International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 01 | Apr-2015 www.irjet.net p-ISSN: 2395-0072

Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation

Aarti Mehndiratta

M.Tech Scholar, Department of Computer Science & Engineering, S.E.C., Sri Ganganagar, Rajasthan,India

---

Abstract - ***In excess of the past few decades with progression in era of information society, computer networks and their related applications are becoming more and more popular. As the use of internet and reliance on the world wide system growing rapidly in daily life increase the number of networked machines which have leads unauthorized activity not only from external attackers, but also from internal attackers, such as disgruntled employees and people abusing their privileges for personal gain. The precious information is always prone to maximum attacks over the network. Attacks may occur due to system vulnerabilities or security breaches, such as system misconfiguration, user misuse or program defects. Attackers can also combine multiple security vulnerabilities into an intelligent attacking system. Therefore, an efficient security model is needed to defense secrete information over the network system. However, a number of approaches have been proposed in context to enhance the security of secrete information but each of them has its own limitation. These limitations represent problem with the current security systems and have led to an increasing interest in design and implementation of an efficient method to secure the secrete information. This paper presents a comprehensive investigation of two popular security techniques, cryptography and steganography, which performs better in comparison of other existing standard and automated security methods.***

Key Words: *Data Hiding, Cryptography, Steganography, AES, DES, DCT, DWT*

1. INTRODUCTION

Nowadays, uses of computer networks have gain tremendous growth to exchange information without any distance barrier. However, such network is most popular for fast and easy process to exchange information over the long distance but the safety and security of long-distance communication remains an issue in the case of confidential data. Day by day with the growth of computer networks, number of techniques has comes in new form to impacting availability, confidentiality, and integrity of critical data that poses a serious problem for safety vulnerabilities. On the other hand, a lot of approaches have been proposed by using the two popular security techniques, cryptography and stegnography, in direction to improve the security of secrete messages over the open communication channels but every time these technologies may not be reliable for communication of secrete information over a long distance that produce a need of additional security mechanisms to secure secrete information. Cryptography is used to scramble the information where the steganography embedded that into the cover medium. This chapter presents current high-tech investigation of these two security techniques with the issues to make clear the insufficiency of recent as well as customary security methods in a better way to the researchers and to motivates them to design a novel security system that improve the level of security.

2. CRYPTOGRAPHY

Cryptography is a widely used technique that encrypts plain text to generate cipher (encrypted) text. Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. Basically cryptography scrambles data for ensuring secrecy and/or authenticity of information and enables to transmit data across insecure networks so that it cannot be read by anyone except the authorized recipient [1, 2]. Cryptology and cryptanalysis are two main branches of cryptography. Cryptology is to keep plaintext secret from eavesdropper or simply the enemy while cryptanalysis deals with the defeating such techniques to recover information or forging information that will be accepted as authentic [3]. Generally, all cryptographic processes have four basic parts:

- **Plaintext -** Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as payroll data, personnel information, or a secret formula being transmitted between organizations.

- **Ciphertext-** Represents plain text rendered unintelligible by the application of a mathematical algorithm. Ciphertext is the encrypted plain text that is transmitted to the receiver.
- **Key-** A mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The key is the only way to decipher the scrambled information.

- **Cryptographic Algorithm –** A mathematical formula used to scramble the plain text to yield ciphertext. Converting plain text to ciphertext using the cryptographic algorithm is called encryption, and converting ciphertext back to plain text using the same cryptographic algorithm is called decryption. Figure 1 depicting the tactic of cryptography.

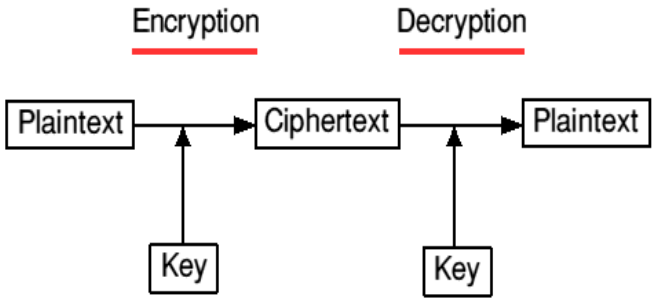

Figure 1 Cryptography

Broadly cryptographic algorithms can be divided into two categories:

- **Stream algorithms–** Operate on plaintext one byte at a time, where a byte is a character, number, or special character. The process is inefficient and slow.

