International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Steganography & Cryptography for Regimented Data Hiding System: A Review

Akash Sharma[1], Nikita Jain[2]

[1]M.Tech Scholar, Department of Computer Science & Engineering, G.I.T., Jaipur, Rajasthan, India

[2]Assistant Professor, Department of Computer Science & Engineering, G.I.T., Jaipur, Rajasthan, India

Abstract: ***Nowadays, due to rapid development of communication techniques & its applications over the open communication channel, security-issues have the top priority. Communication of secret information is a critical factor in information technology that continues to create challenges with increasing levels of sophistication. However, in recent years, two techniques cryptography and steganography have been used widely in direction to trim down the security issues but different terrains pose separate challenges. This paper presents a comprehensive investigation on modern as well as traditional security methods with their inadequacies in direction to explain accessible security techniques in better way to new researchers and motivate them to design and implement a novel system that improve the level of security.***

Keywords: Information Hiding, Security, Steganography, Cryptography.

1. Introduction

Nowadays, due to rapid growing technologies the digital communication media is a more popular pathway for data sharing. Everyone wants to connect and share information at touch of a button. However, quick development of web technologies made easier to send and receive information over long distances but this electronic media is prone to unwanted interception. One of the most significant factors of information technology and data communication is security. All and sundry wants the secrecy and safety of their communicating data. In this context, since the age of network technologies numerous researchers has proposed different approaches to deliver secret information safely between remote users over an insecure channel but still safe and sound communication is a critical factor in information technology that continues to create challenges with increasing levels of sophistication. Although researchers constantly developing improvements to current security systems. However, in modern world of digital communication a complete secure system is a dream but two techniques could be used to secure the secrete data over open channels. These mechanisms are cryptography and steganography [1]. Cryptography addresses the necessary elements for secure communication namely privacy, confidentiality, key exchange, authentication, and non-repudiation. It scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form but reveal the fact that a message in cipher text might arouse suspicion on the part of the recipient. Steganography takes security a step farther from cryptography by hiding the existence of the information. Basically, Steganography can be used to cloak hidden messages in image, audio, video and even text files.

2. Cryptography

The process, discipline or techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form is called cryptography. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers [2, 3]. However, encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable. Cryptography systems can be broadly classified into

2.1 Secret/Symmetric Key Cryptography (SKC):

The symmetric key systems (depicted in figure 1) use a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message.

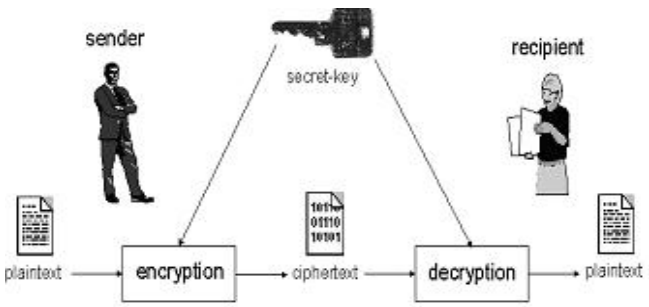

Figure 1: Symmetric Key Cryptography

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher. Examples of algorithms using symmetric-key cryptography:

- ***Caesar Cipher***: Every letter in plain-text is replaced by the third alphabet from it to produce the cipher-text. A-> D, B->E, and so on.
- ***Mono-alphabetic Cipher***: Every letter in plain-text is replaced by some other random alphabet.

