public Key, Private Key pair	Authenticity, Time-stamping , Confidentiality	El-Gamal Algorithm, Schnorr Digital Signature Algorithm	• Do not preserve the view when a data is signed. • It does not show how data is represented, thus becomes less reliable.
Fingerprinting	No	Image, Video, Text	Fingerprint , Unique ID	Hashed data	Hash Functions	Authentication	Rabin's Algorithm, Cryptographic Hash Functions	• It can be duplicated or can be a fraud. • Cost and volume can be one of the factors.
Cryptography	Yes	Text	Plain Text	Cipher text	The public key, Private key pair	Data security	Transposition, Substitution, Stream, Block Ciphers	• Transforms the data, easily visible that some encrypted data is being sent. • Privacy depends only on the secret key, thus less security
Steganography	No	Image, Text, Video, Audio	Payload / Message	Stego image / text / audio / video	Embedding algorithm	Hiding the message	Discrete Cosine Transform (DCT) Spread Spectrum Technique (SST) Least Significant Bit (LSB)	• Once the existence of the message is detected, the message is compromised. • If exercised by wrong notions, it can bring devastating effects to the world.
Crypto-Steganography	Yes	Image, Text, Video, Audio	Text	Cipher text embedded on Stego data	Embedding algorithm along with the private key, public key pair	Security along with hiding the data	Implementing involves LSB technique and MSE [11] and PSNR [11] for quality of image	• Can be at risk if the private key is compromised, but chances are rare.

IV. APPLICATIONS OF INFORMATION SECURITY TECHNIQUES

A. Watermarking

1. **Image Watermarking [15]** – Inserting watermark directly into the message image or data image such as changing the color of the bits of the image to take advantage of perceptual properties or robustness of particular signal manipulations.

2. **Document Watermarking [15] –** This technique was developed to provide copyright under intellectual property rights for the electronic version of text documents, which are in a preformatted version where modification is done based on line spacing and margins between lines, characters, paragraphs, words etc.
3. **Graphics Watermarking [15] –** Watermark is directly embedded into the parameters set by MPEG-4 standards and can be extracted directly as well.
4. **Video Watermarking [15] –** It is to adopt the de facto standard for Video protection. A watermark is designed to manage the copy generations and the minimum data or information that a watermark must convey.
5. **Audio Watermarking [15] –** Mostly it is focused on directly watermarking or bit streaming of the data. Similar to video and image schemes, the use of a predefined set of rules and standards for the protection of audio.

B. Digital Signatures

A digital signature is used to authenticate an owner and to denote its ownership on the document. Uses include sending secure emails, also monitoring the transaction on the web platform. It is also necessary for the registration of patent and trademark.

C. Fingerprinting

Similar to watermarking and digital signatures, fingerprinting has applications based on protecting data integrity and confidentiality by a unique id or a fingerprint.

D. Cryptography

It is used in benchmark algorithms such as AES [16], DES [16], RSA [16], RC4 [16], Diffie-Hellman [16] and many more which uses encryption and decryption techniques for security of information. Apart from this, the real-time application of Cryptography includes:

1. **Message Authentication [16] –** By using an encryption algorithm, a message is converted to cipher text by the use of a private key and transmitted over a public channel.
2. **Time Stamping [16] –** It delivers the non-repudiation property of Cryptography. It denotes that the party at a certain point of time has sent a particular information document and communication happened. This process includes an algorithm known as Blind Signature Scheme that allows the sender to receive message acknowledged by the receiver without revealing any information.
3. **Electronic Money Transfer [16] –** This application has use of cryptography in both hardware and software components. Transactions of money over a publicly secure network happens without any risk because of the strength of Cryptographic algorithms used.
4. **Secure Network Communication [16] –** Secure Socket Layer (SSL) has been developed and implemented for providing security between TCP/IP.

It uses data encryption, server authentication, message integrity and client authentication for communication.