- **Block algorithms –** Operate on plaintext in groups of bytes, called blocks (hence the name block algorithms or block ciphers). Typical block sizes for modern algorithms are 64 bytes, small enough to work with but large enough to deter code breakers. Unfortunately, with the current speed of microprocessors, breaking a 64-byte algorithm using brute force is proving to be to relatively easy task.

For securing the data following three types of cryptographic schemes are mostly used in today scenarios:

2.1 Secret Key Cryptography (SKC)

It also called symmetric-key cryptography scheme uses a single key for both encryption and decryption process. The Data Encryption Standard (DES) is a best example of this cryptosystem that is widely employed by the Federal Government. Figure 2 present illustration of the steps included in secretes key cryptography to make secure communication.

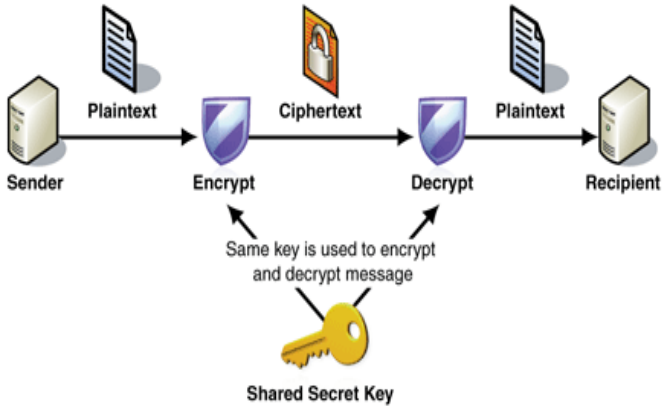

Figure 2 Symmetric / Secrete Key Cryptography

However, this mechanism improves the data security but distribution of the key between sender and its receiver is a challenging task because a not permitted person may get whole information effortlessly once he/she gets secrete key. Thus for secure communication the key security is a imperative issue with this approach.

- **Advantages of Symmetric Key Cryptography**
  - Quick recitation.
  - Rapid check authenticity of key recipients.
  - To get a plain texts same key is required as used at message encrypt time.
- **Disadvantages of Symmetric Key Cryptography**
  - Key sharing is a challenging task. Unauthorized person can get whole information without any effort if he/she gets secrete key.
  - This technique not provide digital signatures that cannot be repudiated

2.2 Public Key Cryptography (PKC)

Public key cryptography is an asymmetric scheme that uses a pair of keys, uses a public key for encryption process of secretes data, and a corresponding private, or secret key for decryption process. In this practice pair of keys required for the process. It is computationally infeasible to deduce the private key from the public key. Any one who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information. The RSA, Diffie-Hellman, Digital Signature Algorithm (DSA), Public-Key Cryptography Standards (PKCS), Key

Exchange Algorithm (KEA) are few examples of Asymmetric-Key Algorithms. Figure 3 shows the working steps of this algorithm.

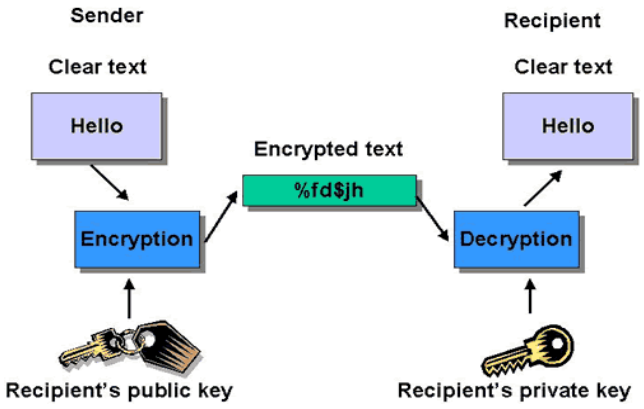

Figure 3 Asymmetric / Public Key Cryptography

- **Advantages of Asymmetric Key Cryptography**
  - Overcome the key distribution issues of symmetric key algorithms.
  - Public-key cryptography is not meant to replace secret-key cryptography, but rather to supplement it, to make it more secure.
  - By using pair of keys it increases the level of security.
  - Can provide digital signatures that can be repudiated
- **Disadvantages of Asymmetric Key Cryptography**
  - A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.
  - Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available.
  - Certification Problems, Many public key systems use a third party to certify the reliability of public keys.

2.3 Hash Functions

Hash functions use a mathematical transformation to irreversibly encrypt information. The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. Hash algorithms are effective because of the extremely low probability that two different plaintext messages will yield the same hash value.