Secret key cryptography algorithms that are in use today include:

- ***Data Encryption Standard (DES): D****ata* ***E****ncryption* ***S****tandard*, a popular symmetric-key encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92. DES uses a 56-bit key and uses the block cipher method, which breaks text into 64-bit blocks and then encrypts them. It operate in CBC (chain block coding), ECB (Electronics codebook) and CFB (Cipher feedback) modes. DES has 16 rounds which mean a total of 16 processing steps are being applied on the input plaintext to produce cipher text. First, 64 bit data is passed through the initial permutation phase and then 16 rounds of processing takes place and finally the last step of final permutation is carried out on the input plaintext which results in 64 bit cipher text. The drawback of this algorithm is that it can be easily prone to brute force attack in which the hacker attempts to break the key by applying all possible combination. In DES there are only 256 possible combinations which are quite easy to crack. So DES is not so secure [4].
- ***Advanced Encryption Standard (AES):*** The Advanced Encryption Standard or AES is a symmetric block cipher Initiated in 1997,used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES was designed not only to replace the Data Encryption Standard (DES) but also to be more secure than its predecessor. Compared to DES, AES offers a large key size, a 128-bit key (the default), a 192-bit key, and a 256-bit key.
- ***Blowfish:*** A symmetric 64-bit block cipher invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.
- ***Twofish:*** A 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Designed by a team led by Bruce Schneier and was one of the Round 2 algorithms in the AES process.

2.2 Public/ Asymmetric Key Cryptography (PKC/AKC):

This systems use a different key for encryption as the one used for decryption as depicted in figure 2. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key.

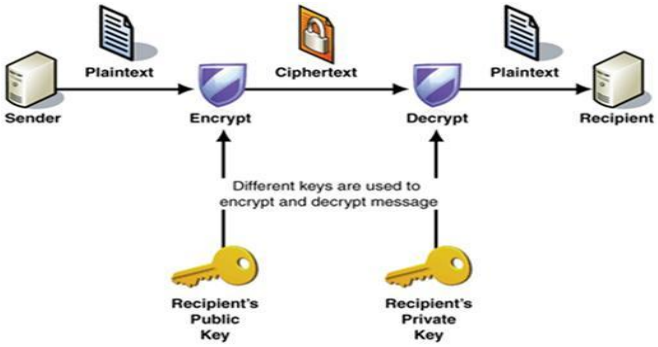

Figure 2: Asymmetric Key Cryptography

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

- ***RSA:*** RSA is a most popular and proven asymmetric crypto graphy algorithm. RSA is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers. Disadvantages of RSA algorithm takes more time for computation process. RSA takes more memory than AES and DES. RSA algorithm produces low level of output bytes
- ***Diffie-Hellman:*** After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key exchange only, and not for authentication or digital signatures.
- ***Digital Signature Algorithm (DSA):*** The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.
- ***ElGamal:*** Designed by Taher Elgamal, a PKC system similar to Diffie-Hellman and used for key exchange.
- ***Elliptic Curve Cryptography (ECC):*** A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

2.3 Hash Functions

This method uses a mathematical transformation to irreversibly "encrypt" information. *Hash functions*, also called *message digests* and *one-way encryption*, are algorithms that, in some sense, use no key (Figure 3). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Figure 3: Hash Function

Hash algorithms that are in common use today include:

- ***Message Digest (MD) algorithms:*** A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
- ***Whirlpool:*** it operates on messages less than 2256 bits in length, and produces a message digest of 512 bits. The design of this has function is very different than that of MD5 and SHA-1, making it immune to the same attacks as on those hashes.
- ***Tiger:*** it designed to be secure, run efficiently on 64-bit processors, and easily replace MD4, MD5, SHA and SHA-1 in other applications. Tiger/192 produces a 192-bit output and is compatible with 64-bit architectures; Tiger/128 and Tiger/160 produce a hash of length 128 and 160 bits, respectively, to provide compatibility with the other hash functions mentioned above.

3. Steganography

Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention. Steganography was used even in ancient times and these ancient methods are called Physical Steganography. Some examples for these methods are messages hidden in messages body, messages written in secret inks, messages written on envelopes in areas covered by stamps, etc. Modern Steganography methods are called Digital Steganography. These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the message within video files, etc. Furthermore, Network Steganography is used in telecommunication networks. This includes techniques like Steganophony (hiding a message in Voice-over-IP conversations) and WLAN Steganography (methods for transmitting Steganograms in Wireless Local Area Networks). The basic steganographic system is shown in Fig.4

Figure 4: Basic Steganographic System

Three basic types of steganography system are as follows

i) **Image Steganography:**-For hiding the secret message into carrier image, which is then converted into stego image.

ii) **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.

iii) **Video Steganography:-** This methodology divides the video into audio and image frames where embedding is performed in the audio file.