E. Steganography

1. **Business Domain [17] –** There are many methods prevailing, all boiling down to a desire for prevention of unauthorized access from becoming alert of the existence of the message. Steganography can be used to hide any sort of message that has prime importance, such as a chemical formula for the chemical industry, trade deals with partner industries or a message for a detective.
2. **Military Applications [17] –** Generally, these organizations have and need a high level of privacy. Thus they highly use these type of technology to prevent their message being illegally used. Military organizations use these for finding coordinates of militant camps, military camps, mines, suspicious tunnels and many more essential land sites. Terrorists use steganography techniques for coordinating between them and keeping their data secret. Also, they coordinate attacks using these techniques.
3. **Miscellaneous [17] –** A cartographer makes imaginary roads or street or a valley to prevent it from copying. The similar idea is to add a fictional head or cover to a message to prevent it from suspicion and spying. The modern applications use steganography applications as watermarks to copyright an entity. Photo collection that comes in a Compact Disk (CD) are often sold with steganography because it can contain a secret message that should be refrained from falling in the hands of illegal authorities.
4. **Medical Domain [18]-[20] –**The use of Steganography and its security aspects, specifically its medical imaging department, may benefit the healthcare industry, greatly. They use standards, which are called DICOM (Digital Imaging and Communication in Medicine). These standards separate the data from the caption and embed the name of the patient in its place which is a safety measure and can be used to prevent the exchange of reports, misbehaving or misplacing the reports, etc. In Medicare domain, Steganography is used in other significant fields such as ECG test reports, X-Ray reports, MRI, CAT-Scan, etc.

F. CryptoSteganography

The latest technology known in Information Security which overcomes the issues of Cryptography and Steganography is in the infant stage, thus uses are lesser known.

Generally, it is used in Text Data transfer by implementing Cryptography techniques of encryption, then embedding the ciphered text onto an image (cover file) and transmitted through some channel.

V. CONCLUSION

Any data transmitted for a communication opts for its security and safety. Communicating parties should have certified themselves for corresponding communication. The trusted third parties should check that the parties are functioning correctly.

Thus information security needs all the above necessities for the proper working of communication channel and security of that channel. This security can be achieved by one or the other methods, based on the requirement of the level of security and sensitivity of data. Each technique has its drawbacks, and a new technique was developed to overcome those. After the developed technique started being breached, there was a need for a more secure and safe technology to be developed. This can be achieved through knowledge of security standards that are predetermined.

REFERENCES

1. Sridhar, K., Dr Syed Abdul Sattar, and M. Chandra Mohan. "Comparison of digital watermarking with other techniques of data hiding." International Journal of Computer Science and Information Technologies (IJCSIT) 5.1 (2014): 350-353.
2. Kirovski, D., & Malvar, H. S. (2003). Spread-spectrum watermarking of audio signals. IEEE transactions on signal processing, 51(4), 1020-1033.
3. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.
4. Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997, October). A concrete security treatment of symmetric encryption. In Proceedings 38th Annual Symposium on Foundations of Computer Science (pp. 394-403). IEEE.
5. Febryan, Aryfandy, Tito Waluyo Purboyo, and Randy Erfa Saputra. "Steganography Methods on Text, Audio, Image and Video: A Survey." International Journal of Applied Engineering Research 12.21 (2017): 10485-10490.
6. Dobsicek, Microslav. "Modern Steganography." 8th International Student Conference on Electrical Engineering FEE CTU. 2004.
7. Por, Lip Yee, and B. Delina. "Information hiding: A new approach in text steganography." WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. No. 7. World Scientific and Engineering Academy and Society, 2008.
8. Pawar, Sagar S., and Vinit Kakde. "Review on Steganography for Hiding Data." International Journal of Computer Science and Mobile Computing 4 (2014): 225-229.
9. Gunjal, Monika, and Jasmine Jha. "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm." International Journal of Computer Trends and Technology (IJCTT) 11.4 (2014): 144-150.
10. Nick Sterling, Sarah Wahl, Sarah Summers, "Spread Spectrum Steganography"
11. Osuolale, A. Festus, "Secure data transfer over internet using Image CryptoSteganography" International Journal of Scientific and Engineering Research, December 2017
12. Surekha, B., and G. N. Swamy. "A spatial domain public image watermarking." International Journal of Security and Its Applications 5.1 (2011): 1-12.
13. Catorcini, Alessandro, et al. "Digital signatures with an embedded view." U.S. Patent No. 7,568,101. 28 Jul. 2009.
14. Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.
15. Podilchuk, Christine I., and Edward J. Delp. "Digital watermarking: algorithms and applications." IEEE signal processing Magazine 18.4 (2001): 33-46.
16. Stallings, William. Cryptography and network security, 4/E. Pearson Education India, 2006.
17. Doshi, Ronak, Pratik Jain, and Lalit Gupta. "Steganography and its applications in security." International Journal of Modern Engineering Research (IJMER) 2.6 (2012): 4634-4638.
18. Orooba Ismaeel Ibraheem Al-Farraji, "Hiding the Results of Medical Test in Medical Digital Image" International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
19. N. Suganya, M. Marimuthu, "ECG Steganography Based Privacy Protecting Of Medical Data for Telemedicine Application" International Journal of Innovative Research in Computer and Communication Engineering, March 2014
20. Manish Trehan, Pawan Kumar, "Hiding Data in X-Ray Scanned Images Using Both Steganography & Cryptography Tecniques" International Journal of Emerging Research in Management &Technology, Spetember 2017
21. Latika, "A Comparative Study of Cryptography, Steganography and Watermarking", Journal of Emerging Technologies and Innovative Research, May 2015
22. Pranali R. Ekatpure, Rutuja N. Benkar, "A Comparative Study of Steganography & Cryptography", International Journal of Science and Research, 2013
23. Patel N., Oza P., Agrawal S. (2019) Homomorphic Cryptography and Its Applications in Various Domains. In: Bhattacharyya S., Hassanien A., Gupta D., Khanna A., Pan I. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 55. Springer, Singapore
24. Parita Oza, Vishakha Khatrecha, Pooja Malvi, "Encryption Algorithm using Rubik's Cube Principle for Secure Transmission of Multimedia Files", International Conference on Multidisciplinary Research & Practice 2016