There are several well-known hash functions in use today:

- **Hashed Message Authentication Code (HMAC):** Combines authentication via a shared secret with hashing.
- **Message Digest 2 (MD2):** Byte-oriented, produces a 128-bit hash value from an arbitrary-length message, designed for smart cards.
- **MD4:** Similar to MD2, designed specifically for fast processing in software.
- **MD5:** Similar to MD4 but slower because the data is manipulated more. Developed after potential weaknesses were reported in MD4.
- **Secure Hash Algorithm (SHA):** Modeled after MD4 and proposed by NIST for the Secure Hash Standard (SHS), produces a 160-bit hash value.

Figure 4 shows the process of Hash function.

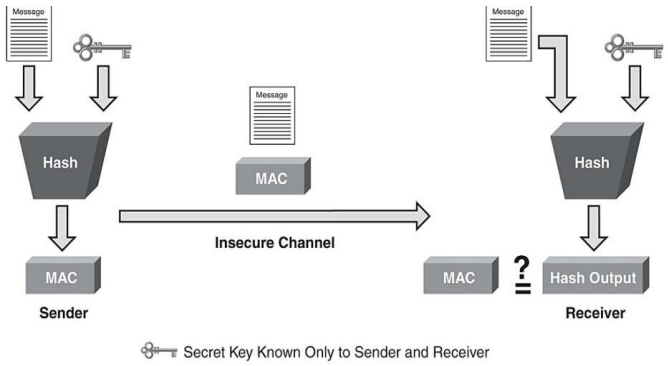

Figure 4 Hash Function

3. STEGANOGRAPHY

Steganography differs from cryptography. The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the

message is. In some cases, sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the best solution for secure communication; it is only part of the solution [4]. Steganography is derived from the Greek word steganos which means "covered" and graphia which means "writing", therefore Steganography means "covered writing". In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. Figure 5 present the steganography system overview.

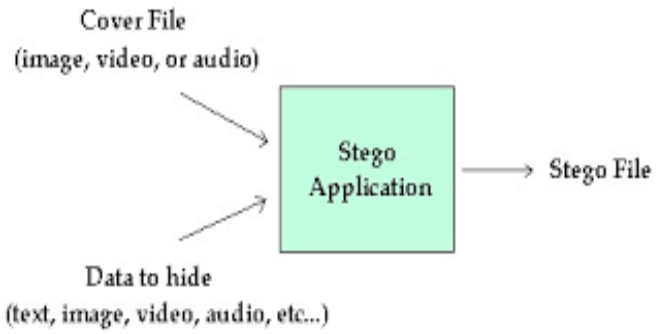

Figure 5 General Steganography Model

The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc. The steganography method provides embedded data in an imperceptible manner with high payload capacity.

Three basic types of steganography system are as follows

- **Image Steganography:-** For hiding the secret message into carrier image, which is then converted into stego image.
- **Audio Steganography:-** The secret message is embedded into unused audio bits as every file contains some unused bits or unused area of bits where secret message can be hided.
- **Video Steganography:-** This methodology divides the video into audio and image frames where embedding is performed in the audio file.

Steganography techniques that are in common use today include:

3.1 Discrete Cosine Transform (DCT):

In this scheme cover image transformed from spatial domain to frequency domain. Two dimension DCT transformations is used. After applying quantization and IDCT on DC coefficient, the encrypted secret image is embedded. This method uses JPEG compression algorithm to convert 8X8 pixel blocks in to 64 DCT co-efficient are modified to embed the encrypted secret .Since the methods works on frequency domain, it produces no noticeable changes in the visual appearance of the image. The disadvantages of this system are that it works only on JPEG files. In DCT, Encrypted secret image is placed in the low and mid frequency co-efficient.

3.2 Discrete wavelet transforms (DWT):

Wavelet transform (WT) converts spatial domain information to the frequency domain information wavelet are used in the image steganographic model because the wavelet transform clearly partitions the high frequency and low –frequency information on a pixel by pixel basis. Many practical tests propose to use the wavelet transform domain for steganography because of a number of advantages. The use of seek transform will mainly address the capacity and robustness of the information hiding system features.