Steganography that are in common use today include:

- **Discrete Cosine Transform (DCT):** In this the cover image is 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.
- **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

4. Related Work

Several techniques have been proposed by researchers for securing electronic communication. In [5] author has proposed a scheme using video file as a cover carrier. Video based steganography can be used as one video file having separate images in frames. Since that the use of the video based steganography can be more eligible than other multimedia files. This author is mainly concerned with how to embed data in a video file in from of bmp images and how we can make use of the internal structure of the video to hide

data to be secured. In [6] author gave a different concept from above the authors using a new approach of hiding image in video. The algorithm is replaces 1 LSB of each pixel in video frame. It becomes very difficult for a intruder to guess that an image is hidden in the video as individual frame are difficult to analyze in a video running at 30 frame per second. In [7] 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.

In [8] 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 [9] 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 [10], 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 [11] 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. A DWT based Dual steganographic technique proposed in [12]. By using DWT, a cover image is decomposed into four subbands. Two secret images are hidden within HL and HH subbands respectively by usage of a pseudo random sequence and a session key. By this technique fair amount of information is transferred in a secured way with an acceptable level of imperceptibility. An enhanced LSB approach proposed in [13] which embed the secret data only in one i.e. blue component instead of all RGB components. With this new technique, the performance of LSB has been improved which leads to the minimization of the distortion level that is negligent to human eye. This will increase the robustness but will decrease the payload capacity. [14] proposed a novel security scheme in which steganography is combined with cryptography. In this scheme, secret data is converted to encrypted form using Advanced Encryption Standard (AES) and then the encrypted data is embedded into the cover image using Pixel Value Differencing (PVD) and K-bit LSB substitution method of steganography. Due to which high security along with good imperceptibility and sufficient amount of payload capacity is obtained.

In [15] authors proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step, finds the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information depending on the matching method. In [16] authors developed a technique in which steganography and cryptography are used together, in which the cover image is first converted into scrambled form and then divided into bit planes in which the secret data is embedded. With this method, good imperceptibility along with high security is obtained but has less payload capacity and also limited to grayscale images only.

In [17], 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 [18] 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 [19], 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 the paper at [20], authors define basic terminologies of steganography, steganography techniques, classifications and review of previous work done by researchers. In paper [21], user selects secret image in BMP format and encrypts using BLOWFISH cryptography Algorithm because BLOWFISH is faster, stronger and gives good performance when compared with DES, 3DES, AES, RC6, RC4. This encrypted image is embedded into video using LSB technique and forms stego video. This method provides confidentiality, authenticity, integrity and non-repudiation. The paper [22] proposed a security scheme where secret data is encrypted using RSA encryption algorithm and then user selects any image suited for hiding particular data and then this secret data is embedded into cover image using LSB. This will make difficult for an attacker to steal sensitive information. Finally, a stego image has been produced. In paper [23] user selects plain text and encrypts using BLOWFISH Algorithm. This encrypted text is embedded into image using LSB technique and forms stego image. Reverse procedure is done for decrypting the secret image.

In paper [24] 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 [25] 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. In [26], 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.

5. Issues with Existing Security Approaches

However, modern security techniques might secure the secrete information but most of methods are based on the cryptographic techniques, where cyber attacker easily arouse these act and intercepts the communication between two separate users to modify, inject, or drop any communication packet. Several paper [4,5,6] discussed problems of cryptography. Issues of cryptographic methods may reduce by using the steganography techniques that provides a high level of security, particularly when it is combined with encryption. The traditional steganography techniques rely on the encoding system's secrecy to secure the information. The system able to provide security but have a problem that if attacker known than it is simple enough to expose the entire received media passing by to check for hidden messages ultimately, such a steganographic system fails. Beside this problem in steganography the image and video codec are block-based and possible bit-errors usually destroy the data only in a single block or even all the blocks in the rest of the row of macro blocks (slice). These block errors decrease the visual quality drastically. Hence, the concealment of such block losses is a realistic situation in many cases, except for the damage of some header information. These inadequacies of modern as well as traditional security methods shows the single security technique either cryptography or steganography is not a turnkey solution to secure the secrete information over the open system. For a strong system it is always better to use both cryptography and steganography together.