AUTHORS PROFILE

Yash Shah (16BIT090**),** student of Information Technology, Institute of Technology, Nirma University, will be starting his 4th year in B. Tech. Engineering Course. He has completed projects which are, "Leave Management System" using Java Technology, "Android Photo Editing Application" using Android and Java Technology, "Secure Data Transfer Using Video Steganography" with Python and Android implementation of related algorithm, "Hospital Management System" using PHP and MySQL and developed a front end of "Restaurant Website" using HTML, CSS and JavaScript. Also, a seminar works on "Data Center Network Architectures". Currently, he is pursuing a Summer Internship at Infibeam Avenues Limited, with Java Development Project namely "Project Management System".

Soham Joshi (16BIT103), student of Information Technology, Institute of Technology, Nirma University, will be starting his 4th year in B. Tech. Engineering Course. He has completed projects which are, "Leave Management System" using Java Technology, "Android Photo Editing Application" using Android and Java Technology, "Secure Data Transfer Using Video Steganography" with Python and Android implementation of related algorithm, "Movie Ticket Booking and Recommendation System" using Android with Java Technology and "Pacman Game" using HTML, CSS and JavaScript. Also, a seminar works on "Web Mining". Currently, he is pursuing Summer Internship at Stallion Archysis Limited, with the project of "Building a 24/7 Web Scrapping Service".

Prof Parita Oza is working as an Assistant Professor in Computer Science and Engineering Department since June 2008. Prof Oza has more than 14 years of teaching experience. She has pursued her BE in Information Technology from C U Shah College of Engineering and Technology and MTech in Information and Communication Technology from Nirma University. Her MTech thesis was in the area of Wireless Sensor Networks. Her research area includes Image Processing and Medical Imaging. She has several publications in international journals and conferences. She teaches at both Undergraduate and post graduate level. Currently, she is working in the area of Medical Imaging for classification and detection of Breast Cancer.

Prof Smita Agrawal is working as Assistant Professor at Department of Computer Science and Engineering, Nirma University since January 2009. She has a professional experience of over 14 years that footholds in academia. She received her Master of Computer Applications degree from Gujarat Vidhyapith in 2004. She is currently pursuing her doctoral studies in the field of Big Data Analytics from CHARUSAT University, Gujarat. Prof. Agrawal has published several research papers in national and international conferences and journals with indexing in Scopus, ICI. Prof Agrawal has conducted ISTE approved STTP in the field of Web Services using PHP. She works in the area of Big Data Analytics, Parallel Processing, Web Development and IoT.