In wavelet, both frequency response and time response information are known exact reconstruction is possible because of up sampling and down sampling of image. Advantages of DWT over DCT as, firstly no need to divide the input coding into non overlapping 20 blocks, it has higher compression ratio avoid blocking artifacts secondly, allows good localization both in time and spatial frequency domain. Thirdly, transformation of the whole image introduces inherent scaling. Finally better identification of which data is relevant to human perception higher high compression ratio. This method provides a high hiding capacity and good stego-image quality results analyses on the parameter peak signal to noise ratio by comparing the DCT domain and DWT domain. Peak signal to noise ratio is measure the quality of the stego-image by calculating the distortion between the stego-image and cover image higher the PSNR more is the security to image

However, the Steganography is closely related to the cryptography method to protect information from unwanted parties but neither alone technology is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. In case, when the steganography fail send the message can be detected, it is still of no use as it is encrypted using cryptography methods.

4. RELATED WORK

In [5] author uses an algorithm based on AES expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the 128 bit key, which changes for every set of pixel. The keys to be used are generated independently at the sender and receiver side based on AES key expansion process. Hence the initial key is shared rather than scaring the whole set of keys. The author gives the information about AES. The AES is provides high encryption quality with minimum memory requirement and computational time.

Steganography with cryptography provide powerful tools for image security over communication. There are various cryptographic technique combined with steganography for additional security [6,7] like DES , S- box mapping etc. However they are very complicated and involves large computation.

In [8] a comparative analysis between Joint Picture Expert Group (JPEG) image stegano and Audio Video Interleaved (AVI) video stegano by quality and size was performed. The authors propose to increase the strength of the key by using UTF-32 encoding in the swapping algorithm and lossless stegano technique in the AVI file. However, payload capacity is low.

In [9] an adaptive invertible information hiding method for Moving Picture Expert Group (MPEG) video is proposed. Hidden data can be recovered without requiring the destination to have a prior copy of the covert video and the original MPEG video data can be recovered if needed. This technique works in frequency domain only. It has the advantages of low complexity and low visual distortion for covert communication applications. However, it suffers from low payload capacity.

In [10], various technologies used in image steganography are proposed. This paper presents a review used for hiding a secret message or image in spatial and transform domain. This paper also proposed techniques for detecting the secret message or image i.e. steganalysis. The paper at [11] introduced a method where secret message is first compressed using wavelet transform technique and then embeds into cover image using LSB where the bits of secret message is inserted into image by using random number generator. In [12], authors give brief review of above techniques used for ensuring security. It proved in this paper that using these techniques, data can be made more secure and robust.

In [13] Author has dealt with three main stenography challenges capacity imperceptibility and security. This is achieved by hybrid data hiding scheme in corporate LSB technique with a key permutation method. A two layers of security system proposed in [14] by login procedure, firstly username and password are required and once login done, key is used to embed the secret data. Due to this, integrity and privacy is maintained. In same way another author has used idea of dual security in [15], secret data firstly converted to encrypted form and then LSB technique of steganography is used to embed it within cover object. By this method, message is transferred with utmost security and can be retrieved without any loss of data.

In [16] author proposed a technique by using LSB steganography and cryptography where the secret information is encrypted using RSA or Diffie Hellman algorithm before embedding in the image with the help of LSB method. With the proposed technique, time complexity is increased but high security is achieved at that cost. In [17] authors Proposed an optimal discrete wavelet transform (DWT) based steganography.Experiments show that the peak signal noise ratio (PSNR) generated by the proposed method is better. In same context a novel image steganography technique proposed in [18] that combines the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) is proposed which embeds secret image in frequency domain of cover image with high matching quality.

In [19], authors used a different approach to hide an image i.e. Hide behind Corner (HBC) algorithm is used to place a key at the image corners. All the keys at the corners are encrypted by generating Pseudo Random Numbers. Then the hidden image is transmitted. The receiver should know all the keys that are used at the corners while encrypting the image. Reverse Data Hiding (RDH) is used to get the original image and the original image is produced when all the corners are unlocked with proper secret keys used for hiding the image.

In paper [20] the authors proposed method gives the hide the information inside the image by using the replacement of LSB and MSB technique in that paper proposed work are as follows first of all find the key i.e. public key and private key according to RSA algorithm approach and encrypted the secret messages this algorithm is the most popular and proven asymmetric key cryptographic algorithm, RSA methodology and encode secret information. The secret information is encrypted and then encrypted ASCII value is transformed in binary form encrypt the information and then subsequently replace the MSB and LSB bit with information. The pixels image is also converted at the same time into the binary form. The image is used as a cover to insert the encrypted information. This process is finished by least significant bit (LSB) encoder which substitutes the least significant bit of pixel values with the encrypted information bits. In that one disadvantage occurred that is in that paper surely the time complication of the complete process increase.