6. Conclusion

This paper has present the investigation of two security approaches, namely cryptography and steganography. Where the cryptography only change the format of the information that cannot be understood by any unauthorized user, the steganography hide the complete information in the cover media, so no one can easily identify that any message is hidden in the presented content. However both of these techniques provide the security to information but the standalone approach based of either of these techniques is not 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] Mihir H Rajyaguru, "Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.
[2] R. Anderson, "Cryptanalytic Properties of Short Substitution Ciphers", Taylor & Francis, Cryptologia, Vol. XIII, No. 1, pp. 61-72, January, 1989.
[3] G. J. Simmons, "Subliminal Channels: Past and Present," European Transactions on Telecommunications, Vol. 4, No. 4, pp. 459-473, Aug 1994.
[4] Diaa Salama, Abdul Minaam ,Hatem M .Abdual-Kader and Mohiy Mohamed Hadhond," Evaluating the effects of Symmetric Cryptography Algorithm an Power Consumption for Network Security.pp.78-87,Sep-2010.
[5] A.K. Al Frajat "Hiding data in video file An overview" Journal of applied sciences 10(15):1644-1649, 2010.
[6] Saurabh singh "Hiding Image to Video" International Journal of engineering science & technology Vol. 2(12), 6999-7003 ,2010.
[7] 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.
[8] 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.
[9] 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
[10] 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

[11] 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
[12] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum" International Journal of Modern Engineering Research, vol. 1, pp. 157-161, 2012
[13] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, " Enhanced Least Significant Bit algorithm For Image Steganography", International Journal of Computational Engineering & Management, vol. 15, pp. 40-42, 2012
[14] Phad Vitthal S.,Bhosale Rajkumar S.,Panhalkar Archana R., " A Novel Security for Secret Data using Cryptography and Steganography" International Journal Computer Network and Information Security, vol. 2, pp. 36-42,2012
[15] Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. European Journal of Scientific Research, 40(2). ISSN: 1450-216X. EuroJournals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.
[16] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M. Bhat, "Data hiding in scrambled images: A new double layer security data hiding technique" Computers and Electrical Engineering, Elsevier,vol. 40,pp. 70-82, 2014
[17] 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.
[18] 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.
[19] 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.
[20] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", International Journal of Advanced Science and Technology, Vol. 54, 2013, pp. 113-124.
[21] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal , "Secure Image Hiding Algorithm using Cryptography and Steganography", IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-8727, Vol. 13(5), August 2013, pp. 1-6.
[22] M.Juneja, P.S. Sandhu, "Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images", International Journal of Applied Research , ISSN: 2249-555X , Vol. 3(5), May 2013, pp. 118-120.
[23] Ajit Singh, Swati Malik, "Securing Data by using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3(5), May 2013, pp. 404-409.
[24] 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.
[25] A Aswathy Nair and Deepu Job,"A Secure Dual Encryption Scheme combined With Steganography" IJETT-Volume 13 Number 5-Jul 2014.
[26] 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.

Author Profile

Mr. Akash Sharma currently pursuing M.Tech(Computer Science) From GIT College Jaipur affilated to Rajasthan Technical University, Kota. He did **B.TECH** in Computer Science and Engineering from **xxxx in 2010.** His interested areas of research are Information Security System, Network security and Algorithms.

Ms. Nikita Jain obtained B.Tech. Degree in Computer Science & Engg. from UPTU in 2005 and also completed her M.Tech. in 2014 from Rajasthan Technical University, Kota. She has more than 20 international and national publications in her account. Her interested research areas are data mining, cryptography, image processing