In paper [21] authors proposed a scheme by including a mixture of cryptography and steganography to data confidentiality over secrecy there by increases the security level. It is used for the securely interchange private information between administrations. In this author suggests a two steps of security first one is encryption process and second one is steganography increase the security level for data hiding. In first stage message is transmitted and is first of all transformed in to a cipher image by using the first encryption process. Then in second stage this cipher image is to be transformed in to an intermediate text by using the second encryption process. The intermediate cipher text or information created hidden text inside a cover image by using steganography to hidden the presence of the secret and this resultant steganography image is transferred to the receiver done the network. Thus in that paper dual encryption and steganography scheme are proposed the encryption process is fully dependent on a key, encryption process used the RSA algorithm and steganography technique is used for the embedding of the image, steganography used LSB technique.

5. Conclusion

This paper presents a state of the art investigation work in the area of two popular information security approaches, namely cryptography and steganography. However both of techniques provide security for secrete information, Where cryptography modify set-up of the information in way that only its authorized recipient person can get the text message, the steganography hide complete information in the cover media, so no one can easily identify that any message is hidden in the presented content but no one standalone approach is so good for practice. Therefore to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed. Future work can be done in way to combining the concepts of cryptography and stegnography, to provide more security to the secrete message.

REFERENCES

[1] Menezes, Alfred , Paul C van Oorschot ,Scott A. Vanstone, " Handbook of Applied Cryptography. CRC Press", October 1996 , ISBN 0-8493-8523-7.

[2] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[3] W. Stallings, Cryptography and network security: principles and practice. Prentice Hall, 2010, vol. 998.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012

[5] B. Subramanan "Image encryption based on aes key expansion" in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.

[6] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, "Security Improvisation in image Steganography using DES",3rd IEEE Trans. International Conference IACC -2013, Page(s): 1094 – 1099.

[7] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, Monika Sharma "Image Stenography: Self Extraction Mechnanism", UACEE International Journal of Advances in Computer Science and its Applications- IJCSIA Vol -3 Issue -2 ,ISSN 2250-3765 Pg-145-148, 2013.

[8] R.Kavitha and A. Murugan, "Lossless Steganography on AVI File using Swapping Algorithm", International Conference on Computational Intelligence and Multimedia Applications, pp. 83-88, Sivakasi-Tamil Nadu, Dec. 2007

[9] Yueyun Shang, "A New Invertible Data Hiding in Compressed Videos or Images", Third International Conference on Natural Computation (ICNC 2007), Vol. 4, pp. 576-580, Haikou, Aug. 2007.

[10] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, Dec 2012, pp. 171-177.

[11] Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Pwer and Computing Technologies, March 2013, pp. 1197-1200.

[12] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Stegocrypto - A Review of Steganography Techniques using Cryptography", International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, Vol. 4, 2013, pp. 423-426.

[13] Marghny Mohamed"Data hiding by LSB substitution using genetic optimal key permutation " in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.

[14] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, vol. 2, pp. 102-108, 2011

[15] K.Sakthisudhan, P.Prabhu, "Dual Steganography Approach for Secure Data Communication" International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, vol. 38, pp. 412-417, 2012

[16] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" International Journal Modern Education and Computer Science, vol. 6, pp. 27-34, 2012
[17] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.
[18] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.
[19] Hemalatha M., Prasanna A., Dinesh Kumar R., Vinoth kumar D., "Image Steganography using HBC and RDH Technique", International Journal of Computer Applications Technology and Research, Vol.3, 2014, pp. 136-139.
[20] Basant Sah and Vijay Kumar,"A New Approach to Data hiding Using Replacement of LSB and MSB" ISSN: 2277 128X Volume 3, Issue 11, November 2013.
[21] A Aswathy Nair and Deepu Job,"A Secure Dual Encryption Scheme combined With Steganography" IJETT-Volume 13 Number 5-Jul 2014.

BIOGRAPHIES

Ms. Aarti Mehndiratta currently pursuing M.Tech (Computer Science) from Sri Ganganagar Engineering College, Sri Ganganagar, affiliated to Rajasthan Technical University, Kota. She did B.TECH in Computer Science and Engg. from Sri Balaji College of Engg. & Technology, Jaipur in 2012. Her interested research areas are Network Security, Information Security System.

